On the complexity of algorithms

Διδάσκων: Διδάσκοντες: Ζάχος Ε., Λιανέας Θ., Φωτάκης Δ.

Ονοματεπώνυμο: Σεβαστού Νικολέτα

ΑΛΜΑ

2023-2024

Περιεχόμενα

1 Εισαγωγή

Κάποια από τα προβλήματα που συνάντησαν οι επιστήμονες τον 20ο αιώνα έχουν να κάνουν με τη δυσκολία των προβλημάτων.

α′ Είναι όλα τα προβλήματα το ίδιο δύσκολα;

β′ Είναι εφικτό όλα τα προβλήματα να λυθούν σε χρόνο της αρεσκείας μας;

Ένα πρόβλημα ίσως υπολογίζεται σε πεπερασμένο χρόνο, αλλά κανείς δεν θα ήθελε αυτό το πεπερασμένο να είναι πολύ "μεγάλο". Οπότε μέσα στην κλάση των προβλημάτων που λύνονται, υπάρχουν οι τάξεις των "καλών" επιλύσιμων προβλημάτων.

1.1 Μια σύντομη ιστορική αναδρομή

1.1.1 Το πρόγραμμα του Hilbert

Το 1900 στο International Congress of Mathematicians (Διεθνές Συμπόσιο Μαθηματικών) ο Hilbert παρουσίασε 10 προβλήματα, από μια λίστα 23, που θεωρούσε ότι θα απασχολούσαν τη μαθηματική κοινότητα τον 20ο αιώνα. Αρκετά παραμένουν άλυτα και άλλα έχει αποδειχθεί ότι δεν μπορούν να λυθούν.

Το 1928 ο 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;

Αυτή η πρόκληση είναι γνωστή ως «Πρόβλημα απόφασης», «Decidability Problem» ή «Entscheidungsproblem» (Γερμανικά).

Το 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.

Το Entscheidungsproblem σχετίζεται με το 10ο πρόβλημα στη λίστα των 23 προβλημάτων του Hilbert.

1.1.2 Η υπολογιστική πολυπλοκότητα

Εικόνα 1: Η/Υ γενιάς του 1963

Μετά από την εισήγηση του θεωρητικού μοντέλου των μηχανών Turing και την ανάπτυξη των Η/Υ τις δεκαετίες του 1940 και του 1950, έγινε αντιληπτό ότι η μνήμη και ο χρόνος είναι προβλήματα που δεν λαμβάνει υπ΄ όψιν του το θεωρητικό μοντέλο.

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. Έτσι γεννήθηκε η υπολογιστική πολυπλοκότητα. Από τότε πολλές κλάσεις αποφάνσιμων προβλημάτων (θα δούμε τον ορισμό) ανακαλύφθηκαν, πολλά ερωτήματα τέθηκαν και λύθηκαν και κάποια έμειναν άλυτα.

Εδώ θα παραλείψουμε πολλά από αυτά που εν συντομία αναφέραμε για να δούμε μόνο λίγα αποτελέσματα που παρουσίασαν οι Hartmanis και Stearns.

2 On the complexity of algorithms

2.1 Τί είναι μια μηχανή Turing;

Πριν μελετήσουμε την έννοια του «υπολογίσιμος» και τα προβλήματα που λύνονται, πρέπει να δούμε πως υπολογίζουμε, δηλαδή το μοντέλο υπολογισμού που θα χρησιμοποιήσουμε. Και αυτό θα το κάνουμε γιατί υπάρχουν πολλά μοντέλα υπολογισμού, άλλα πιο ισχυρά από τα άλλα και άλλα ισοδύναμα με τα άλλα. Κάποια από αυτά που δεν θα δούμε είναι ο λ-λογισμός, η συνδυαστική λογική και τα συστήματα Post. Οι μηχανές Turing θυμίζουν πολύ τους σημερινούς υπολογιστές, αλλά δημιουργήθηκε το 1936 για να δώσουν λύση στο Entscheidungsproblem και είναι πρόδρομος των σημερινών Η/Υ.

