Οι Κλάσεις ***P*** και ***NP***

Είδη Προβλημάτων

1. Προβλήματα Απόφασης (ΝΑΙ/ΌΧΙ)
2. Προβλήματα Αναζήτησης (επιστροφή δομής που πληροί κάποιες απαιτήσεις)
3. Προβλήματα Βελτιστοποίησης (επιστροφή βέλτιστης δομής/τιμής ως προς κάποια απαίτηση)
4. Προβλήματα Απαρίθμησης (όλες οι δομές που πληρούν κάποιες απαιτήσεις)
5. Προβλήματα Άθροισης (πλήθος δομών που πληρούν κάποιες απαιτήσεις)

Προβλήματα Απόφασης

Θα ασχοληθούμε με προβλήματα στα οποία η απάντηση είναι ΝΑΙ/ΟΧΙ. Μήπως αυτό είναι κάπως περιοριστικό;

- Σε προβλήματα βελτιστοποίησης δεν είναι. (βρες το ελάχιστο πλήθος ⇔ βρες αν υπάρχει λύση <όριο)

- Για υπολογισμό γενικών συναρτήσεων δεν είναι σε υπολογισιμότητα αλλά είναι στην πολυπλοκότητα (σε μερικές περιπτώσεις π.χ. $f(x) = 2^x$).

Διαφορές Πολυπλοκοτήτων

- Ο πολυωνυμικός χρόνος είναι μικρός.
- Ο εκθετικός χρόνος είναι μεγάλος.

	10	20	30	40	50	60
n	.00001 second	.00002 second	.00003 second	.00004 second	.00005 second	.00006 second
n^2	.00001 second	.00004 second	.00009 second	.00016 second	.00025 second	.00036 second
n^3	.00001 second	.00008 second	.027 second	.064 second	.125 second	.216 second
n^5	.1 second	3.2 seconds	24.3 seconds	1.7 minute	5.2 minutes	13.0 minutes
2^n	.001 second	1.0 second	17.9 minutes	12.7 days	35.7 years	366 centuries
3^n	.059 second	58 minutes	6.5 years	3855 centuries	$2 \cdot 10^8$ centuries	$1.3 \cdot 10^{13}$ centuries

Πολυωνυμικός vs Εκθετικός

Ισχυρισμός: Όλα τα «λογικά» μοντέλα υπολογισμού είναι πολυωνυμικά ισοδύναμα.

Κάθε ένα μπορεί να εξομοιώσει το άλλο με το πολύ πολυωνυμική επιβάρυνση στον χρόνο εκτέλεσης.

Ερώτησεις:

Είναι ένα πρόβλημα επιλύσιμο σε γραμμικό χρόνο;

Εξαρτάται από το μοντέλο

Σε πολυωνυμικό χρόνο;

Ανεξάρτητο από το μοντέλο!!! (Μάλλον)

Η Κλάση *P*

Ορίζουμε μία κλάση αρκετά μεγάλη ώστε να μην επηρεάζεται από μικρές αλλαγές του μοντέλου.
μαθηματικώς ευσταθής κλάση

Ορισμός: *P* είναι το σύνολο των προβλημάτων που είναι επιλύσιμα σε πολυωνυμικό χρόνο.

$$P = \bigcup_{c \geq 0} DTIME(n^c)$$

Η κλάση αυτή είναι σημαντική αφού:

Όλες οι παραλλαγές των Η/Υ (λογικές) είναι πολυωνυμικά ισοδύναμες με έναν απλό Η/Υ.

Σε γενικές γραμμές αντιστοιχεί στα ρεαλιστικώς επιλύσιμα προβλήματα (βατά/διαχειρίσιμα).

Η Κλάση P

- Η μετάβαση από εκθετικό σε πολυωνυμικό χρόνο για ένα πρόβλημα απαιτεί συνήθως εξαιρετική διαίσθηση.
- Αν βρεθεί ένας μη αποδοτικός πολυωνυμικός αλγόριθμος για ένα πρόβλημα, συνήθως μπορούμε να βρούμε έναν πιο αποδοτικό μετά.

