



ΗΥ - 280 Θεωρία Υπολογισμού

Διάλεξη 15

Κωνσταντίνος Βάρσος

Τμήμα Επιστήμης Υπολογιστών – Πανεπιστήμιο Κρήτης

Χειμερινό εξάμηνο 2025 - 26

Υπολογισιμότητα

Τι είδαμε στην Διάλεξη 14

- Μη-διαγνωσιμότητα A_{TM} .
- Το πρόβλημα του Τερματισμού.
- Μη επιλύσιμα προβλήματα.
- Μέθοδος Αναγωγής.
- Αναγωγή μέσω υπολογιστικού χρονικού.

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Συνήθως η μέθοδος αυτή χρησιμοποιείται όταν η μη-διαγνωσιμότητα σχετίζεται με κάποιον έλεγχο ύπαρξης [10ο πρόβλημα Hilbert]

■ Έστω TM M και w συμβολοσειρά εισόδου. Ένα **υπολογιστικό χρονικό** της M επί της w είναι μια ακολουθία φάσεων $\{C_1, C_2, \dots, C_\ell\}$ τ.ω.:

- $C_1 = q_0 w$ είναι η αρχική φάση,
- C_i παράγει C_{i+1} για όλα τα $1 \leq i < \ell$, και
- C_ℓ είναι μια φάση τερματισμού [είτε σε κατάσταση αποδοχής είτε σε κατάσταση απόρριψης].

Αν C_ℓ είναι αποδεκτή, τότε το χρονικό ονομάζεται **αποδεκτό**. Αν C_ℓ είναι απορριπτέα, τότε το χρονικό ονομάζεται **απορριπτικό**.

■ Η M αποδέχεται την w ανν η M επί της w έχει ένα αποδεκτό υπολογιστικό ιστορικό.

Αναγωγή μέσω του υπολογιστικού χρονικού

- Ένα **γραμμικώς φραγμένο αυτόματο** (LBA) είναι μια φραγμένη TM M τ.ω. όταν η M εκτελείται σε οποιαδήποτε συμβολοσειρά εισόδου w , η κεφαλή της παραμένει πάντα εντός των πρώτων $|w|$ κελιών.
- Η 'γραμμικότητα' προέρχεται από το ότι $|\Gamma| > |\Sigma|$.
- Οι μηχανές για τα A_{DFA} , E_{DFA} , A_{CFG} , E_{CFG} , A_{CFL} είναι LBA.

Αναγωγή μέσω του υπολογιστικού χρονικού

Λήμμα. Έστω M LBA με $|K| = q$ και $|\Gamma| = g$. Το πλήθος των διαφορετικών φάσεων του M για ταινία μήκους n είναι qng^n .

Απόδειξη. Κάθε φάση του M αποτελείται από: 1) την κατάσταση, 2) την θέση της κεφαλής στην ταινία, και 3) το περιεχόμενο της ταινίας.

Υπάρχουν q καταστάσεις, η θέση της κεφαλής έχει n πιθανές θέσεις, και σε μια ταινία μήκους n μπορούν να καταχωρηθούν μέχρι g^n διαφορετικές συμβολοσειρές από σύμβολα ταινίας.

Πολλαπλασιάζοντας τους τρεις όρους βρίσκουμε το αποτέλεσμα. □

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Έστω το πρόβλημα

$$A_{\text{LBA}} = \{ \langle M, w \rangle \mid \text{η TM } M \text{ είναι LBA που αποδέχεται } w \}.$$

Θεώρημα. Η A_{LBA} είναι διαγνώσιμη.

Απόδειξη. (Ιδέα) Κατασκευάζουμε TM, L , για την A_{LBA} . Προσομοιώνουμε την M για είσοδο w . Εάν κάποια στιγμή η προσομοίωση αποδεχτεί ή απορρίψει, αποδεχόμαστε ή απορρίπτουμε. Για να ανιχνεύσουμε τυχόν εγκλωβισμό εκμεταλλευόμαστε τα φραγμένα χαρακτηριστικά της M .

$L =$ “Για είσοδο $\langle M, w \rangle$:

1. Προσομοιώνουμε το M για w μέχρι να τερματίσει ή να συμπληρώσει qng^n βήματα.
2. Εάν το M αποδεχτεί, αποδεχόμαστε.
Εάν το M απορρίψει, απορρίπτουμε.
Εάν το M δεν τερματίσει, απορρίπτουμε.”

□

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Έστω το πρόβλημα

$$E_{LBA} = \{\langle M \rangle \mid \text{η TM } M \text{ είναι LBA και } L(B) = \emptyset\}.$$

Θεώρημα. Η E_{LBA} είναι μη-διαγνώσιμη.

