On the complexity of algorithms

Σεβαστού Νικολέτα

ΑΛΜΑ

2023

Περιεχόμενα

Εισαγωγή

Μια σύντομη ιστορική αναδρομή

Το πρόγραμμα του Hilbert

Η υπολογιστική πολυπλοκότητα

On the complexity of algorithms

Προαπαιτούμενα για να δούμε τα αποτελέσματα

Αποτελέσματα των Hartmanis και Stearns

Μια σύντομη ιστορική αναδρομή

Εισαγωγή

- 1900: International Congress of Mathematicians
- 1928: Hilbert μαζί με τον Ackermann έθεσαν την εξής πρόκληση:

  Υπάρχει αλγόριθμος (ή όπως το ονόμασαν «καθορισμένη μέθοδος») που να λαμβάνει ως είσοδο έναν ισχυρισμό και να απαντά «ναι» ή «όχι» ανάλογα με το αν είναι καθολικά αληθής; («Πρόβλημα απόφασης»)

- 1936: ο Turing ανέπτυξε σε μια δημοσίευσή του την ιδέα των Turing Machines. Ανεξάρτητα ο ένας από τον άλλο, οι Church και Turing απέδειξαν ότι η απάντηση στο «Πρόβλημα απόφασης» είναι «όχι», δεν υπάρχει τέτοιος αλγόριθμος.

Εισαγωγή

Σχήμα: Η/Υ γενιάς του 1963

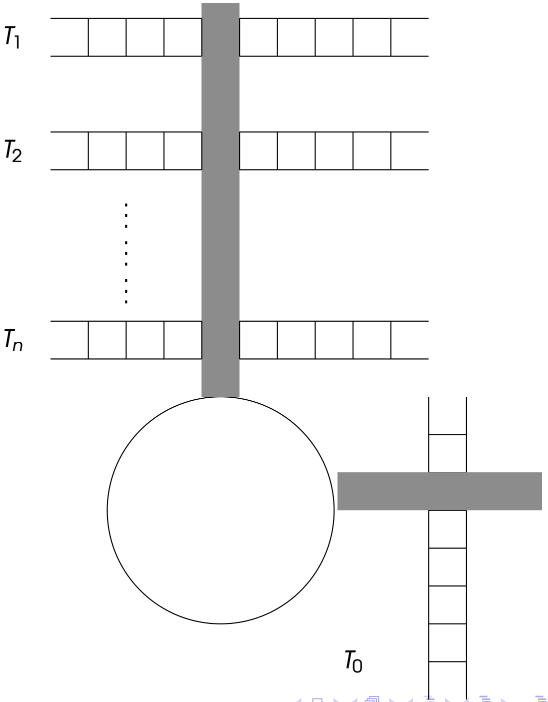
Εισαγωγή

Οι Hartmanis και Stearns στο άρθρο τους ``On the complexity of algorithms'' το 1963 έδωσαν την ιδέα-κλειδί για τη μέτρηση της χρονικής και της χωρικής πολυπλοκότητας.

Πριν μελετήσουμε την έννοια του «υπολογίσιμος» και τα προβλήματα που λύνονται, πρέπει να δούμε πως υπολογίζουμε.

Τί είναι μια μηχανή Turing;

Διαισθητική περιγραφή της λειτουργίας της TM


T_1
T_2
T_n
T_0

Τί είναι μια μηχανή Turing;

Αυστηρός μαθηματικά ορισμός

Τί είναι μια μηχανή Turing;

Ορισμός 1

Μια **μηχανή Turing** (στο εξής ΜΤ ή TM) M με n ταινίες $T_1, .., T_n$ είναι ένα σύνολο πλειάδων $(3n+4)$ στοιχείων. Πιο συγκεκριμένα:

$$(q_i, s_{i_1}, \ldots, s_{i_n}, s_{j_0}, \ldots, s_{j_n}, m_0, m_1, \ldots, m_n, q_j)$$

όπου κάθε στοιχείο παίρνει πεπερασμένες το πλήθος τιμές και για κάθε επιλογή των πρώτων $n+1$ στοιχείων υπάρχει μοναδική πλειάδα στο σύνολο (δηλαδή η ΜΤ είναι ντετερμινιστική).

