(1) Γιατί ο αλγ 2 είναι βέλτιστος;
(2) Γιατί δεν δημιουργούνται κύκλοι αρνητ. μήκους;

(2) Έστω s-t συντομ. μονοπ. (ως προς κόστος)
Αν είχε αρνητικό κόστος
⋮

Erickson

Όχι στις εξετάσεις πως λύνεται αλλά μετασχηματισμοί

Ποιόν αλγόριθμο θα χρησιμοποιήσω; (για τα μονοπ)
Johnson

Πέμπτη Υπολ. Πολυπλ. - Παγουρτζής
Πε 14/12/2023

Παγουρτζής

Μηχανές Turing & υπολογισιμότητα

Hilbert: αυτοματοποίηση μαθηματικών

Διοφαντικές: πολυωνυμικής μορφής εξισώσεις με ακέραιους συντελεστές (έχει ακέραιες ρίζες?)

* Δεν υπάρχει αλγόριθμος για όλες

Gödel Μαθηματικά όχι πλήρη: συστήματα αποδείξεων για μαθηματικές αλήθειες ⇝ δεν μπορούν να αποδείξουν ούτε τις μαθηματικές αλήθειες, πόσο μάλλον άλλα μεταφυσικά ερωτήματα

Turing: υπολογιστικό κομμάτι: διαδικασία για απόδειξη αυτών των αληθειών οι TM
↓
Τι μπορούμε τελικά να υπολογίσουμε;

για τους Η/Υ
Θεώρ. Gödel: τα μαθηματικά δεν αυτοματοποιούνται

+ Robinson, Davis κά

Matijasevic (1970) ⇝ όχι αλγόρ. για διοφ. εξισώσεις

→ ίσως σε άπειρους πολλά χρόνια

* Πρόβλημα Διακριτού λογαρίθμου → λύνεται (δεν ξέρω αν είναι NP-compl)

* Πρόβλ. που δεν ξέρουμε αν λύνεται (αν ανήκει στο REC) ↳ που ίσως λύνεται, ίσως όχι αλλά δεν ξέρουμε ακόμη

εικασία

Collatz: ^{n}σειρά $f(x) = \begin{cases} (3x+1)/2, & x: \text{odd} \\ x/2 & x: \text{even} \end{cases}$

Ξεκινώ από $x^{\text{τυχόν}}$ & υπολογίζω $\underbrace{f^i(x)}_{\text{σύνθεση}}$ $i \in \mathbb{N}^+$

Η εικασία λέει ότι πάντα υπάρχει ($\forall x \in \mathbb{N}$) i μετά από το οποίο τα f^j φθίνουν (πάντα φτάνω σε δύναμη του 2 π.χ)

Είτε κάνει ατέρμονο loop
Είτε (ως τώρα πειραματικά δεν έχουν βρει αντιπαράδειγμα) για όλους τερματίζει στο 1

Μαθηματικά: χωρίς αλγόριθμο σε πόσα βήματα θα τερματίσει (αν αποδειχθεί ότι η εικασία ισχύει → αλγόριθμος: "Επίστρεψε ναι")
Επιστ. Η/Υ: αλγόριθμος που να το βρίσκει, χωρίς να υπολογίζει τα f^i διαδοχικά δηλ.
(αν η απάντηση μαθηματικά είναι ότι δεν ισχύει ⇒ αλγόριθμος για συγκεκριμένες κατηγορίες φυσικών)
∃? αλγόριθμος που για είσοδο $x \in \mathbb{N}$ ~~που~~ να απαντά αν η διαδικασία Collatz τερματίζει ή όχι (& τα 2)

Προβλήματα
- → απόφασης (ΝΑΙ/ΟΧΙ)
- → απάντηση για κάποια είσοδο (άπειρες το πλήθος εισόδους συνήθως)
- → απάντηση για πεπερασμένο σύνολο εισόδων αλλά μεγάλο πλήθος ⇝ λιγότερο ενδιαφέρον

Προβλ. Βελτιστ.

fo: κόστος, κέρδος κλπ

Παραδείγματα

Knapsack, ↓ μεγαλύτερη αξία

TSP ↓ κύκλος Hamilton βέλτιστου κόστους

Προβλ. απόφασης

Υπάρχει κύκλος Hamilton Απόφ;

Πρόβλ. εύρεσης

Βρες κύκλο Hamilton

- Λύνω πρόβλημα βελτιστοποίησης ⇒ (εύκολο) λύνω πρόβλ. απόφ. (παίρνω λύση κ ελέγχω αν ικανοποιεί τη συνθήκη του προβλ. απόφ)
- Λύνω πρόβλ. απόφ ⇒ (δύσκολο) λύνω πρόβλ. βελτιστ.