Απόδειξη. Με αναγωγή από το A_{TM} στο E_{LBA} μέσω υπολογιστικού χρονικού. Υποθέτουμε ότι έχουμε έναν διαγνώστη R για το E_{LBA} . Χρησιμοποιώντας τον R , κατασκευάζουμε έναν διαγνώστη S για το A_{TM} :

$S =$ “Για είσοδο $\langle M, w \rangle$:

1. Κατασκευάζουμε έναν LBA B τ.ω. $L(B) \neq \emptyset$ ανν το M αποδέχεται το w .
2. Εκτελούμε τον R στο $\langle B \rangle$.
3. Αν ο R αποδεχτεί, τότε **απορρίπτει**.

Αν ο R απορρίψει, **αποδέχεται**.”

Ο S δεν είναι εφικτός, συνεπώς ούτε και ο R . Άρα, η E_{LBA} μη-διαγνώσιμη. □

Αναγωγή μέσω του υπολογιστικού χρονικού

■ $L(B) \neq \emptyset \iff B$ αποδέχεται το w .

Η κατασκευή του LBA B ακολουθεί τα εξής βήματα:

- Το B θα προσομοιώσει τη TM B πάνω στην είσοδο w .
- Η ταινία του B θα περιοριστεί στο μήκος της w , συν κάποια επιπλέον κελιά για τις ανάγκες της προσομοίωσης [γραμμικός περιορισμός].
- Το B θα χρησιμοποιήσει τις καταστάσεις και τους κανόνες μετάβασης της M για να εκτελέσει την προσομοίωση.
- Αν η M αποδεχθεί το w , τότε το B θα εισέλθει σε τερματική κατάσταση, υποδεικνύοντας ότι η γλώσσα $L(B)$ δεν είναι κενή.
- Αν η M δεν αποδεχθεί το w , τότε το B θα βρεθεί σε απορριπτική κατάσταση ή θα εγκλωβιστεί, άρα $L(B) = \emptyset$.

...

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Αν $L(B) \neq \emptyset$. Αυτό σημαίνει ότι υπάρχει κάποια ακολουθία μεταβάσεων του B που οδηγεί σε αποδεκτική κατάσταση.

- Επειδή ο B προσομοιώνει τη ΤΜ M , αυτή η αποδεκτική κατάσταση αντιστοιχεί σε αποδοχή της εισόδου w από την M .
- Άρα, η M αποδέχεται το w .

■ Αν M αποδέχεται το w .

- Επειδή η M αποδέχεται το w , υπάρχει μια ακολουθία μεταβάσεων στην M που οδηγεί σε αποδεκτική κατάσταση.
- Το B , προσομοιώνοντας την M , θα ακολουθήσει τις ίδιες μεταβάσεις, και επειδή η ταινία του είναι γραμμικά φραγμένη, θα φτάσει σε αποδεκτική κατάσταση.
- Άρα, η γλώσσα $L(B)$ δεν είναι κενή.

$$L(B) \neq \emptyset \iff M \text{ αποδέχεται το } w.$$

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Κατασκευάζουμε το B έτσι ώστε να αποδέχεται ακριβώς όλες τις συμβολοσειρές της μορφής

$$\#C_1\#C_2\#C_3\#\dots\#C_\ell\#$$

όπου οι $C_1, C_2, \dots, C_\ell$ αποτελούν ένα αποδεκτό υπολογιστικό ιστορικό της M στο w .

$$[L(B) \neq \emptyset \iff M \text{ αποδέχεται το } w]$$

■ Αυτόματο B

$B =$ “Για είσοδο x :

1. Αν το x δεν είναι της μορφής $\#C_1\#C_2\#C_3\#\dots\#C_\ell\#$ για συμβολοσειρές $C_1, C_2, \dots, C_\ell$, τότε **απορρίπτει**.
2. Επαληθεύει αν το $\#C_1\#C_2\#C_3\#\dots\#C_\ell\#$ ικανοποιεί τα παρακάτω.
 - i) $C_1 = q_0w$.
 - ii) C_i παράγει C_{i+1} για όλα τα $1 \leq i < \ell$.
 - iii) C_ℓ αποδεκτή φάση τερματισμού.
3. Αν και οι τρεις συνθήκες είναι αληθείς, τότε **αποδέχεται**, αλλιώς **απορρίπτει**.

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Έστω το πρόβλημα

$$ALL_{CFG} = \{ \langle G \rangle \mid \eta \ G \ \text{είναι CFG και } L(G) = \Sigma^* \}.$$

Θεώρημα. Η ALL_{CFG} είναι μη-διαγνώσιμη.

Ιδέα. Δείχνουμε ότι για μια TM M και μια συμβολοσειρά w , μπορούμε να κατασκευάσουμε ένα PDA D .

- Το D αποδέχεται όλες και μόνο τις συμβολοσειρές που δεν είναι αποδεκτά υπολογιστικά χρονικά $C_1, C_2, \dots, C_\ell$ της M στο w .
- Για το PDA (για τεχνικούς λόγους), κωδικοποιούμε ένα χρονικό με κάθε δεύτερη φάση αντεστραμμένη:

$$C_1 \# C_2^R \# C_3 \# C_4^R \dots \# C_\ell.$$

Αναγωγή μέσω του υπολογιστικού χρονικού

Άρα η M με είσοδο w , κατασκευάζει D που παράγει όλες τις συμβολοσειρές αν και μόνο αν η M δεν αποδέχεται το w .