Ορισμός 2.1. *Μια **μηχανή Turing** (στο εξής ΜΤ ή ΤΜ) Μ με n ταινίες* $T_1, .., T_n$ *είναι ένα σύνολο πλειάδων* $(3n+4)$ *στοιχείων. Πιο συγκεκριμένα:*

$$(q_i, S_{i_1}, ..., S_{i_n}, S_{j_0}, ..., S_{j_n}, m_0, m_1, ..., m_n, q_j)$$

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). Επιπλέον:*

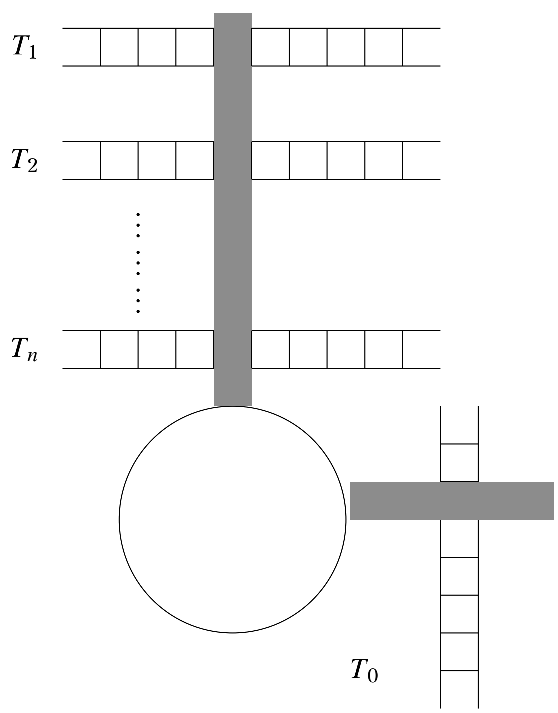
- *έχει μια ταινία* T_0 *που είναι η ταινία εξόδου*
- q_i*: η κατάσταση στην οποία βρίσκεται η ΜΤ μια δεδομένη στιγμή*
- $\underbrace{S_{i_1}, ..., S_{i_n}}_{n}$*: τα σύμβολα που διαβάζει στις n ταινίες η Μ τη δεδομένη στιγμή*
- $\underbrace{S_{j_0}, ..., S_{j_n}}_{n+1}$*: τα σύμβολα που εκτυπώνει στην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

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.*

Περιγραφή της λειτουργίας της ΤΜ

Η ΤΜ έχει έναν μηχανισμό καταστάσεων (πεπερασμένων το πλήθος) και n ταινίες άπειρες και προς τα δύο άκρα, χωρισμένες σε κελιά. Με τη χρήση μιας κεφαλής σε κάθε ταινία (δηλαδή κάθε ταινία έχει τη δική της κεφαλή) διαβάζει τα σύμβολα που είναι γραμμένα στα κελιά των ταινιών, αλλά μόνο ένα από κάθε ταινία τη φορά. Η κεφαλή κάθε ταινίας μπορεί να μετακινηθεί σύμφωνα με τη συνάρτηση καταστάσεων κατά ένα κελί το πολύ, δεξιά ή αριστερά και ανεξάρτητα από τις κινήσεις των άλλων κεφαλών. Η μετάβαση από μία κατάσταση σε μία επόμενη γίνεται με μοναδικό τρόπο (ντετερμινιστική TM). Η κεφαλή γράφει (αφού σβήσει το προϋπάρχον) στο κελί κάθε ταινίας που διάβασε ένα σύμβολο πριν η TM μεταβεί στη νέα κατάσταση· νέο ή το προϋπάρχον. Στην ταινία εξόδου οι κινήσεις γίνονται μόνο προς τα δεξιά και κανένα σύμβολο που γράφτηκε δεν μπορεί να σβηστεί.

Ο χρόνος που κάνει η TM για να εκτελέσει ένα βήμα υπολογισμού (να γράψει ένα σύμβολο, να μετακινηθεί κατά ένα κελί, να διαβάσει ένα σύμβολο) θα είναι για εμάς μονάδα μέτρησης του χρόνου για όλες τις διαδικασίες παρακάτω και θα θεωρούμε ότι είναι ίδιος για όλες τις ενέργειες της κεφαλής. Στην πολυταινιακή οι κινήσεις στις n ταινίες γίνονται ταυτόχρονα από τις n κεφαλές.