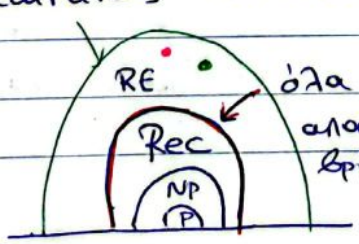
Μπορώ να προσέγγισω της αντικειμενικής συν/σης κ χρειάζομαι (κάτι δύσκολο) να έχω διαδικασία που να βρίσκει το στιγμιότυπο για τη βέλτιστη τιμή της αντικειμ. συν/σης

Μπορώ να περιορίσω τη μελέτη μου στα προβλ. απόφασης γιατί εσωκλείουν όλη την ουσία των ερωτημάτων μας. Επίσης έχουν κωδικοποίηση ως μιας γλώσσα.

Ντετερμινιστικές TM

Συνολική κατάσταση ή διαμόρφωση (ή στιγμιότυπο)

Recursively Enumerable (το 10ο πρόβλ. Hilbert ανήκει εδώ), Halting Problem



όλα τα προβλήματα που μας απασχολούν σε μάθημα αλγορίθμων βρίσκονται μέσα σε αυτό (ίσως πολύ κακού χρόνου) dovetailing

Κόλπο: για να μην κολλάει αν θέλω να δοκιμάσω σε μηχανή που ↑ όλες τις δυνατές εισόδους.
1 βήμα της x_1, (1 βήμα x_2, 2 βήματα x_1)
$x_1 . x_2 . . . . . .$

x_1

x_2

(3 βήμ. x_1, 2 βημ. x_2, 1 βήμα x_3)
κοκ...

- μοντέλο Post ⇝ παραλλαγή MT
- prewriting συστήματα Markov
- γεν. γραμματικές

έως διαφ 19

από L στην L'

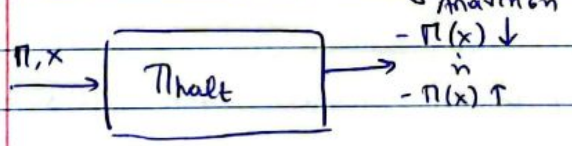
SOS Αναγωγές ← συν/ση f: τ.ω. $x \mapsto f(x)$ με τρόπο που $x \in L \Leftrightarrow f(x) \in L'$ (έχει 1 κατεύθυνση. f: όχι αναγκαία αντιστρέψιμη)
Θεωρία Υπολογισιμότητας
Θεωρία Πολυπλοκότητας logspace, time

μηχανές που δεν αποδέχονται τίποτα

$\langle M,x \rangle \in L_{Halt} \Leftrightarrow \langle M' \rangle \in L_{empty}$

Δε 18/12/2023

Θα θέλαμε (για το HP)



Έστω ότι υπάρχει. Μπορώ να απαριθμήσω όλα τα προγράμματα/TM: $\Pi_0, \Pi_1, \dots$ και όλες τις δυνατές εισόδους $x_0, x_1, \dots$
Φτιάχνω πίνακα που μου λέει αν $\Pi_i(x_j)$ τερματίζει ~~σε~~ στο (i,j) στοιχείο

- Αν η είσοδος δεν είναι σωστή το ελέγχω
- Αν μου δώσουν ένα πρόγρ. μπορώ να βρω μηχανιστικά αν είναι το Π_i

Τα αποτελέσματα του Π_{halt}

	x_0	x_1	x_2	$\dots$
Π_0	✓	—	✓	
Π_1	—	✓	—	
$\vdots$	—	—	—	$\ddots$

$\forall i$ μπορώ να ελέγξω το $\Pi_i(x_i)$ με το Π_{halt} αν υπάρχει το Π_{halt} (δηλ. κοιτάζω τη διαγώνιο του πίνακα)