- Έτσι, αν η M αποδέχεται το w , το D δεν παράγει κάποια συγκεκριμένη συμβολοσειρά.
- Αυτή η συγκεκριμένη συμβολοσειρά είναι αποδεκτό υπολογιστικό χρονικό για την M στο w .
- Δηλαδή, το D έχει σχεδιαστεί για να παράγει όλες τις συμβολοσειρές που δεν είναι αποδεκτά υπολογιστικά χρονικά για την M στο w .

Αποτυχία Υπολογιστικού Χρονικού. Ένα υπολογιστικό χρονικό αποτυγχάνει αν:

- 1 Το C_1 δεν είναι η αρχική φάση.
- 2 Το C_ℓ δεν είναι αποδεκτή φάση.
- 3 Κάποιο C_{i+1} δεν παράγεται από το C_i .

Αναγωγή μέσω του υπολογιστικού χρονικού

■ Το D επιλέγει μη ντετερμινιστικά μια αποτυχία για έλεγχο.

1. Για να ελέγξει το C_1 , το D διαβάζει το C_1 , αποδεχόμενο αν το πρώτο σύμβολο δεν είναι το q_{start} ή αν η συμβολοσειρά μεταξύ του q_{start} και του πρώτου $\#$ δεν είναι το w .
2. Για να ελέγξει το C_ℓ , το D διαβάζει το C_ℓ , αποδεχόμενο αν εμφανιστεί μια κατάσταση διαφορετική από το q_{accept} (ή αν εμφανιστούν περισσότερες από μία καταστάσεις).

Αναγωγή μέσω του υπολογιστικού χρονικού

3. Για να ελέγξει μια αποτυχία στη δ , το D επιλέγει ένα C_i για να συγκρίνει με το C_{i+1} .
 - Το D αναθέτει το C_i στη στοίβα.
 - Στη συνέχεια διαβάζει το C_{i+1} , συγκρίνοντας τα σύμβολα με το C_i .
 - Το C_i είναι ανεστραμμένο σε σχέση με το C_{i+1} . Τα σύμβολα που αφαιρούνται από τη στοίβα πρέπει να ταιριάζουν με αυτά που διαβάζονται από το C_{i+1} [εκτός από αλλαγές λόγω της δ].
 - Το D αποδέχεται αν η μετάβαση είναι άκυρη.
- Παρατηρήστε ότι το D απορρίπτει μόνο αποδεκτά υπολογιστικά χρονικά της M στο w .
- Έτσι, αν το D αποδέχεται όλες τις συμβολοσειρές, τότε δεν υπάρχουν τέτοια χρονικά [και έτσι η M δεν αποδέχεται το w].
- Ως εκ τούτου, θα μπορούσαμε να χρησιμοποιήσουμε έναν διαγνώστη R για το ALL_{CFG} για να διαγνώσουμε το A_{TM} .

Αναγωγή μέσω του υπολογιστικού χρονικού

Θεώρημα. Η ALL_{CFG} είναι μη-διαγνώσιμη.

Απόδειξη. Έστω ότι ALL_{CFG} διαγνώσιμη με διαγνώστη R . Θα κατασκευάσουμε TM S για το A_{TM} .

$S =$ “Για είσοδο $\langle M, w \rangle$:

1. Κατασκευάζουμε PDA D για M και w όπως περιγράφηκε.
2. Μετατρέπουμε το D στην CFG G .
3. Εκτελούμε το R για την G .

Αν R αποδέχεται $\langle G \rangle$, απορρίπτουμε. [μη αποδεκτά χρονικά]

Αν R απορρίψει $\langle G \rangle$, αποδεχόμαστε. [$\exists$ αποδεκτό χρονικό]”



Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Δείξτε ότι η γλώσσα

$$INF_{PDA} = \{ \langle M \rangle \mid M \text{ είναι PDA και } L(M) \text{ άπειρη} \}.$$

είναι διαγνώσιμη.

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Δείξτε ότι η γλώσσα

$$INF_{PDA} = \{ \langle M \rangle \mid M \text{ είναι PDA και } L(M) \text{ άπειρη} \}.$$

είναι διαγνώσιμη.

Λύση. Θα σχεδιάσουμε μια TM T που αποφασίζει το INF_{PDA} :

$T =$ “Για είσοδο $\langle M \rangle$, όπου M ένα PDA :

1. Κατασκευάζουμε ισοδύναμη CFG G από το M .
2. Αποδέχεται $\langle M \rangle$ αν $\exists$ παραγωγή $A \xRightarrow{+} uAv$ για κάποια $u, v \in \Sigma^*$.

Αλλιώς, απορρίπτει.”