Τί είναι μια μηχανή Turing;

- έχει μια ταινία T_0 που είναι η ταινία εξόδου
- q_i: η κατάσταση στην οποία βρίσκεται η ΜΤ μια δεδομένη στιγμή
- $\underbrace{S_{i_1}, \ldots, S_{i_n}}_{n}$: τα σύμβολα που διαβάζει στις n ταινίες η M τη δεδομένη στιγμή
- $\underbrace{S_{j_0}, \ldots, S_{j_n}}_{n+1}$: τα σύμβολα που εκτυπώνει στην ταινία T_0 και στις n ταινίες η M, ενώ είναι στην κατάσταση q_i και διαβάζει τα $S_{i_1}, \ldots, S_{i_n}$
- $\underbrace{m_0, m_1, \ldots, m_n}_{n+1} \in \{Left, Right, No\ Move\}$: οι κινήσεις που θα κάνει η M στις $n+1$ ταινίες με τον περιορισμό $m_0 \neq Left$
- q_j: η νέα κατάσταση στην οποία θα μεταβεί η ΜΤ

Τί είναι μια μηχανή Turing;

Η ταινία εξόδου δεν μετριέται στις n ταινίες. Θεωρούμε ότι οι $T_1, T_2, .., T_n$ είναι είτε κενές, είτε έχουν κάποια συμβολοσειρά ως είσοδο, ενώ η T_0 είναι κενή, όταν αρχίζει η ΜΤ την λειτουργία της.

Τί είναι μια χρονική συνάρτηση;

Ορισμός 2 Έστω $T : \mathbb{N}^+ \to \mathbb{N}^+$. Η T είναι **υπολογίσιμη** αν υπάρχει ΜΤ που έχει ως έξοδο $T(n)$ για είσοδο n. Αν επιπλέον η T είναι γνησίως αύξουσα τότε λέμε ότι T είναι μια **χρονική συνάρτηση** (time-function).

Τί είναι μια T-υπολογίσιμη δυαδική ακολουθία;

Ορισμός 3

Έστω $T : \mathbb{N}^+ \to \mathbb{N}^+$ χρονική συνάρτηση. Μια δυαδική ακολουθία α λέγεται ***T*-υπολογίσιμη** ανν υπάρχει TM M τ.ω. ο n-οστός όρος της α να υπολογίζεται σε $T(n)$ το πολύ βήματα.

Τί είναι η κλάση S_T;

Ορισμός 4

Αν μια δυαδική ακολουθία α είναι T-υπολογίσιμη τότε λέμε ότι $a \in S_T$, με S_T να είναι η κλάση όπου περιέχονται όλες οι T-υπολογίσιμες ακολουθίες.

Αναγνωρίσιμο και αποφάνσιμο σύνολο

Ορισμός 5 Λέμε ότι ένα υποσύνολο του $\{0,1\}^*$ είναι **αναγνωρίσιμο**[1] αν υπάρχει μια TM M που να εκτυπώνει όλες τις συμβολοσειρές που ανήκουν σε αυτό (επιτρέπονται και επαναλήψεις). Ισοδύναμα αν υπάρχει ΜΤ που λαμβάνει ως είσοδο μια συμβολοσειρά w και έχει ως έξοδο το 1 αν αυτό ανήκει στο σύνολο. Αν η συμβολοσειρά δεν ανήκει τότε λέμε ότι «κολλάει»/ τρέχει ατέρμονα (συμβολίζουμε $M(w)\uparrow$). Πρακτικά δεν γνωρίζουμε αν ανήκει η συμβολοσειρά, σε αυτή την περίπτωση (ανά πάσα στιγμή θα μπορούσε να σταματήσει).

[1] Λέγεται και αναδρομικά απαριθμήσιμο ή ότι ανήκει στην κλάση RE

Αναγνωρίσιμο και αποφάνσιμο σύνολο

Ορισμός 6 Λέμε ότι ένα υποσύνολο του $\{0, 1\}^*$ είναι **αποφάνσιμο**[2] αν υπάρχει μια ΤΜ M που να εκτυπώνει όλες τις συμβολοσειρές που ανήκουν σε αυτό σύμφωνα με κάποια διάταξη που θα είναι προκαθορισμένη (για να αποφύγουμε τις επαναλήψεις). Ισοδύναμα αν υπάρχει ΜΤ που λαμβάνει ως είσοδο μια συμβολοσειρά w και έχει ως έξοδο το 1 αν αυτό ανήκει στο σύνολο και 0 αν δεν ανήκει. Συμβολίζουμε $M(w)\downarrow_{yes}$ και $M(w)\downarrow_{no}$ αντίστοιχα ή πιο γενικά $M(w)\downarrow$.