Παραδείγματα: Προβλήματα στο P

Αριθμητική: Πρόσθεση, αφαίρεση, πολλαπλασιασμός, διαίρεση με υπόλοιπο.

Αλγόριθμοι σε Ακέραιους: Μέγιστος Κοινός Διαιρέτης.

Έρευνα Λειτουργίας: Μέγιστες ροές, γραμμικός προγραμματισμός.

Άλγεβρα: Πολλαπλασιασμός μητρώων, υπολογισμός οριζουσών, αναστροφή μητρώου, επίλυση γραμμικών συστημάτων.

Αλγόριθμοι Γραφημάτων: BFS και DFS σε γραφήματα, Ελάχιστο ζευγνύον δένδρο, εύρεση μονοπατιού Euler.

Κωδικοποίηση

Για αριθμούς:

- Δυαδική αναπαράσταση (Καλή)
- Μοναδιαία αναπαράσταση μη-ρεαλιστική (εκθετικά μεγαλύτερη)

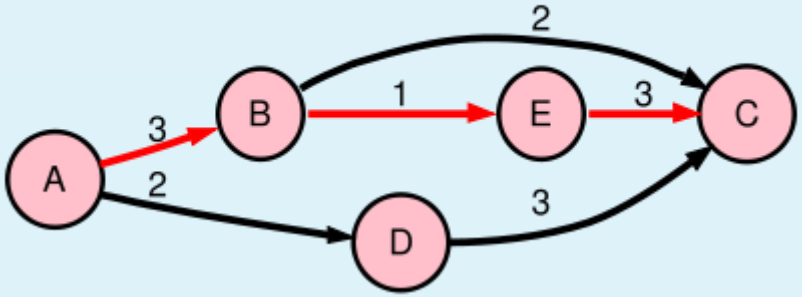
Για γραφήματα:

- Λίστα κόμβων και ακμών (Καλή)
- Πίνακας γειτνίασης (Καλή)

Το Πρόβλημα της Διαδρομής

Δοθέντος ενός κατευθυντικού γραφήματος G και κόμβους s και t, υπάρχει διαδρομή από το s στο t;

ΔΙΑΔΡΟΜΗ = $\{\langle G, s, t\rangle \mid$ Το G έχει κατευθυντική διαδρομή από το s στο t.$\}$



Πολυπλοκότητα Διαδρομής

Θεώρημα:

$$\text{ΔΙΑΔΡΟΜΗ} \in P$$

Όταν δεν ξέρουμε τι να κάνουμε : Εξάντληση

- Έστω n το πλήθος των κόμβων του G
- Κάθε διαδρομή από το s στο t δεν χρειάζεται να επαναλαμβάνει κόμβους, άρα έχει μήκος $\leq n$
- Εξετάζουμε κάθε μονοπάτι του G μήκους $\leq n$
- Ελέγχουμε αν πάει από το s στο t.

$O(n^n)$ συνολικά μονοπάτια.
Ουπς, δεν ανήκει στο P!!

Ερώτηση: Ποια η πολυπλοκότητα του αλγόριθμου;

Πολυπλοκότητα Διαδρομής (BFS)

Θεώρημα:

$$\text{ΔΙΑΔΡΟΜΗ} \in P$$

1. Μαρκάρουμε τον s
2. Επαναλαμβάνουμε μέχρι να μην μείνει καμία κορυφή:
   - Διαπέραση ακμών του G.
   - Αν η ακμή (a, b) από μαρκαρισμένο κόμβο a σε μη-μαρκαρισμένο κόμβο b,
   - Τότε μαρκάρισε το b.
3. Αν το t είναι μαρκαρισμένο τότε αποδεχόμαστε, αλλιώς απορρίπτουμε.

Ερώτηση: Ποια η πολυπλοκότητα;

Γραμμική…. Ως προς τι;;;;

Αμοιβαία Πρώτοι

Δύο αριθμοί είναι αμοιβαία πρώτοι αν το 1 είναι ο μεγαλύτερος ακέραιος που διαιρεί τέλεια και τους δύο αριθμούς.