Αυτο-αναφορά

Θέλω να φτιάξω κάτι που ταιριάζει με όλα αυτά αλλά λειτουργεί "ανάποδα"

Υπάρχει πρόγραμμα: $\Pi_D(x_i) = \begin{cases} \uparrow \ (\to \text{infinite loop}) & \text{αν } \Pi_i(x_i)\downarrow \ (\to \text{τερματίζει}) \\ \downarrow & \text{αν } \Pi_i(x_i)\uparrow \end{cases}$

Διαφορετικά από όλη τη διαγώνιο. Είναι καλά ορισμένο.

$\Downarrow$

Π_D: είναι κάποιο Π_j της απαρίθμησης

αν $\Pi_j(x_j)\downarrow \Rightarrow \Pi_D(x_j)\uparrow$ (Π_D " Π_j)

αν $\Pi_j(x_j)\uparrow \Rightarrow \Pi_D(x_j)\downarrow$ (Π_D " Π_j)

} άτοπο $\Rightarrow \nexists\, \Pi_{halt}$

Το $L_1 = \{\langle M \rangle : M(\varepsilon)\downarrow\}$

$L_2 = \{\langle M \rangle : M(17)\downarrow \text{ και}\}$

} είναι επίσης μη-επιλύσιμα

* όχι ιδιότητα όλων γλωσσών

Θεώρημα Rice: οποιαδήποτε μη-τετριμμένη* η ιδιότητα των γλωσσών που αναγνωρίζονται από μηχανές turing είναι μη-υπολογίσιμη

π.χ.
* όλες οι έξοδοι τελειώνουν στο 3 / είναι περιττός
→ TM, λ-λογ, συνδ. λογική, RAM

Υπολογιστική πολυπλοκότητα (κλασικά μοντέλα) → όχι κβαντικά

Discr. Knapsack ⇝ ψευδοπολυωνυμικό ως προς είσοδο → εκθετικός χρόνος

- Γενικά → πολυωνυμικό ως προς αναπαράσταση εισόδου

έχει σχέση ⊊ αυτό

$DTIME[t(n)] \subsetneq DTIME[\omega(t(n))]$

Fine Grained Complexity

$DTIME(n^{2-\varepsilon}) \subsetneq DTIME(n^2) \subsetneq DTIME(n^{2+\varepsilon})$

ανεξάρτητο εισόδου

$P = \bigcup_{k \geq 0} DTIME(n^k)$ $(k \in \mathbb{N})$

$EXP = \bigcup_{k \geq 0} DTIME(2^{n^k})$

$P \subsetneq EXP$

Primality :

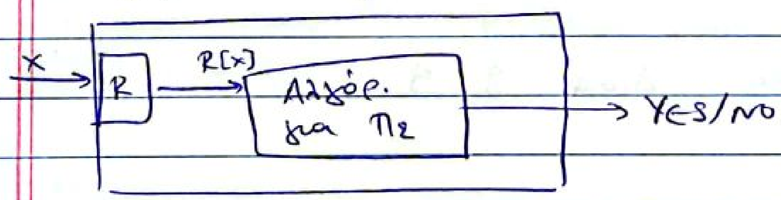
Πολυωνυμική αναγωγή

many-one polynomial reduction

$x \in L(\Pi_1) \Leftrightarrow R(x) \in L(\Pi_2)$

SOS

Αλγόριθμος για Π_1



Αλλά η αναγωγή δεν είναι αναστρέψιμη συν/ση (ίσως ∃ x ≠ y με R(x) = R(y))

Από αντιθετοαντίστροφο αν $\Pi_1 \Rightarrow \Pi_2$
σύνολο σύνολο

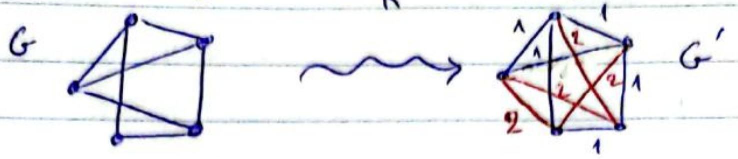
- $\Pi_2 \in P \rightarrow \Pi_1 \in P$ (min cut, max flow)