Εικόνα 2: n-ταινιακή TM

2.2 Τί είναι μια χρονική συνάρτηση;

Ορισμός 2.2. *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).*

2.3 Τί είναι μια T-υπολογίσιμη δυαδική ακολουθία;

Ορισμός 2.3. *Έστω $T : \mathbb{N}^+ \to \mathbb{N}^+$ χρονική συνάρτηση. Μια δυαδική ακολουθία α λέγεται T-**υπολογίσιμη** ανν υπάρχει ΤΜ M τ.ω. ο n-οστός όρος της α να υπολογίζεται σε $T(n)$ το πολύ βήματα.*

2.4 Τί είναι η κλάση S_T;

Ορισμός 2.4. *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.*

2.5 Αναγνωρίσιμο και αποφάνσιμο σύνολο

Χάριν απλότητας θεωρούμε σύνολα συμβολοσειρών στο $\{0,1\}^*$, όπου το σύνολο $\{0,1\}^*$ λέγεται **Kleene star του** $\{0,1\}$ και είναι το σύνολο με όλες τις συμβολοσειρές που περιέχουν 0 και 1 και είναι οποιουδήποτε πεπερασμένου μήκους. Οποιοδήποτε άλλο σύνολο αντί του αλφαβήτου $\{0,1\}$ μπορεί να μετατραπεί στο $\{0,1\}$.

Ορισμός 2.5. *Λέμε ότι ένα υποσύνολο του $\{0,1\}^*$ είναι* ***αναγνωρίσιμο***[1] *αν υπάρχει μια ΤΜ 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).*

Ορισμός 2.6. *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*

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

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

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 $M(w) \downarrow$.

Χωρίς να μπούμε σε λεπτομέρειες, θα πούμε ότι υπάρχει διαδικασία που μπορεί να κωδικοποιήσει με "μοναδικό" τρόπο μια TM (όπως την ορίσαμε ως σύνολο και όχι ως λειτουργία) στο $\{0, 1\}^*$ και να δώσουμε αυτή την συμβολοσειρά ως είσοδο σε μια άλλη TM. Μπορούμε ακόμα να αποφασίσουμε αν μια συμβολοσειρά είναι κωδικοποιήση TM ή όχι.

Πρέπει ακόμα να πούμε ότι υπάρχει μια TM που προσομοιώνει όλες τις άλλες λαμβάνοντας με κάποιον τρόπο την κωδικοποίησή τους.

2.6 Halting Problem/HP

Ορισμός 2.7. *Ονομάζουμε **Halting Problem/HP** το σύνολο των ζευγών συμβολοσειρών (κωδικοποιήση TM M, συμβολοσειρά w) για τα οποία ισχύει ότι $M(w) \downarrow$.*

Θεώρημα 2.8. *Το HP είναι αναδρομικά απαριθμήσιμο (recursively enumerable), αλλά όχι αποφάνσιμο.*

Χωρίς απόδειξη.

Θεώρημα 2.9. *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 δεν ανήκουν στην S_T. Μέσα σε αυτές που δεν ανήκουν μπορώ να βρω μια που να υπολογίζεται από TM.

2.7 Αποτελέσματα των Hartmanis και Stearns

Θεώρημα 2.10. *Αν δύο δυαδικές ακολουθίες a, b διαφέρουν μόνο σε πεπερασμένα το πλήθος στοιχεία τότε για χρονικής συνάρτηση T έχουμε ότι*

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

Χωρίς απόδειξη

Θεώρημα 2.11. *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. Έστω ότι υπάρχει A ΤΜ που αποφασίζει αν $\alpha \in S_T$ ή αν $\alpha \notin S_T$. Έστωσαν ακόμη M τυχαία τυχαία ΤΜ, είσοδος w και M_1 ΜΤ που εκτυπώνει μια ακολουθία $\boxed{\beta \notin S_T}$. Η M_1 υπάρχει λόγω του θεωρήματος 2.9. Δημιουργώ μια ΤΜ M_2 ως εξής:

- για όλα τα βήματα που κάνει η M με είσοδο w πριν σταματήσει η M_2 εκτυπώνει 0.
- αν M σταματά μετά από κ βήματα τότε η M_2 εκτυπώνει τα $\kappa, \kappa+1, ...$ στοιχεία της β που θα τύπωνε η M_1.

Άρα οι ακολουθίες που τυπώνει η M_2 είναι της μορφής:

$$0, .., 0, \beta_\nu, \beta_{\nu+1}, ...$$

για κάποιο φυσικό ν.