Εφόσον όλοι οι αλγόριθμοι σε αυτή τη μηχανή τερματίζουν σε πεπερασμένο χρόνο, η γλώσσα INF_{PDA} είναι διαγνώσιμη. □

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Δείξτε ότι η γλώσσα

$$L = \{\langle M \rangle \mid M \text{ DFA που δεν αποδέχεται καμία συμβολοσειρά με περιττό πλήθος } 1\}.$$

είναι διαγνώσιμη.

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Δείξτε ότι η γλώσσα

$L = \{\langle M \rangle \mid M \text{ DFA που δεν αποδέχεται καμία συμβολοσειρά με περιττό πλήθος } 1\}.$
είναι διαγνώσιμη.

Λύση. Θα σχεδιάσουμε μια TM B η οποία διαγιγνώσκει την L :

$B =$ “Για είσοδο $\langle M \rangle$, όπου M ένα DFA :

1. Κατασκευάζουμε ένα DFA C που αποδέχεται όλες τις συμβολοσειρές με περιττούς 1.
2. Κατασκευάζουμε ένα DFA D τ.ω. $L(D) = L(M) \cap L(C)$.
3. Ελέγχουμε εάν $L(D) \neq \emptyset$ [χρησιμοποιούμε τον διαγνώστη R της E_{DFA}].
4. Αν ο R αποδέχεται, **αποδέχεται**.

Αλλιώς, **απορρίπτει**.”

Εφόσον όλοι οι αλγόριθμοι σε αυτή τη μηχανή τερματίζουν σε πεπερασμένο χρόνο, η γλώσσα L είναι διαγνώσιμη. □

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Αδρανής κατάσταση ενός PDA P είναι μια κατάσταση στην οποία δεν μεταβαίνει ποτέ το P . Δείξτε ότι η γλώσσα του προβλήματος είναι διαγνώσιμη.

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Αδρανής κατάσταση ενός PDA P είναι μια κατάσταση στην οποία δεν μεταβαίνει ποτέ το P . Δείξτε ότι η γλώσσα του προβλήματος είναι διαγνώσιμη.

Λύση. Έστω $U_{\text{PDA}} = \{\langle P \rangle \mid P \text{ είναι ένα PDA που έχει αδρανείς καταστάσεις}\}$. Θα κατασκευάσουμε μια TM T η οποία να διαγιγνώσκει την U_{PDA} .

Πρώτα, θα ορίσουμε το πρόβλημα $E_{\text{PDA}} = \{\langle P \rangle \mid P \text{ είναι ένα PDA και } L(P) = \emptyset\}$. Τώρα δείχνουμε ότι το E_{PDA} είναι διαγνώσιμο με έναν διαγνώστη D :

$D =$ "Για είσοδο $\langle P \rangle$, όπου P ένα PDA :

1. Μετατρέπουμε το P σε μια ισοδύναμη CFG G .
2. Εκτελούμε τον διαγνώστη R της E_{CFG} .
3. Αν ο R αποδέχεται, **αποδέχεται**.
Αν ο R απορρίπτει, **απορρίπτει**."

Αυτή η γλώσσα είναι διαγνώσιμη επειδή όλα τα βήματα στην κατασκευή της παίρνουν πεπερασμένο χρόνο και η E_{CFG} είναι διαγνώσιμη. ...

Διαγνωσιμότητα

[Άσκηση από βιβλίο M.Sipser] Αδρανής κατάσταση ενός PDA P είναι μια κατάσταση στην οποία δεν μεταβαίνει ποτέ το P . Δείξτε ότι η γλώσσα του προβλήματος είναι διαγνώσιμη.

Λύση. ... Τώρα δείχνουμε ότι το U_{PDA} είναι διαγνώσιμο με έναν διαγνώστη T :

$T =$ "Για είσοδο $\langle P \rangle$, όπου P ένα PDA [$P = (K, \Sigma, \Gamma, \delta, s, F)$]:

1. $\forall q \in K$:

a. Τροποποίησε το P έτσι ώστε $F = \{q\}$.

b. Εκτέλεσε το D στην είσοδο $\langle P \rangle$. Αν το D αποδεχτεί, **αποδέχεται**.

2. **Απορρίπτει** $\langle P \rangle$."

Εφόσον το E_{PDA} είναι διαγνώσιμο, το U_{PDA} είναι διαγνώσιμο. □

Αναγωγή

■ Έστω η γλώσσα

$$EQ_{CFG} = \{ \langle G, H \rangle \mid G, H \text{ είναι CFGs και } L(G) = L(H) \}.$$

Θεώρημα. Η EQ_{CFG} είναι μη-διαγνώσιμη.

Απόδειξη. Η ALL_{CFG} είναι μη-διαγνώσιμη. Έστω ότι η EQ_{CFG} είναι διαγνώσιμη. Άρα υπάρχει διαγνώστης R για την EQ_{CFG} .

Μπορούμε να κατασκευάσουμε έναν διαγνώστη M για την ALL_{CFG} .