- Το 10 και 21 είναι αμοιβαία πρώτοι
- Το 10 και 22 δεν είναι αμοιβαία πρώτοι

ΑΜΟΙΒΑΙΑ_ΠΡΩΤΟΙ = {⟨x, y⟩ | οι x και y είναι αμοιβαία πρώτοι}

Αμοιβαία Πρώτοι

Εξάντληση: δοκίμασε όλους τους αριθμούς μέχρι min(x,y) και έλεγξε αν διαιρούνται.

Πολυπλοκότητα;;;

Αν το x, y σε μοναδιαία μορφή:

- Το μέγεθος του $\langle x \rangle$, είναι x
- Έλεγχος των δυνατών διαιρετών του x, y είναι πολυωνυμικός

Αν το x, y σε δυαδική μορφή:

- Το μέγεθος του $\langle x \rangle$, είναι $\log x$
- Έλεγχος των δυνατών διαιρετών του x, y είναι εκθετικός

Τέτοιου τύπου αλγόριθμος ονομάζεται *ψευδο-πολυωνυμικός*.

Ο Αλγόριθμος του Ευκλείδη

Εύρεση Μέγιστου Κοινού Διαιρέτη, E:

Σε είσοδο $\langle x, y \rangle$

1. Επανέλαβε μέχρι $y = 0$
    1. $x \leftarrow x \bmod y$
    2. Αντάλλαξε το x με y
2. Έξοδος x

Πολυπλοκότητα;;;

1.Κάθε εκτέλεση του βήματος 1 μειώνει το x τουλάχιστον κατά το ήμισυ.

2.Πλήθος εκτελέσεων του 1 είναι $O(\min\{\log_2 x\,, \log_2 y\})$

Άρα πολυωνυμικός αλγόριθμος. Άρα: **ΑΜΟΙΒΑΙΑ_ΠΡΩΤΟΙ** $\in \boldsymbol{P}$

Η Κλάση NTime

Έστω:

$$f : \mathbb{N} \to \mathbb{N}$$

μία συνάρτηση.

Ορισμός:

NTIME($f(n)$) = {L | Η L είναι ένα πρόβλημα που λύνεται από έναν ανταιτιοκρατικό αλγόριθμο σε $O(f(n))$ βήματα.}

Η Κλάση *NP*

Ορισμός:

Η κλάση *NP* είναι το σύνολο των προβλημάτων που επιλύονται σε πολυωνυμικό χρόνο από έναν μη-αιτιοκρατικό Η/Υ.

