Mηχανές Turing

Turing Machines (TM)

- Απλός ιδεατός υπολογιστής (υπολογιστικό μοντέλο).
- Πεπερασμένη συσκευή με δυνητικά άπειρη ταινία.
- Η ταινία υποδιαιρείται σε κύτταρα που περιέχουν 0 ή 1.
- Σε κάθε χρονική στιγμή η κεφαλή της ΤΜ βρίσκεται στο «τρέχον» κύπαρο.
- Βασικές λειτουργίες μιας TM:
 - Διαβάζει το τρέχον κύπαρο.
 - Γράφει 1 ή 0 στο τρέχον κύπαρο.
 - Κάνει τρέχον το αμέσως αριστερότερο ή δεξιότερο κύτταρο.

Παράδειγμα

$$M = (K, \Sigma, \delta, s, \{h\})$$

$$K = \{q_0, q_1, h\}$$

$$\Sigma = \{1, \sqcup, \rhd\}$$

$$s=q_0$$

Συνάρτηση μετάβασης:

Υπολογισμός:

$$\begin{array}{c} (q_1,\rhd \, \underline{\sqcup} \, 1111) & \vdash_M (q_0,\rhd \, \underline{\sqcup} \, \underline{1}111) \\ \vdash_M (q_1,\rhd \, \underline{\sqcup} \, \underline{\sqcup} \, 111) \\ \vdash_M (q_0,\rhd \, \underline{\sqcup} \, \underline{\sqcup} \, \underline{1}11) \\ \vdash_M (q_1,\rhd \, \underline{\sqcup} \, \underline{$$

Βασικές ΤΜ

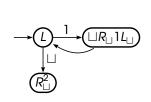
- ▶ Μηχανές εγγραφής συμβόλων: π.χ. αν 1 ∈ Σ τότε M_1 : 1.
- Μηχανές μετακίνησης κεφαλής: M_←: L, M_→: R
- Χτίσιμο σύνθετων μηχανών από απλούστερες:



- Mηχανές R_□, R_□, L_□, L_□
- $R^{\frown \sqcup} \stackrel{1}{\rightarrow} L1$

Παραδείγματα ΤΜ

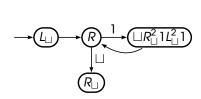
Μηχανή δεξιάς μετατόπισης της εισόδου ($\sqcup w \underline{\sqcup} \to \sqcup \sqcup w \underline{\sqcup}$):

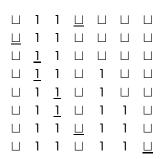




Παραδείγματα ΤΜ

Μηχανή αντιγραφής της εισόδου: ($\sqcup w \underline{\sqcup} \to \sqcup w \sqcup w \underline{\sqcup}$)





Υπολογισμοί με ΤΜ

Συμβάσεις

- ▶ Αρχική συνολική κατάσταση: $(s, \rhd \underline{\sqcup}w)$.
- Η είσοδος w δεν περιέχει κενά.
- ightharpoonup Δύο καταστάσεις τερματισμού: $H = \{y, n\}$.
- y : συνολική κατάσταση αποδοχής.
- n : συνολική κατάσταση απόρριψης.
- Η μηχανή δέχεται την είσοδο w αν παράγει μια συνολική κατάσταση αποδοχής.
- Η μηχανή απορρίπτει την είσοδο w αν παράγει μια συνολική κατάσταση απόρριψης.

ΤΜ σαν αναγνωριστές γλώσσας

Έστω $\Sigma_0\subseteq \Sigma-\{\sqcup,\rhd\}$. Λέμε ότι μια TM M αποφασίζει μια γλώσσα $L\subseteq \Sigma_0^*$ ανν $\forall w\in \Sigma_0^*$:

- ▶ η M δέχεται την w, αν w ∈ L,
- ▶ η M απορρίπτε την w, αν $w \notin L$.