ταίριασμα σε διμερή γραφ → max flow

HC

HAMILTON ~~PATH~~ CYCLE σε TSP

G $\rightsquigarrow_{R}$ (G', n)



∃ HC ⟺ ∃ TSP με κόστος ≤ n

$HC \leq_p TSP(D)$ (D = Decision)

Γνωρίζουμε ότι είναι NP-πλήρες → TSP(D) είναι NP-πλήρες

Δεν έχω πολ. χρόνου για HC ⇒ TSP

δεν έχω πολ. χρόνου για TSP

Η αναγωγή πρέπει να είναι ευκολότερη (υπολογιστικά) από τα δυσκολότερα προβλήματα της ευκολότερης κλάσης για να είναι επιχείρημα για την κατάρρευση των κλάσεων. (έχει σχέση με κλειστότητα κλάσεων)

Αν ήταν εκθετικού χρόνου θα πήγαινα σίγουρα από P στο NP

Για την P → θέλουμε λογαριθμικό χώρο

Βλ. Διαφ. Β — P, NP κλειστές ως προς πολυων. αναγ.

Βλ. παραδείγματα Διαφ 9-11

2ο σετ γραπτών

(1) Θυμίζει πίνακες συναρ. προγρ

Ίσως να υπάρχει άπληστος (θέλει απόδειξη)

(2)

(3) Βλ. φυλλ. όχι short. path → βγάζω μέγιστη

2 Dijkstra

$$\min_{(u,v)\in E}\{\underbrace{d(s,u)}_{\text{1 Dij}} + 0 + \underbrace{d(v,t)}_{\text{1 Dij}}\}$$

② ∀ u θέλει 1 ταμπέλα — στο Dij θέλω k ταμπέλες
τώρα (έχω μηδεν. 0/1/…/k ακμ.)
Dij → με τις k ταμπέλες — επόμ. βήμα μηδεν. ακμή
→ δεν μηδενίζω ακμή

Ισοδύναμο k+1 αντίγραφα
Ανάμεσα στα αντίγραφα ακμή {u,v} ⟺ {u,v} ∈ E(G)
βάρους 0

ψευδοπολυωνυμικό
④ (β) έχει πολλές λύσεις όπως με 3α
με πόση βενζίνη φτάνουμε σε μια κορ.

⑤ (α) γενίκευση του matching
(β) εξήγηση κριτηρίου τερματ. (είναι βέλτιστο γιατί…
(γ) ελάχ. VC / max Ind. Set
στο G συγκρούονται αν θέλουν το ίδιο
κάστρο (στο διμερές γράφ)

⑥ αναγωγή σε min cost flow → χρειάζεται αναί-ρεση
(γιατί δεν με μέγιστο επικαλ. διάστ.)
↳ SOS
⇓ γι' αυτό δεν δουλεύει Dyn. Prog.

!! αναγωγή με πολυων. μέγεθος γραφ.
(όχι ψευδοπολυων.)

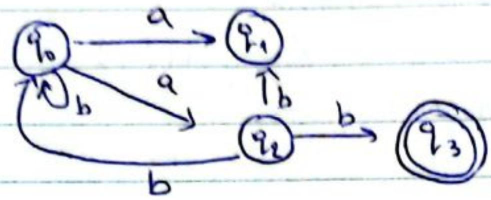
Προθεσμία 28/12 Τρίτη
2η Προγρ Σοκολ. → όχι greedy (Dyn Pr) → $O(n^2)$
↳ μετά τις γιορτές — θέλουμε $O(n\cdot k)$
↓ μικρή αλλαγή κώδικα

Πε 21/12/2023

$\Pi_1 \le_p \Pi_2$

Ham. Path $\le_p$ TSP (D)

Υπενθύμιση NFA : χάνονται τα διαβασμένα



Στις NDTM όμως μπορώ να ξαναδιαβάσω

Μπορώ να σκέφτομαι ως ισοδύναμα το να κάνει ταυτόχρονα βήμα κ' επιγραφή συμβόλου με το να τα κάνει χωριστά

NP : κλάση υπολογιστικών προβλημάτων ώστε ο χρόνος υπολογισμού είναι το πολύ πολυωνυμικός