[2] Λέγεται και διαγνώσιμο, αποφασίσιμο, αποκρίσιμο, αναδρομικό ή ότι ανήκει στην κλάση REC

Να πως μαθηματικοποιείται η πρόκληση των Hilbert και Ackermann:

Ορισμός 7 Ονομάζουμε **Halting Problem/HP** το σύνολο των ζευγών συμβολοσειρών (κωδικοποιήση TM M, συμβολοσειρά w) για τα οποία ισχύει ότι $M(w)\downarrow$.

Θεώρημα 8 *Το HP είναι αναδρομικά απαριθμήσιμο (recursively enumerable), αλλά όχι αποφάνσιμο.*

Χωρίς απόδειξη.

Θεώρημα 9 *Το σύνολο όλων των T-υπολογίσιμων δυαδικών ακολουθιών είναι αναδρομικά απαριθμήσιμο (recursively enumerable)*

Χωρίς απόδειξη. Θα αναφέρουμε μόνο ότι από την απόδειξη προκύπτει πως το σύνολό τους είναι αριθμήσιμο, ενώ το σύνολο των δυαδικών ακολουθιών είναι υπεραριθμήσιμο. Προκύπτει από αυτό ότι υπάρχουν δυαδικές ακολουθίες που <u>δεν</u> ανήκουν στην S_T. Μέσα σε αυτές που δεν ανήκουν μπορώ να βρω μια που να υπολογίζεται από TM.

Θεώρημα 10

Αν δύο δυαδικές ακολουθίες a, b διαφέρουν μόνο σε πεπερασμένα το πλήθος στοιχεία τότε για χρονικής συνάρτηση T έχουμε ότι

$$a \in S_T \text{ iff } b \in S_T$$

Χωρίς απόδειξη

Θεώρημα 11 *Αν T είναι μια χρονική συνάρτηση, τότε δεν υπάρχει TM (δηλ. διαδικασία-αλγόριθμος) που να αποφασίζει αν μια τυχαία δυαδική ακολουθία α ανήκει στην S_T (πρακτικά αν μπορώ να φτιάξω τα πρώτα n στοιχεία της σε χρόνο $T(n)$).*

Απόδειξη. Με εις άτοπο απαγωγή. □

Απόδειξη

Έστω ότι υπάρχει A TM που αποφασίζει αν $\alpha \in S_T$ ή αν $\alpha \notin S_T$. Έστωσαν ακόμη M τυχαία τυχαία TM, είσοδος w και M_1 MT που εκτυπώνει μια ακολουθία $\boxed{\beta \notin S_T}$. Η M_1 υπάρχει λόγω του θεωρήματος 9. Δημιουργώ μια TM M_2.

Απόδειξη

$$(*)\ \alpha \in S_T \text{ ανν } M \text{ δεν σταματά με είσοδο } w$$

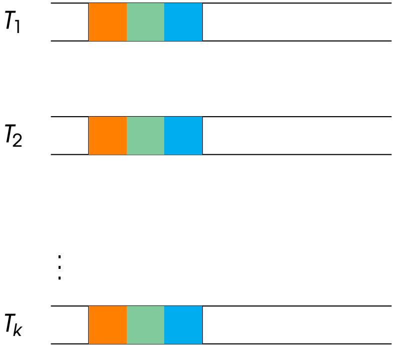
Γιατί;

Πόρισμα 1 *Δεν υπάρχει TM που να αποφασίζει αν $S_U = S_T$, ούτε όμως και αν $S_U \subseteq S_T$ για τυχούσες χρονικές συναρτήσεις U, T.*

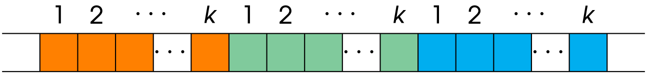
Χωρίς απόδειξη.

Θεώρημα 12 *Αν μια δυαδική ακολουθία α είναι T-υπολογίσιμη από πολυταινιακή ΜΤ M, τότε α είναι T^2-υπολογίσιμη από μονοταινιακή ΜΤ M_1.*

Απόδειξη



Σχήμα: k ταινίες ΤΜ της M



Σχήμα: ταινία της M_1

ΤΕΛΟΣ