Μια γλώσσα ονομάζεται <mark>αναδρομική</mark> αν υπάρχει μια TM που την αποφασίζει.

<u>ΠΡΟΣΟΧΗ:</u> Μια ΤΜ αποφασίζει μια γλώσσα αν <u>ΠΑΝΤΑ ΤΕΡΜΑΤΙΖΕΙ</u> είτε σε μια συνολική κατάσταση αποδοχής, είτε σε μια συνολική κατάσταση απόρριψης.

ΤΜ σαν υπολογιστές συναρτήσεων

Έστω συνάρτηση $f: \Sigma_0^* \to \Sigma_0^*$ ($w \to f(w)$). Λέμε ότι μια TM M υπολογίζει τη συνάρτηση f αν για κάθε $w \in \Sigma_0^*$ η μηχανή τερματίζει με ταινία $\triangleright \sqcup f(w)$.

Μια συνάρτηση f λέγεται <mark>αναδρομική</mark> αν υπάρχει ΤΜ που υπολογίζει την f. Γράφουμε τότε M(w)=f(w).

Αναδρομικά απαριθμίσιμες γλώσσες

Λέμε ότι μια TM M ημιαποφασίζει μια γλώσσα $L\subseteq \Sigma_0^*$ αν για κάθε $w\in \Sigma_0^*$ ισχύει ότι $w\in L$ αν και μόνο άν η M τερματίζει με είσοδο w.

Μια γλώσσα λέγεται αναδρομικά απαριθμίσιμη αν και μόνο αν υπάρχει ΤΜ που την ημιαποφασίζει.

<u>ΠΡΟΣΟΧΗ:</u> Αν μια γλώσσα ημιαποφασίζεται από μια TM τότε για τα στοιχεία της γλώσσας η TM πάντα τερματίζει, όμως για τα στοιχεία του Σ_0^* η TM <u>ΔΕΝ ΤΕΡΜΑΤΙΖΕΙ ΠΟΤΕ</u>.

Παράδειγμα: η μηχανή $R^{\frown \overline{a}}$ ημιαποφασίζει τη γλώσσα

 $\mathit{L} = \{w \mid w \in \{\mathit{a},\mathit{b}\}^*$ каї w періе́хеї тоυλа́хіσтоν е́va $\mathit{a}\}$

Αναδρομικά απαριθμίσιμες γλώσσες

Παρατηρήσεις

- Οι ΤΜ που ημιαποφαζίζουν γλώσσες δεν είναι αναγνωριστές γλωσσών.
- Αν η είσοδος δεν ανήκει στη γλώσσα η ΤΜ δεν θα τερματίσει ποτέ κι έτσι δεν ξέρουμε ποτέ αν έχουμε περιμένει αρκετά για μια απάντηση.
- Αντίθετα, ένα πεπερασμένο αυτόματο τερματίζει ΠΑΝΤΑ.

Θεωρήματα:

- Αν μια γλώσσα είναι αναδρομική τότε είναι αναδρομικά απαριθμίσιμη (το αντίστροφο δεν ισχύει).
- Αν μια L είναι αναδρομική τότε η L̄ είναι αναδρομική.

Παραλλαγές ΤΜ

Παραλλαγές των TM με την ίδια υπολογιστική δυνατότητα, όχι όμως και αποδοτικότητα είναι:

- πολλές ταινίες, μνήμη πλέγματος, μνήμη περισσότερων διαστάσεων,
- μεγαλύτερο Σ,
- πολλές παράλληλες κεφαλές,
- μη ντετερμινιστικές μεταβάσεις,

Καθολική ΤΜ

Κάθε ΤΜ μπορεί να κωδικοποιηθεί από ένα φυσικό αριθμό κάτω από ένα κατάλληλο σχήμα κωδικοποίησης. Όμοια κωδικοποιείται και η είσοδος οποιασδήποτε μηχανής.