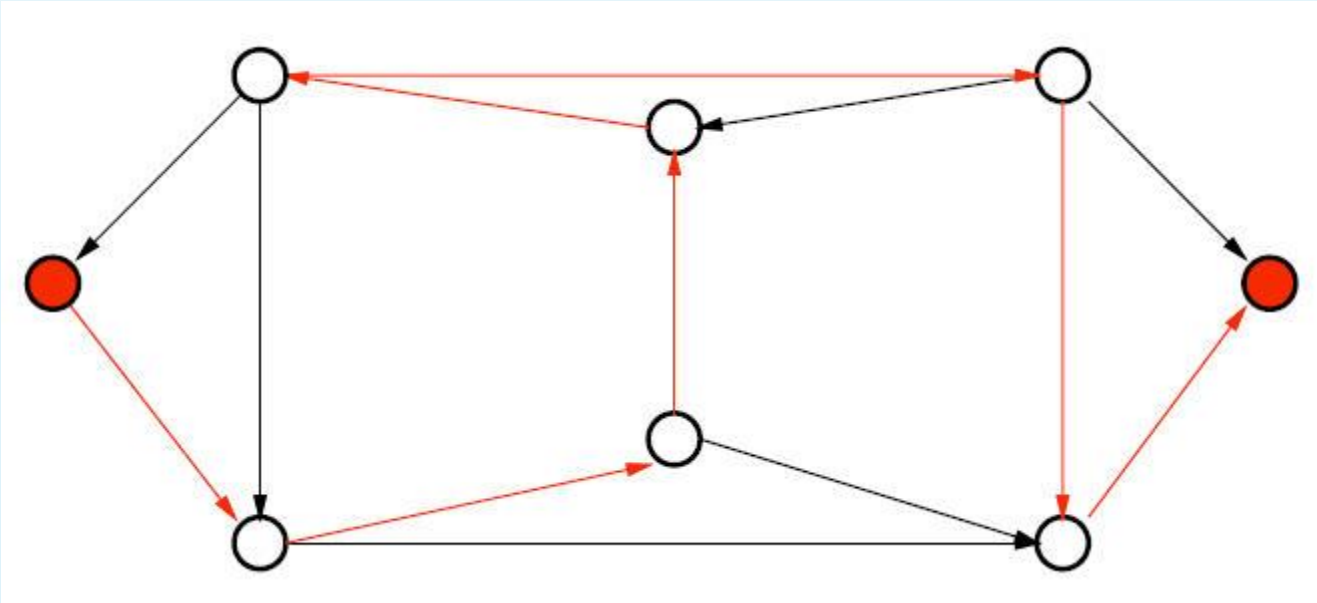
$$NP = \bigcup_{c \geq 0} NTIME(n^c)$$

Η κλάση *NP* είναι σημαντική αφού:

- Η *NP* είναι αναλλοίωτη σε κάθε επιλογή «λογικού» ανταιτιοκρατικού μοντέλου υπολογισμού.
- Αντιστοιχεί σε προβλήματα των οποίων η λύση «δεν μπορεί» να παραχθεί αποδοτικά αλλά μπορεί να ***ελεγχθεί*** αποδοτικά.

Hamiltonian Μονοπάτι

Ένα Hamiltonian μονοπάτι σε ένα κατευθυντό γράφημα G, επισκέπτεται κάθε κόμβο ακριβώς μία φορά.



Hamiltonian Μονοπάτι

HAMPATH = {⟨G, s, t⟩ | Το G έχει μονοπάτι Hamiltonian από το s στο t}

Ερώτηση: Πόσο δύσκολη είναι η επίλυση του προβλήματος;

Εύκολη μία εκθετικού χρόνου λύση παράγοντας όλα τα δυνατά μονοπάτια και ελέγχοντας κάθε ένα από αυτά αν είναι Hamiltonian.
(Εξαντλητική Αναζήτηση)

Επίλυση από έναν Ανταιτιοκρατικό Η/Υ (NTM)

Σε είσοδο $\langle G, s, t \rangle$,

1. Μάντεψε και γράψε μία λίστα από αριθμούς $p_1, \ldots, p_m$
2. Ελέγχουμε για επαναλήψεις
3. Ελέγχουμε αν $p_1 = s$ και $p_m = t$
4. Ελέγχουμε αν (p_i, p_{i+1}) είναι μία ακμή του G

Βήμα 1: ανταιτιοκρατικός πολυωνυμικός χρόνος

Βήματα 2 και 3: απλοί έλεγχοι σε πολυωνυμικό χρόνο.

Βήμα 4: απλός έλεγχος σε πολυωνυμικό χρόνο

Hamiltonian Μονοπάτι

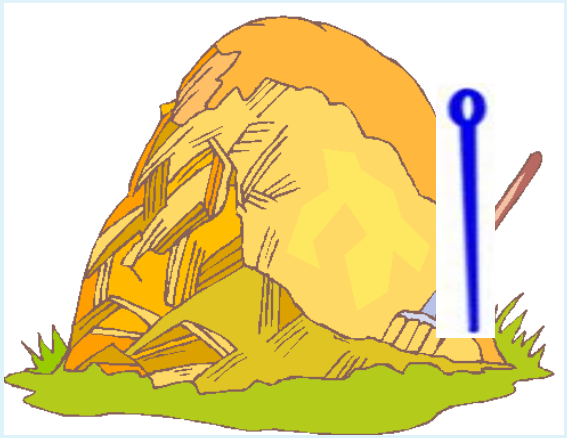
Αυτό το πρόβλημα έχει μία πολύ ενδιαφέρουσα ιδιότητα: ***πολυωνυμική επαληθευσιμότητα***

- Δεν ξέρουμε έναν γρήγορο τρόπο για να βρούμε ένα τέτοιο μονοπάτι
- αλλά μπορούμε να ελέγξουμε γρήγορα αν ένα δοθέν μονοπάτι είναι Hamiltonian.