Αν α είναι η ακολουθία που τυπώνει η M_2 για την τυχαία ΤΜ M και την τυχαία είσοδο w που διαλέξαμε, λόγω του θεωρήματος 2.10 θα έχουμε ότι:

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

Γιατί;

($\Rightarrow$) αν $\alpha \in S_T$ και M σταματά, έστω σε ν βήματα, τότε η M_2 θα τυπώσει $0, .., 0, \beta_\nu, \beta_{\nu+1}, ...$ Η α όμως διαφέρει από τη β μόνο σε $\nu - 1$ στοιχεία. Άρα από θεώρ. 2.10 $\beta \in S_T$ άτοπο.

($\Leftarrow$) αν M δεν σταματά, τότε η M_2 τυπώνει συνεχώς μηδενικά και έτσι η ακολουθία α (θυμηθείτε ότι θέλουμε να τυπώνει σε $T(n)$ βήματα το πολύ το n-οστό ψηφίο και αυτό γίνεται εκ κατασκευής της M_2) είναι στην S_T.

Αν M λοιπόν σταματά για είσοδο w τότε από την $(*)$ έχω ότι $A(\alpha)\downarrow_{no}$, αφού $\alpha \notin S_T$. Αν M όμως δεν σταματά για είσοδο w τότε από την $(*)$ έχω ότι $A(\alpha)\downarrow_{yes}$, αφού $\alpha \in S_T$.

Αυτό σημαίνει όμως ότι για τυχαία ΤΜ και είσοδο σε αυτή μπορώ να αποφασίσω αν θα τερματίσει δημιουργώντας την ΤΜ Δ:

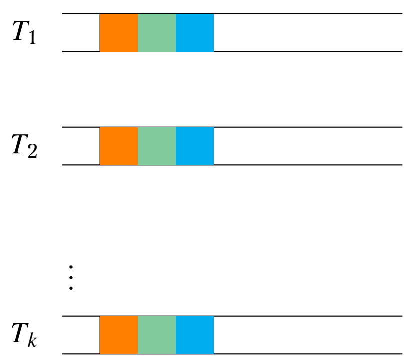
- Για είσοδο την κωδικοποίηση μιας ΤΜ M και μιας συμβολοσειράς w ηΔ προσομοιώνει την M_2 που αντιστοιχεί στην στην $M(w)$.
- Για την ακολουθία που έχει έξοδο η M_2, προσομοιώνει την A με αυτή την είσοδο
- Αν η A βγάλει 0/όχι, η Δ απαντά 1/ναι.
- Αν η A βγάλει 1/ναι, η Δ απαντά 0/όχι.

Δηλαδή το Halting Problem είναι αποφάνσιμο. ΑΤΟΠΟ από θεώρ. 2.8. Συνεπώς δεν υπάρχει TM που να αποφασίζει αν μια τυχαία δυαδική ακολουθία α ανήκει στην S_T. □

Πόρισμα 2.12. *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.*

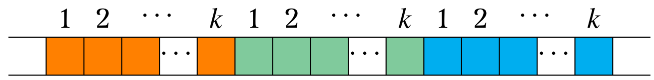
Χωρίς απόδειξη.

Θεώρημα 2.13. *Αν μια δυαδική ακολουθία α είναι T-υπολογίσιμη από πολυταινιακή MT M, τότε α είναι T^2-υπολογίσιμη από μονοταινιακή MT M_1.*