↙ κατάσταση

Διαμόρφωση $\langle q_0, \underline{a}\, b \rangle$ το q_0 διαβάζει το a

↑ θέση κεφαλής υποδεικνύεται με μπάρα

$\langle q_1, a\underline{b} \rangle$ το q_1 διαβάζει το b

Άλλως συμβολισμός (ε, q_0, ab)

↓ διαβάζει το a (κ' το γράφω πριν από σύμβολο που διαβάζει)

↙ επόμενη κατάσταση (μετακινήθηκε)

$(\varepsilon, q_0, ab) \vdash (a, q_1, b)$

Για υπολογισιμότητα Όχι πολυπλοκότητα

Είναι ισοδύναμο να έχω δέντρο υπολογισμού με [πολλά παιδιά/υποδέντρα σε κάθε κόσμο] με το [2 παιδιά / κόμβο]

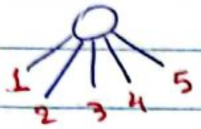
Γιατί;

-Έστω ότι έχω $(q_i, w_1 \underline{\sigma} \overline{w_2})$ σ_1 ω'

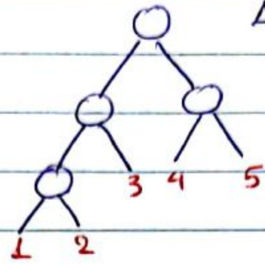
$\swarrow$ $\searrow$

$(q_j, w_1 \underline{\sigma'} w_2)$ $(q_k, w_1 \sigma \underline{\sigma_2} w')$ άλλαξε το σ_2

Αν έχω 5 κλάδους σε ένα κόμβο κάνω το εξής:



~~>



Δυαδικό (με αλλαγή στις καταστάσεις)
Αυξάνει το ύψος του δέντρου

Πόσο αυξάνει; κατά λογαριθμικό παράγοντα

η αύξηση εξαρτάται από το μέγεθος της εισόδου ή το πλήθος των συμβόλων;

Η συν/ση μετάβασης επηρεάζεται μόνο από το σύμβολο της εισόδου. Αυξάνουν μόνο οι επιλογές που έχω για καταστάσεις.

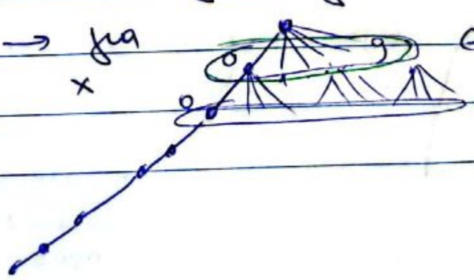
N(x) λήγει αν $(q_0, \underline{x_1} x_2 \dots x_n) \vdash^* (yes, \dots)$

* Θεωρητικά δεν με νοιάζει αν κολλούν τα κλαδιά που θα απέρριπταν αν έχω κλαδί που αποδέχεται

Αν είχα διοφαντική $3xy^2z^5 + 17x^3y^{15}z - 123xy^{71} = 0$

DTM → ∃ ακέραια ρίζα στο $[-10^6, 10^6]$?
έχω $8 \cdot 10^{18}$ βήματα (3 μεταβλητές $2 \cdot 10^6$ επιλογές για κάθε 1)

NDTM → για x



επιλογές μονάδων
επιλογές δεκάδων
⋮
έως εκατομμυριάδα

1.000.000

8 βήματα για x
↓
σύνολο 21 για όλες τις μεταβλ.

Εδώ το $[-10^6, 10^6]$ είναι είσοδος

Προσοχή! Δεν πρέπει να εξαρτάται από είσοδο το πλήθος των κλάσεων σε κάθε βήμα γιατί τότε θα ήταν όλα $O(1)$. Πρέπει να τα βάλω σε έναν "αλγόριθμο"

Εδώ είχα γραμμικό "αλγόρ" ως προς μέγεθος εισόδου (ύψος του δέντρου γραμμικό)

* Το μόνο που έχουμε στα χέρια μας για προσομοίωση NDTM με DTM είναι μια εκθετικού χρόνου διαδικασία