Μια καθολική TM U δέχεται σαν είσοδο τις κωδικοποιήσεις μιας οποιασδήποτε TM M και της εισόδου της w. Στη συνέχεια η U «τρέχει» την M με είσοδο w. Η U τερματίζει αν και μόνο άν η M τερματίζει.

Οι φυσικοί αριθμοί είναι ένα μετρήσιμο σύνολο. Άρα υπάρχουν μετρήσιμα πολλές κωδικοποιήσεις ΤΜ. Οι γλώσσες όμως είναι γενικά μη μετρήσιμα σύνολα (γιατί;). Άρα υπάρχουν γλώσσες που δεν μπορούν να αποφασιστούν από ΤΜ.

Θέση των Church - Turing

Όλα τα γνωστά και άγνωστα ντετερμινιστικά υπολογιστικά μοντέλα είναι μεταξύ τους ισοδύναμα.

Το παράνω είναι θέση ή αλλιώς αίτημα, π.χ. το αίτημα των παραλλήλων ευθειών στην Ευκλείδια γεωμετρία. Ένα αίτημα γίνεται δεκτό χωρίς απόδειξη.

Είναι μάλλον απίθανο να προταθεί στο μέλλον ένα υπολογιστικό μοντέλο ισχυρότερο από τις ΤΜ.

Υπολογιστικά μοντέλα

Δεν χρειάζεται να καθορίσουμε ένα συγκεκριμένο υπολογιστικό μοντέλο για τη λύση κάποιου προβλήματος.

Αν ένα πρόβλημα λύνεται από κάποιο υπολογιστικό μοντέλο τότε θα λύνεται και από οποιοδήποτε άλλο με το πολύ πολυωνυμική απώλεια χρόνου.

Μερικά ντετερμινιστικά υπολογιστικά μοντέλα:

- προγράμματα Pascal, JAVA, . . . με ή χωρίς αναδρομή,
- προγράμματα WHILE (μόνη δομή ελέγχου το WHILE),
- προγράμματα GOTO και IF,
- assembler-like RAM, URM (universal register machine,
- single register machine (ένας καταχωρητής),
- ΤΜ με πρόσβαση σε ένα μόνο κύπαρο της τανίας σε κάθε βήμα.

Μηχανιστική απαρίθμιση προγραμμάτων

- Αν $\Sigma = \{a_1, a_2, \dots, a_m\}$ είναι το αλφάβητο μιας γλώσσας προγραμματισμού, κάθε πρόγραμμα ανήκει στο Σ^* .
- ightharpoonup Όμως $\Sigma^*=\cup_{n=0}^\infty \Sigma_n$ και κάθε Σ_n (σύνολο συμβολοσειρών του Σ με μήκος n) είναι πεπερασμένο.
- Τα στοιχεία κάθε συνόλου μπορούν να διαταχθούν αλφαβητικά οπότε μπορούμε να θεωρήσουμε την ακόλουθη απαρίθμηση για το Σ*:

```
\begin{array}{ll} \Sigma_0 : & \{\epsilon\} \\ \Sigma_1 : & \{a_1, a_2, \dots, a_m\} \\ \Sigma_2 : & \{a_1 a_1, a_1 a_2, \dots, a_1 a_m, \dots, a_m a_m\} \\ \vdots \end{array}
```

- Η παραπάνω απαρίθμιση μπορεί να γίνει με πρόγραμμα.
- Με κατάλληλη χρήση compiler για τον έλεγχο ορθότητας μπορούμε να κατασκευάσουμε μηχανιστικά μια απαρίθμιση των συντακτικά ορθών η προγραμμάτων

Το πρόβλημα τερματισμού

Halting Problem (HP)

- Ο μεταγλωπιστής ελέγχει για τη συντακτική ορθότητα των προγραμμάτων.
- Τι γίνεται όμως με τα λάθη χρόνου εκτέλεσης;
- Υπάρχει πρόγραμμα που μπορεί να ελέγχει αν ένα συντακτικά ορθό πρόγραμμα θα σταματήσει κάποτε ή αν θα τρέχει για πάντα;
- Δυστυχώς τέτοιο πρόγραμμα δεν υπάρχει!
- Το HP είναι μή επιλύσιμο!