$M =$ “Για είσοδο $\langle G \rangle$ όπου G ένα CFG:

1. Δημιουργούμε μια CFG H τ.ω. να αποδέχεται όλες τις συμβολοσειρές.
2. Χρησιμοποιήσουμε τον R για $\langle G, H \rangle$.
3. **Αποδέχεται**, αν R αποδέχεται.
Απορρίπτει, αν R απορρίπτει.”

...

Αναγωγή

$M =$ “Για είσοδο $\langle G \rangle$ όπου G ένα CFG:

1. Δημιουργούμε μια CFG H τ.ω. να αποδέχεται όλες τις συμβολοσειρές.
2. Χρησιμοποιήσουμε τον R για $\langle G, H \rangle$.
3. Αποδέχεται, αν R αποδέχεται.
Απορρίπτει, αν R απορρίπτει.”

Η μηχανή M είναι ένας έγκυρος διαγνώστης για το ALL_{CFG} , καθώς στο 1., μπορούμε εύκολα να επιλέξουμε μια γραμματική χωρίς συμφραζόμενα που αποδέχεται κάθε συμβολοσειρά σε πεπερασμένο χρόνο. Επιπλέον, το EQ_{CFG} είναι διαγνώσιμο, οπότε τα 2. και 3. θα τερματίσουν σε πεπερασμένο χρόνο.

Επομένως, το M είναι διαγνώστης για το ALL_{CFG} , αντίφαση.

Συνεπώς, το EQ_{CFG} είναι μη-διαγνώσιμη.



Αναγωγή

Θεώρημα. Η EQ_{CFG} είναι co-αναγνωρίσιμη. [Συμπληρωματικά αναγνωρίσιμη, Άσκηση βιβλίο M.Sipser]

Απόδειξη. Μπορούμε να σχεδιάσουμε μια μηχανή αναγνώρισης για αυτό.

$M =$ “Για είσοδο $\langle G_1, G_2 \rangle$ όπου G_1 και G_2 είναι CFG:

1. Επαναλάβετε τα παρακάτω για $i = 1, 2, 3, \dots$

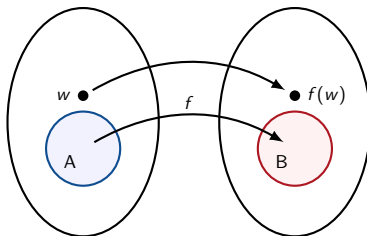
Με τη συμβολοσειρά s_i , αν $\langle G_1, s_i \rangle \in A_{CFG} \neq \langle G_2, s_i \rangle \in A_{CFG}$, **αποδέχεται.**”

Δεδομένου ότι το A_{CFG} είναι διαγνώσιμο και το σύνολο Σ^* είναι αριθμήσιμο, η μηχανή M πάντα τερματίζει και αποδέχεται αν $\langle G_1, G_2 \rangle \notin EQ_{CFG}$. $\square$

Απεικονιστική Αναγωγή

■ Η συνάρτηση $f : \Sigma^* \rightarrow \Sigma^*$ είναι **υπολογίσιμη** αν υπάρχει ΤΜ M , όπου M με είσοδο w τερματίζει έχοντας μόνο $f(w)$ στην ταινία, για κάθε τις συμβολοσειρά w .

■ Η γλώσσα A είναι **απεικονιστικά αναγώγιμη** στη B ($A \leq_m B$), αν υπάρχει υπολογίσιμη συνάρτηση f τ.ω. $w \in A \iff f(w) \in B$.



■ Η συνάρτηση f είναι η **αναγωγή** της A στη B .

Απεικονιστική Αναγωγή

Έστω ότι $A \leq_m B$.

Σχόλια.

■ Η f είναι συνάρτηση, επομένως κάθε συμβολοσειρά αντιστοιχεί σε κάποια συμβολοσειρά. Αλλά κάθε συμβολοσειρά στο B ή $\overline{B}$ δεν χρειάζεται να έχει προεικόνα (pre-image).

■ Το m στη σημειογραφία της απεικονιστικής αναγωγής σημαίνει ‘πολλές-προς-μία’ (many-to-one).

■ Το $A \leq_m B$ διαισθητικά σημαίνει ότι το B είναι τουλάχιστον τόσο δύσκολο όσο το A . Με άλλα λόγια, μια λύση για το B θα έδινε μια λύση για το A .

■ Η απεικονιστική αναγωγή χρησιμοποιείται στην Θεωρία Αποφασισιμότητας και στην Θεωρία Πολυπλοκότητας.

Απεικονιστική Αναγωγή

π.χ., Η γλώσσα A_{TM} ανάγεται με απεικόνιση στη $\bar{E}_{TM}$.

Η υπολογίσιμη συνάρτηση αναγωγής έχει την μορφή $f(\langle M, w \rangle) = \langle M_w \rangle$.

Καθώς, $\langle M, w \rangle \in A_{TM}$ ανν $\langle M_w \rangle \in \bar{E}_{TM}$. [M αποδέχεται $w \iff L(\langle M_w \rangle) \neq \emptyset$.]