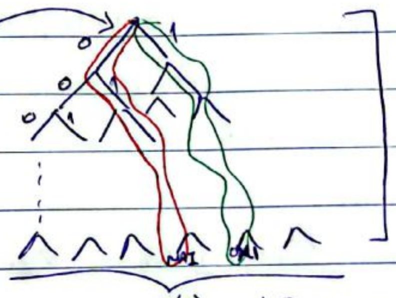
— Έγινε αλλαγή στο 5γ στη 2η γραπτή

— 2η Προγραμμ. μετά τις γιορτές

→ δεν χρησιμοποιεί ο ορισμός με το u NDTM $p(x)$

Πιστοποιητικό u: πολυωνυμικού μεγέθους άρα έχω ένα δέντρο

το u: δείχνει το μονοπάτι



ναι ⇒ είναι λύση

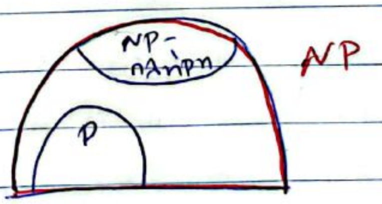
όχι ⇒ δεν είναι λύση

$2^{p(n)}$ όλες οι δυνατές λύσεις με πολυωνυμικό πλήθος bits

διαφ. 11 $L=\{x\in\Sigma^*: \exists y\in\Sigma^*, (x,y)\in R\}$

$x\notin L \Leftrightarrow \forall y\in\Sigma^* \ (x,y)\notin R$

μόνο πολυωνυμικού μήκους δηλ. στην πραγματικότητα έχω $y\in\Sigma^{p(|x|)}$



~~Θεώ.~~ Ladner
Αν $P\neq NP$ ⇒ υπάρχουν ενδιάμεσα
→ διακριτός λογάριθμος
→ ισομορφ. γράφων
→ πρόβλ. πρώτων/σύνθετος
Εκεί η απόφαση → πολυωνυμ.
εύρεση παραγόντων

Factoring (D)

Input: n, k

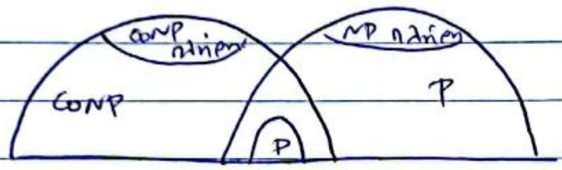
Question: $\exists\ r < k$ τ.ω. $r > 1,\ r \mid n$?

(προβλ. ισοδύναμο με παραγοντοποίηση)

όμως δεν ξέρουμε αν είναι ενδιάμεσο, στο P, ή ... NP-πλήρες

Εικάζεται ότι δεν είναι NP-πλήρες, ούτε στο P (είναι όμως στο NP)

Έχουμε υποεκθετικό αλγόριθμο $2^{(\log n)^{1/3} \dots}$



Έστω $\Pi_1, \Pi_2 \in NP$, $\Pi_1 \leq_p \Pi_2$

1 $\Pi_1 \in P \Rightarrow \Pi_2 \in P$ ΛΑΘΟΣ

REACHABILITY ⟶ πιο ΔΥΣΚΟΛΟ από P

(G, s, t) ναι ⇝ $M(w)$ που τερματίζει πάντα

όχι ⇝ $M(w)\uparrow$

many-one

* Μπορεί να έχω απεικόνιση των $x \in \Pi_1$ σε πολύ λιγότερα στιγμιότυπα του Π_2. Αλλά θέλω να διαχωρίζει σωστά προβλήματα

2 $\Pi_2 \in P \Rightarrow \Pi_1 \in P$ ΣΩΣΤΟ

3 Π_2 όχι NP-πλήρες $\Rightarrow \Pi_1$ όχι NP-πλήρες ΣΩΣΤΟ

Αν προς άτοπο ήταν $\Rightarrow \Pi_2$: NP-πλήρες

(προσοχή $\Pi_1, \Pi_2 \in NP$)

4 ΣΩΣΤΟ (από ορισμό NP-πληρότητας)

Θ. Cook τη λειτουργία κάθε TM μπορώ να την "προσομοιώσω" με έναν προτασιακό τύπο

SAT → συλλαμβάνει τη δυσκολία όλων των NP προβλ.
→ Paper : Διαφ 19
Karp ⇝ επόμενες αναγωγές γνωστών προβλημάτων
NP-complete