Το ΗΡ είναι μη επιλύσιμο

- Έστω ότι π₀, π₁, . . . είναι μια μηχανιστική απαρίθμιση όλων των προγραμμάτων μιας γλώσσας προγραμματισμού.
- Υποθέτουμε ότι το HP είναι επιλύσιμο.
- Μπορούμε δηλαδή να αποφανθούμε αν το πρόγραμμα π_i με είσοδο j σταματάει.
- Κατασκευάζουμε ένα πρόγραμμα π που ελέγχει αν το πρόγραμμα π_n με είσοδο n ($\pi_n(n)$) σταματάει ή όχι.
- ▶ Το πρόγραμμα π , ανάλογα με τον προηγούμενο έλεγχο, σταματάει αν το $\pi_n(n)$ δεν σταματάει, και αντιστρόφως:

```
read(n); if \pi_n(n) terminates then loop_forever else halt
```

- lacktriangle Το π είναι πρόγραμμα της γλώσσας συνεπώς είναι κάποιο π_i .
- ▶ Το $\pi_i(i)$ σταματάει αν και μόνο αν το $\pi(i)$ σταματάει και αυτό συμβαίνει αν και μόνο αν το $\pi_i(i)$ δεν σταματάει. Αντίφαση.
- 'Αρα το HP είναι μη επιλύσιμο!

Παρατηρήσεις

- Μπορούμε να κατασκευάσουμε μηχανιστικά μια άπειρη λίστα όλων των προγραμμάτων με την αντίστοιχη είσοδο για την οποία σταματούν.
- Επιλύουμε έτσι το HP;
- Φυσικά όχι! Αν το $\pi_k(n)$ δεν έχει εμφανιστεί στη λίστα, δεν ξέρουμε αν θα προστεθεί αργότερα ή αν δε θα εμφανισθεί ποτέ!
- Το HP είναι αναδρομικά απαριθμήσιμο

Πολλά άλλα προβλήματα είναι μη επιλύσιμα.

Αποκρίσιμα και καταγράψιμα σύνολα

Ένα σύνολο S λέγεται αποκρίσιμο ή υπολογίσιμο ή επιλύσιμο ή αναδρομικό (decidable, computable, solvable, recursive) ανν υπάρχει αλγόριθμος που σταματάει ή μια υπολογιστική μηχανή που δίνει έξοδο «ναι» για κάθε είσοδο $a \in S$ και έξοδο «όχι» για κάθε είσοδο $a \notin S$.

Ένα σύνολο S λέγεται καταγράψιμο ή αναδρομικά απαριθμήσιμο (listable, effectively generatable, recursively enumerable) ανν υπάρχει γεννήτρια διαδικασία ή μηχανή που καταγράφει όλα τα στοιχεία του S. Στην, πιθανώς άπειρη, λίστα εξόδου επιτρέπονται οι επαναλήψεις και δεν υπάρχει περιορισμός για την διάταξη των στοιχείων.

Μερικές απλές ιδιότητες

- 1. Av to S eíval αποκρίσιμο τότε και το \overline{S} eíval αποκρίσιμο.
- 2. Αν το S είναι αποκρίσιμο τότε το S είναι και καταγράψιμο.
- 3. Av to S kai \overline{S} eívai kataypá ψ iµa tóte to S eívai anokpí σ iµo.
- 4. Αν το S είναι καταγράψιμο με γνησίως αύξουσα διάταξη τότε το S είναι αποκρίσιμο.