$M_w =$ “Για είσοδο x :

1. Αν $x \neq w$ απορρίπτει.
2. Αλλιώς εκτελεί την M για w .
3. Αν η M αποδέχεται, αποδέχεται.”



Απεικονιστική Αναγωγή – Ιδιότητες

Θεώρημα. Αν $A \leq_m B$ και γλώσσα B διαγνώσιμη, τότε και η γλώσσα A διαγνώσιμη.

Απόδειξη. Έστω f μια αναγωγή από της A στη B και ο διαγνώστης R για την B . Κατασκευάζουμε την ΤΜ S , για την A , ώστε εξής:

$S =$ “Για είσοδο w :

1. Υπολόγισε $f(w)$.
2. Προσπέλασε την R με είσοδο $f(w)$ και έλεγξε αν $f(w) \in B$.
3. Αν R τερματίζει τότε επέστρεψε το ίδιο αποτέλεσμα.”

□

Απεικονιστική Αναγωγή – Ιδιότητες

Θεώρημα. Αν $A \leq_m B$ και A είναι μη-διαγνώσιμη, τότε και η B είναι μη-διαγνώσιμη.

Απόδειξη. Αν A μη-διαγνώσιμη και η B διαγνώσιμη, αντιφάσκει με το προηγούμενο θεώρημα. $\square$

Θεώρημα. Αν $A \leq_m B$ και B είναι αναγνωρίσιμη, τότε και η A είναι αναγνωρίσιμη.

Απόδειξη. Έστω TM M_B αναγνωρίζει B και f αναγωγή από το A στο B . Κατασκευάζουμε νέα TM M_A :

$M_A =$ "Για είσοδο w :

1. Υπολόγισε $f(w)$.
2. Εκτέλεσε M_B για $f(w)$ και επέστρεψε το ίδιο αποτέλεσμα."

Απόδειξη ορθότητας: Εφόσον f αναγωγή: $w \in A \iff f(w) \in B$

$w \in A \iff f(w) \in B, M_A$ και M_B αποδέχονται.

$w \notin A \iff f(w) \notin B, M_A$ και M_B απορρίπτουν. $\square$

Απεικονιστική Αναγωγή – Ιδιότητες

Θεώρημα. Αν $A \leq_m B$ και A είναι μη-αναγνωρίσιμη, τότε και η B είναι μη-αναγνωρίσιμη.

Απόδειξη. Αν A μη-αναγνωρίσιμη και η B αναγνωρίσιμη, αντιφάσκει με το προηγούμενο θεώρημα. $\square$

Απεικονιστική Αναγωγή – Ιδιότητες

Θεώρημα. Αν $A \leq_m B$ και A είναι μη-αναγνωρίσιμη, τότε και η B είναι μη-αναγνωρίσιμη.

Απόδειξη. Αν A μη-αναγνωρίσιμη και η B αναγνωρίσιμη, αντιφάσκει με το προηγούμενο θεώρημα. $\square$

Θεώρημα. Αν $A \leq_m B$ και A δεν είναι co-αναγνωρίσιμη, τότε και η B δεν είναι co-αναγνωρίσιμη.

Απόδειξη. Αν A όχι co-αναγνωρίσιμη, τότε $\bar{A}$ όχι αναγνωρίσιμη. Εφόσον $A \leq_m B$, τότε $\bar{A} \leq_m \bar{B}$. Αλλά, $\bar{B}$ όχι αναγνωρίσιμη. Επομένως, η B δεν είναι co-αναγνωρίσιμη. $\square$

Απεικονιστική Αναγωγή – Ιδιότητες

Σχόλια

- Απεικονιστική Αναγωγή: Μετατροπή ερωτήσεων για το A σε ερωτήσεις για το B .
 - Ειδική περίπτωση αναγωγής.
 - Χρήσιμο για την απόδειξη μη-αναγνωρισιμότητας.

- Γενική Αναγωγή: Αναγωγή από A σε B , χρησιμοποιούμε τον επιλυτή του B ώστε να λύσουμε το A . [Το A μπορεί να λυθεί και με άλλους τρόπους, αλλά λύνεται σίγουρα μέσω του B .]
 - Εννοιολογικά ευκολότερη ιδέα.
 - Χρήσιμο για την απόδειξη μη-διαγνωσιμότητας.

- Στην γενική αναγωγή, το A ανάγεται στο $\bar{A}$.

- Μπορεί να μην υπάρχει απεικονιστική αναγωγή από το A στο $\bar{A}$, π.χ., $\overline{A_{TM}} \not\leq_m A_{TM}$.

Αναγωγή

Μερικές οδηγίες

- Για να αποδείξουμε ότι B μη-διαγνώσιμο:
 - Δείχνουμε ότι ένα μη-διαγνώσιμο A ανάγεται στο B . [συχνά χρησιμοποιούμε το A_{TM} , όχι όμως πάντοτε.]
 - Υποθέτουμε ότι υπάρχει TM R που διαγιγνώσκει για το B .
 - Κατασκευάζουμε TM S που διαγιγνώσκει για το A , άτοπο.