Εικόνα 3: k ταινίες TM της M

Απόδειξη. Έστω ότι η M έχει k ταινίες και το σύνολο των συμβόλων που εμφανίζονται σε αυτές είναι Σ. Στην ταινία της M_1 αποθηκεύουμε τα σύμβολα όπως φαίνεται στην εικόνα 2.7. Για να ξέρουμε πού είναι η κεφαλή κάθε ταινίας από αυτές της M προσθέτουμε ένα σύνολο συμβόλων στο Σ. Το νέο σύνολο συμβόλων θα είναι $\Sigma' = \Sigma \cup \underline{\Sigma} = \Sigma \cup \{\underline{a} : a \in \Sigma\}$, δηλαδή προσθέτουμε κάποια σύμβολα ίδια με του Σ, αλλά με κάποια επιπλέον ένδειξη για να χρησιμοποιηθούν αντί για τις k κεφαλές. Επίσης θα προσθέσουμε ένα σύμβολο που θα οριοθετεί μεταξύ τους τα περιεχόμενα των k ταινιών στην ταινία της M. Έστω το #. Η συνάρτηση μεταβάσεων θα αλλάξει για να αντικατοπτρίζει τις αλλαγές που κάναμε, αλλά θα έχει πάλι πεπερασμένο πλήθος καταστάσεων. Δεν μας απασχολεί η αλλαγή της, αφού δεν επηρεάζει την πολυπλοκότητα, για αυτό και παραπέμπουμε στο [3] (σελ 30) για την περιγραφή της αλλαγής. Πριν από κάθε μετατόπιση συμβόλων, η TM θα πρέπει να μετακινεί και όλα τα άλλα που χρειάζονται για να κάνει χώρο.



Εικόνα 4: ταινία της M_1

Πώς προσομοιώνει η M_1 ένα βήμα της M;

- Η M_1 σαρώνει μία φορά από αριστερά προς τα δεξιά την ταινία της για να βρει τα προς ανάγνωση σύμβολα και να τα "αποθηκεύσει".
- Ξανα-σαρώνει από δεξιά προς αριστερά για να ενημερώσει τα κελιά και να μετακινήσει τους δείκτες (τα σύμβολα που δείχνουν πού είναι οι κεφαλές)
- Αν η M μετακινούσε δεξιά κάποιο σύμβολο, τότε η M_1 για να δημιουργήσει χώρο, μετακινεί όσα σύμβολα έπονται αυτού μία θέση δεξιά, και μετά αυτό. Αυτό θα χρειαστεί να το κάνει και για τις αριστερές μετατοπίσεις.

Πλήθος βημάτων που κάνει η M_1

Η M υπολογίζει την συμβολοσειρά που θέλω εκ κατασκευής σε $T(n)$ βήματα το πολύ. Άρα σε κάθε ταινία η συμβολοσειρά δεν μπορεί να ξεπερνά σε μήκος το $T(n)$. Για κάθε βήμα της M από τα $T(n)$, η M_1:

- περνά το πολύ 2 φορές από τα γεμάτα κελιά της ταινίας της για ανάγνωση, αποθήκευση και ενημέρωση των «κεφαλών»
- για κάθε μετατόπιση συμβόλου περνάει το πολύ 4 φορές όλα τα γεμάτα κελιά της ταινίας της (για να τα μετακινήσει) και 8 φορές από κενό κουτί στα πλευρικά της συμβολοσειράς, άρα έχω ότι για κάθε μετατόπιση η κεφαλή μετακινεί το πολύ $4T(n)+8$ σύμβολα. Σε ένα βήμα της M όμως γίνονται το πολύ k μετατοπίσεις συμβόλων, άρα σύνολο $4k(T(n)+2)$ το πολύ βήματα για κάθε μετατόπιση συμβόλου της M.

Η M κάνει το πολύ $T(n)$ βήματα μέχρι να τερματίσει. Άρα η πολυπλοκότητα (αγνοώντας τις σταθερές και το k που είναι ανεξάρτητο του n) είναι $O(T^2(n))$

$\square$

Αναφορές

[1] *Theory of Computation (Διαφάνειες)*, Lor. De Stefani, Brown University

[2] *Εισαγωγή στη θεωρία υπολογισμού*, Michael Sipser, ΠΕΚ 2η έκδοση

[3] *Computational Complexity*, Papadimitriou C., Addison-Wesley

[4] *Θεωρία Αναδρομής*, Ζώρος Δ., (Σημειώσεις) Μαθηματικό ΕΚΠΑ

[5] *A Short History of Computational Complexity*, L. Fortnow, S. Homer

[6] *Stanford Encyclopedia of Philosophy*, Λήμμα Hilbert's Program, ανάκτηση: 13/10/2023

[7] *Dictionary of Cognitive Science, University of Alberta*, Λήμμα Decidability Problem, ανάκτηση: 13/10/2023

[8] *Wikipedia*, Λήμμα Hilbert's Problems, ανάκτηση: 13/10/2023

[9] *Wikipedia*, Λήμμα Entscheidungsproblem, ανάκτηση: 13/10/2023