Υποδείξεις:

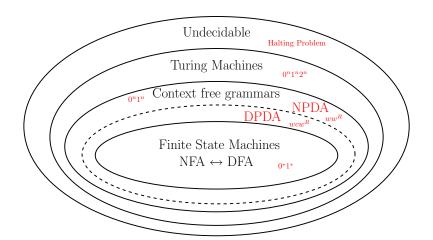
- 1. Στο πρόγραμμα που αποκρίνεται για το S αντέστρεψε το «ναι» και το «όχι» πριν από την έξοδο.
- 2. Τρέξε το πρόγραμμα που αποκρίνεται για το S διαδοχικά για όλους τους φυσικούς αριθμούς.
- Τρέξε βήμα-βήμα παράλληλα τα προγράμματα που καταγράφουν τα S και S μέχρι η είσοδος να εμφανιστεί σε κάποια λίστα εξόδου.
- Τρέξε το πρόγραμμα που καταγράφει το S μέχρι η είσοδος να εμφανιστεί ή ξεπεραστεί στη λίστα εξόδου.

Θεώρημα Rice

Οποιαδήποτε μη τετριμένη ιδιότητα των προγραμμάτων είναι ένα μη επιλύσιμο πρόβλημα!

- Ένα πρόγραμμα τερματίζει με μια δεδομένη είσοδο;
- Ένα πρόγραμμα χωρίς είσοδο τερματίζει;
- Για ένα πρόγραμμα υπάρχει κάποια είσοδος για την οποία το πρόγραμμα τερματίζει;
- Ένα πρόγραμμα τερματίζει για κάθε πιθανή είσοδο;
- Δύο διαφορετικά προγράμματα τερματίζουν με τις ίδιες εισόδους;
- **...**

Το σύμπαν της υπολογισιμότητας



Θεωρία Πολυπλοκότητας

- Στη Θεωρία Υπολογισμού, μας ενδιαφέρει μόνον αν ένα πρόβλημα είναι υπολογίσιμο ή όχι.
- Αν ένα πρόβλημα είναι υπολογίσιμο, τότε είναι αδιάφορο τι ποσότητα αγαθών πρέπει να διατεθεί για να λυθεί το πρόβλημα.
- Στη Θεωρία Πολυπλοκότητας θεωρούμε μόνο υπολογίσιμα προβμήματα και προσπαθούμε να δούμε αν λύνονται κάτω από περιορισμούς.
- Οι υπολογιστικοί πόροι που συνήθως θεωρούνται περιορισμένοι είναι ο χρόνος υπολογισμού και ο επιπλέον χώρος μνήμης για ενδιάμεσα αποτελέσματα.
- Αυτοί οι περιορισμοί, καθώς και άλλα χαρακτηριστικά των υπολογισμών, ορίζουν κλάσεις πολυπλοκότητας.

Βασικοί ορισμοί

- ΤΙΜΕ(t(n)) ανήκουν τα προβλήματα που μπορούν να επιλυθούν από ντετερμινιστική ΤΜ σε χρόνο t(n).
- NTIME(t(n)) ανήκουν τα προβλήματα που μπορούν να επιλυθούν από μη ντετερμινιστική TM σε χρόνο t(n).
- NSPACE(s(n)) ανήκουν τα προβλήματα που μπορούν να επιλυθούν από μη ντετερμινιστική TM με χρήση επιπλέον χώρου s(n).

Ορισμοί κλάσεων πολυπλοκότητας

```
\mathbf{P} = \bigcup_{i>1} \mathrm{TIME}(n^i)
           NP = \bigcup_{i>1} NTIME(n^i)
    PSPACE = \bigcup_{i>1} SPACE(n^i)
 NPSPACE = \bigcup_{i>1} NSPACE(n^i)
             L = SPACE(\log n)
           NL = NSPACE(\log n)
         \text{EXP} = \bigcup_{i>1} \text{TIME}(2^{n^i})
EXPSPACE = \bigcup_{i>1} DSPACE(2^{n'})
```