- Για να αποδείξουμε ότι B μη-αναγνωρίσιμο:
 - Δείχνουμε ότι ένα T-μη-αναγνωρίσιμο A ανάγεται με απεικόνιση στο B . [συχνά χρησιμοποιούμε για A το $\overline{A_{TM}}$, όχι όμως πάντοτε.]
 - Βρίσκουμε την συνάρτηση απεικόνισης f .

Αναγωγή

■ Υπενθυμίζουμε ότι:

$$A_{TM} = \{\langle M, w \rangle \mid M \text{ είναι TM που αποδέχεται τη συμβολοσειρά } w\}$$

$$HALT_{TM} = \{\langle M, w \rangle \mid M \text{ είναι TM που τερματίζει στη συμβολοσειρά } w\}.$$

■ Στην Διάλεξη 14, αποδείξαμε ότι η $HALT_{TM}$ είναι μη-διαγνώσιμη δείχνοντας ότι η A_{TM} ανάγεται στη $HALT_{TM}$.

■ Για να δείξουμε ότι $A_{TM} \leq_m HALT_{TM}$. Χρειαζόμαστε μια συνάρτηση f με:

Είσοδος: $\langle M, w \rangle$.

Περιγραφή:

$$\langle M, w \rangle \in A_{TM} \iff f(\langle M, w \rangle) = \langle M', w' \rangle \in HALT_{TM}.$$

Έξοδος: $f(\langle M, w \rangle) = \langle M', w' \rangle$.

Αναγωγή

■ Θα δείξουμε ότι $A_{\text{TM}} \leq_m \text{HALT}_{\text{TM}}$

Απόδειξη. Η ΤΜ F υπολογίζει την αναγωγή f .

$F =$ “Για είσοδο $\langle M, w \rangle$:

1. Κατασκευάζουμε την εξής ΤΜ M' :

$M' =$ “Για είσοδο x :

1. Εκτέλεσε την M με είσοδο το x .

2. Αν η M αποδεχθεί, τότε **αποδέξου**.

3. Αν η M απορρίψει, τότε μπες σε βρόγχο.”

2. $\langle M', w \rangle$.”

Απόδειξη ορθότητας: $\langle M, w \rangle \in A_{\text{TM}} \iff \langle M', w \rangle \in \text{HALT}_{\text{TM}}$.

□

Αναγωγή

■ Έστω η γλώσσα $E_{TM} = \{\langle M \rangle \mid M \text{ είναι TM και } L(M) = \emptyset\}$.

Θεώρημα. Η γλώσσα E_{TM} είναι μη-αναγνωρίσιμη.

Απόδειξη. Θα δείξουμε ότι $\overline{A_{TM}} \leq_m E_{TM}$. Θα κατασκευάσουμε μια υπολογίσιμη συνάρτηση f που παίρνει ως είσοδο το $\langle M, w \rangle$ και παράγει ως έξοδο το $\langle M' \rangle$ τ.ω. M δεν αποδέχεται το $w \iff L(M') = \emptyset$.

Είσοδος: $\langle M, w \rangle$

Περιγραφή: Κατασκευάζουμε μια TM M' η οποία με είσοδο x εκτελεί τα εξής (σημειώνεται ότι η M' έχει κωδικοποιημένη την περιγραφή της M και του w στη δική της περιγραφή):

- Αν $x \neq w$, τότε απορρίπτει.
- Αλλιώς, προσομοίωση της M στο w . Αν η M αποδεχθεί/απορρίψει, τότε αποδέχεται/απορρίπτει.

Έξοδος: $\langle M' \rangle$

...

Αναγωγή

■ Έστω η γλώσσα $E_{TM} = \{\langle M \rangle \mid M \text{ είναι TM και } L(M) = \emptyset\}$.

Θεώρημα. Η γλώσσα E_{TM} είναι μη-αναγνωρίσιμη.

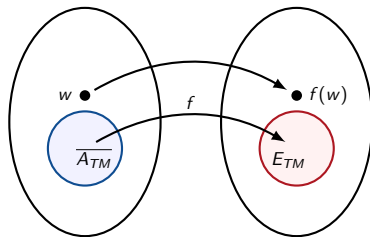
Απόδειξη. (Ορθότητα)

Αν η M δεν αποδέχεται το w , τότε η M' δεν αποδέχεται καμία είσοδο. Άρα, $L(M') = \emptyset$

Αν η M αποδέχεται το w , τότε η M' αποδέχεται μόνο την συμβολοσειρά w . Άρα, $L(M') = \{w\}$

Συνεπώς, M δεν αποδέχεται το $w \iff L(M') = \emptyset$. Άρα, $\overline{A_{TM}} \leq_m E_{TM}$.

Η γλώσσα E_{TM} δεν είναι T-αναγνωρίσιμη. $\square$



Αναγωγή

■ Έστω η γλώσσα $EQ_{TM} = \{\langle M_1, M_2 \rangle \mid M_1, M_2 \text{ είναι TM και } L(M_1) = L(M_2)\}$.