Με άλλα λόγια:

- Η επαλήθευση ορθότητας ενός μονοπατιού φαίνεται να είναι πιο εύκολη από το να βρούμε αν υπάρχει ένα τέτοιο

Είναι η εξαντλητική αναζήτηση απαραίτητη;



Όχι αν έχεις μαγνήτη (ή vodafone)

Σύνθετοι Αριθμοί

Ένας φυσικός αριθμός είναι σύνθετος αν είναι γινόμενο δύο φυσικών αριθμών μεγαλύτερων του 1.

COMP = $\{ \langle x \rangle \mid x = pq$ για ακέραιους $p, q > 1\}$

Δεν έχουμε αποδοτικό πολυωνυμικό αλγόριθμο για να επιλύουμε το συγκεκριμένο πρόβλημα αλλά μπορούμε εύκολα να επαληθεύσουμε αν ένας αριθμός είναι σύνθετος

$2^{O\left(\sqrt[3]{n \log n}\right)}$ για αριθμούς με n bits

Στην πραγματικότητα, το καλοκαίρι του 2002, δύο φοιτητές (σαν και εσάς) και ο καθηγητής τους βρήκαν τρόπο να το κάνουν σε πολυωνυμικό χρόνο.

Επαληθευσιμότητα

Ένας επαληθευτής για την γλώσσα A είναι ένας αλγόριθμος V έτσι ώστε:

$$A = \{w \mid \text{Ο } V \text{ αποδέχεται τη λέξη } \langle w,c\rangle, \text{ για κάποια λέξη } c\}$$

- Ο επαληθευτής χρησιμοποιεί την επιπρόσθετη πληροφορία c για να επαληθεύσει το αν $w \in A$.
- Μετράμε το χρόνο της επαλήθευσης με βάση το μήκος του w.
- Η λέξη c καλείται πιστοποιητικό (ή απόδειξη) του w αν ο V αποδέχεται τη λέξη $\langle w,c\rangle$.
- Ένας πολυωνυμικός επαληθευτής εκτελείται σε πολυωνυμικό χρόνο ως προς το $|w|$ (άρα $|c| \leq |w|^{O(1)}$).
- Μια γλώσσα A είναι πολυωνυμικά επαληθεύσιμη αν έχει πολυωνυμικό επαληθευτή.

Πιστοποιητικά για HAMPATH

Για το HAMPATH, ένα πιστοποιητικό για

$$\langle G,s,t\rangle \in \text{HAMPATH}$$

είναι απλά το Hamiltonian μονοπάτι από το s στο t.

Μπορούμε να επαληθεύσουμε σε χρόνο πολυωνυμικό σε σχέση με το $|\langle G\rangle|$ αν το μονοπάτι είναι Hamiltonian.

Πιστοποιητικά για Συνθετότητα

Για τους σύνθετους αριθμούς ένα πιστοποιητικό για:

$$x \in \text{COMPOSITES}$$

είναι απλά κάποιος από τους διαιρέτες του.

Μπορούμε να επαληθεύσουμε σε χρόνο πολυωνυμικό ως προς $|x|$ αν ο δοθέν διαιρέτης πραγματικά διαιρεί το x.

Επαληθευσιμότητα

Δεν είναι όλα τα προβλήματα πολυωνυμικώς επαληθεύσιμα.

Δεν υπάρχει τρόπος να επαληθεύσουμε σε πολυωνυμικό χρόνο το co-HAMPATH.

Θα δούμε πολλά παραδείγματα όπου η γλώσσα L είναι πολυωνυμικώς επαληθεύσιμη αλλά το συμπλήρωμά της, $co\text{-}L$, δεν είναι γνωστό αν είναι πολυωνυμικώς επαληθεύσιμο.