Βασικές ιδιότητες

- Κάθε ντετερμινιστική ΤΜ μπορεί να θεωρηθεί ως μη ντετερμινιστική με μια μόνο επιλογή σε κάθε βήμα:
 - ▶ TIME(f(n)) ⊆ NTIME(f(n))
 - ▶ SPACE(f(n)) \subseteq NSPACE(f(n))
- Σε χρόνο f(n) δεν μπορεί να εξεταστεί χώρος (αριθμός θέσεων στην ταινία της TM) παραπάνω από f(n):
 - ▶ TIME(f(n)) ⊆ SPACE(f(n))
 - ▶ NTIME(f(n)) \subseteq SPACE(f(n))
- Υπάρχει η εξής ιεραρχία:

$$L\subseteq NL\subseteq P\subseteq NP\subseteq PSPACE=NPSPACE$$

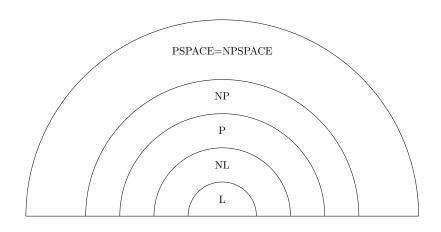
Ανοικτά προβλήματα

$$L\supseteq NL\supseteq P\supseteq NP\supseteq PSPACE$$

Έπαθλο 1.000.000\$ από το Clay Mathematics Institute:

$$P \stackrel{?}{=} NP$$

Το σύμπαν των κλάσεων πολυπλοκότητας



Αναγωγές

Το πρόβλημα «τι θα φάει μια μπλέ αγελάδα;» έχει τη λύση «φαγητό για μπλέ αγελάδες». Προκύπτει τώρα το πρόβλημα «τι θα φάει μια ροζ αγελάδα;». Μια λύση αυτού του προβλήματος είναι «κλείνουμε τη μύτη της ροζ αγελάδας, περιμένουμε να γίνει μπλέ και στη συνέχεια την ταίζουμε με φαγητό για μπλέ αγελάδες».

Μια αναγωγή συνδέει μεταξύ τους προβλήματα με υπολογιστικά «εύκολο» τρόπο. Εύκολες συναρτήσεις και προβλήματα είναι αυτά που υπολογίζονται σε πολυωνυμικό χρόνο.

FP είναι το σύνολο των συναρτήσεων που υπολογίζεται από ντετερμινιστική TM σε πολυωνυμικό χρόνο.

Aναγωγή \leq_m^P (κατά Karp): Το πρόβλημα A ανάγεται στο πρόβλημα B:

$$A \leq_m^P B: \exists f \in FP: (x \in A \Leftrightarrow f(x) \in B), \forall x \in A$$

Δύσκολα και πλήρη προβλήματα

Λέμε ότι μια κλάση γλωσσών C είναι κλειστή ως προς μια αναγωγή \leq αν $A \leq B$ και $B \in C \Rightarrow A \in C$

Κλάσεις πολυπλοκότητας κλειστές ως προς την αναγωγή κατά Karp (\leq_m^p) είναι μεταξύ άλλων οι P, PSPACE, EXP, EXPSPACE.

Λέμε ότι το πρόβλημα A είναι C-δύσκολο (C-hard) ως προς την αναγωγή \leq , αν $\forall B \in C$: $B \leq A$. Η έννοια της δυσκολίας δίνει ένα κάτω όριο για την πολυπλοκότητα ενός προβλήματος : «το πρόβλημα A είναι τουλάχιστο τόσο δύσκολο όσο οποιοδήποτε πρόβλημα μιας C».

Λέμε ότι το πρόβλημα A είναι C-πλήρες (C-complete) ως προς την αναγωγή \leq , αν A είναι C-hard ως προς \leq και $A \in C$.

Πλήρη προβλήματα μέσα στο σύμπαν της πολυπλοκότητας