■ Θα δείξουμε ότι $E_{TM} \leq_m EQ_{TM}$.

Απόδειξη. Θα κατασκευάσουμε υπολογίσιμη συνάρτηση f η οποία παίρνει είσοδο $\langle M \rangle$ και παράγει αποτέλεσμα $\langle M_1, M_2 \rangle$ τ.ω. $L(M) = \emptyset \iff L(M_1) = L(M_2)$.

Είσοδος: $\langle M \rangle$

Περιγραφή:

- Θέτει $M_1 := M$.
- Κατασκευάζει TM M_2 τ.ω. να απορρίπει όλες τις εισόδους [$L(M_2) = \emptyset$]

Έξοδος: $\langle M_1, M_2 \rangle$

...

Αναγωγή

■ Θα δείξουμε ότι $E_{\text{TM}} \leq_m EQ_{\text{TM}}$.

Απόδειξη. (Ορθότητα)

$$L(M) = \emptyset \iff L(M_1) = \emptyset \iff L(M_1) = L(M_2)$$

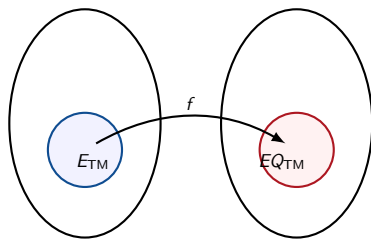
Άρα,

$$L(M) = \emptyset \iff L(M_1) = L(M_2)$$

Δηλαδή,

$$E_{\text{TM}} \leq_m EQ_{\text{TM}}.$$

Η γλώσσα E_{TM} δεν είναι T-αναγνωρίσιμη. $\square$



Αναγωγή

■ Έστω η ακόλουθη διαδικασία (Δ):

```
while  $x \neq 1$  do  
  if  $x$  is odd then  $x \leftarrow 3x + 1$   
  if  $x$  is even then  $x \leftarrow x/2$   
halt
```

π.χ., Ξεκινώντας από το 14, παίρνουμε την ακολουθία 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.

■ Αν η A_{TM} ήταν διαγνώσιμη μέσω μιας ΤΜ H , πως θα χρησιμοποιούσατε την H ώστε να κατασκευάσετε μια ΤΜ η οποία να επιστρέφει τη σωστή απάντηση για το (Δ);

Αναγωγή

■ Έστω C η ΤΜ για το Δ .

■ Εφόσον έχουμε ένα πρόγραμμα που λύνει το πρόβλημα του τερματισμού, θα κατασκευάσουμε μια ΤΜ F η οποία παίρνει έναν αριθμό x , επαναλαμβάνει την Δ , και σταματά μόλις φτάσει στο 1. Μια τέτοια ΤΜ υπάρχει και είναι η ακόλουθη,

$F =$ “Για είσοδο x :

1. Όσο $x \neq 1$:

Αν x άρτιος $x \leftarrow x/2$,

Αν x περιττός $x \leftarrow 3x + 1$.”

Αναγωγή

■ Δημιουργούμε μια νέα ΤΜ B που ξεκινά με έναν δεδομένο x , και καλεί το πρόγραμμα τερματισμού H στο F και x . Αν το H λέει ότι το F δεν τερματίζει στο x , τότε σταματάμε. Αν το H λέει ότι το F τερματίζει στο x , τότε αυξάνουμε το x κατά 1, και επαναλαμβάνουμε τη διαδικασία. Και πάλι, είναι εύκολο να δείξουμε ότι μια τέτοια ΤΜ υπάρχει, και είναι η ακόλουθη

$B =$ “Για είσοδο x :

1. Όσο $H(F, x)$:
 $x \leftarrow x + 1.$ ”

■ Τέλος, καλούμε το H στο C και 1. Αν το H λέει ότι το C με 1 δεν θα τερματίσει, τότε προφανώς η λύση στο $3x + 1$ είναι ότι η σειρά θα καταλήγει πάντα στο 1 για οποιοδήποτε x . (δηλαδή, δεν υπάρχει αντιπαράδειγμα)

Αναγωγή

■ Έστω η ακόλουθη διαδικασία (Δ):

```
while  $x \neq 1$  do  
  if  $x$  is odd then  $x \leftarrow 3x + 1$   
  if  $x$  is even then  $x \leftarrow x/2$   
halt
```

■ Εικασία Collatz: Η (Δ) θα φτάσει στο **1** ξεκινώντας από οποιονδήποτε θετικό ακέραιο x .

■ Παραμένει άλυτη! Μέχρι στιγμής έχουν ελεγχθεί όλοι οι ακέραιοι μέχρι τον 2^{68} [πηγή, Wikipedia]

■ Χρησιμοποιείται στην κρυπτογράφηση σήματος/εικόνας, ανακάλυψη πληροφορίας, watermarking, κτλ.