Η NP και Επαληθευσιμότητα

Θεώρημα: Ένα πρόβλημα ανήκει στην κλάση *NP* αν και μόνο αν είναι πολυωνυμικά επαληθεύσιμο.

Απόδειξη – Διαίσθηση:

- Η NTM εξομοιώνει τον επαληθευτή μαντεύοντας την απόδειξη.
- Ο επαληθευτής εξομοιώνει την NTM, χρησιμοποιώντας ως απόδειξη τον αποδεκτικό κλάδο υπολογισμού (πολυωνυμικά μεγάλο).

Ισχυρισμός: Αν η A έχει πολυωνυμικό επαληθευτή τότε μπορεί να επιλυθεί από μία NTM σε πολυωνυμικό χρόνο.

Έστω V ένας πολυωνυμικός επαληθευτής της A.

- Μονοταινιακή TM
- Χρόνος εκτέλεσης n^k

N: σε είσοδο w μήκους n

- Ανταιτιοκρατικά επέλεξε λέξη c μήκους n^k
- Τρέξε τον V *στο* $\langle w,c \rangle$
- Αν η V αποδέχεται, αποδεχόμαστε αλλιώς απορρίπτουμε

Ισχυρισμός: Αν η A επιλύεται από μία NTM N σε πολυωνυμικό χρόνο n^k, τότε η A έχει πολυωνυμικό επαληθευτή.

Κατασκευάζουμε έναν πολυωνυμικό επαληθευτή V ως εξής:

V: σε είσοδο w μήκους n, και σε λέξη c μήκους n^k

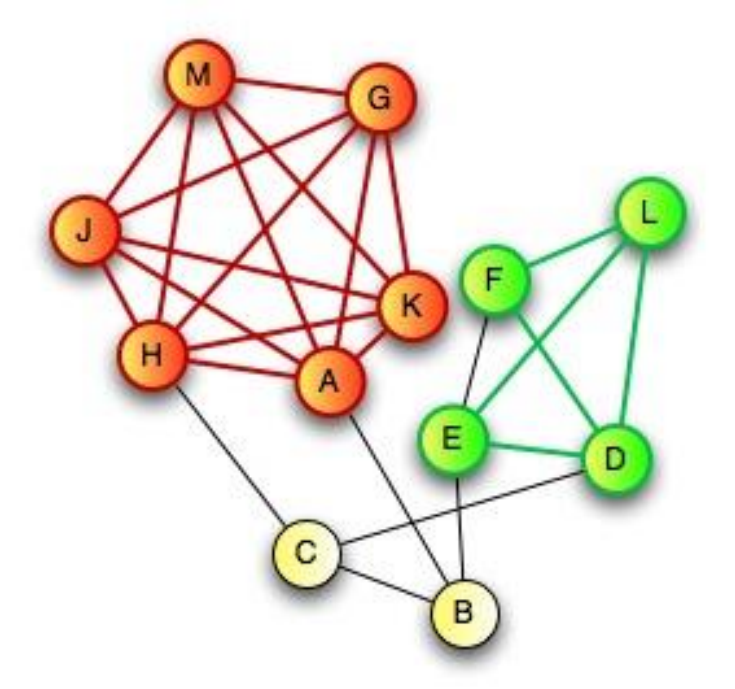
- Εξομοιώνουμε την N σε είσοδο w, χρησιμοποιώντας κάθε σύμβολο του c σαν περιγραφή της ανταιτιοκρατικής επιλογής σε κάθε βήμα της N.
- Αν αυτός ο κλάδος αποδέχεται, αποδεχόμαστε αλλιώς απορρίπτουμε.

Παραδείγματα: Κλίκα

Μία κλίκα σε ένα γράφημα είναι ένα υπογράφημα όπου κάθε ζευγάρι συνδέεται με μία ακμή.

Μία k-κλίκα είναι μία κλίκα τάξης k.

Ποια είναι η μεγαλύτερη k-κλίκα παρακάτω;



Κλίκα

ΚΛΙΚΑ = $\{\langle G, k\rangle \mid$ Ο G είναι ένα γράφημα με k-κλίκα$\}$

Θεώρημα:

$$\textit{ΚΛΙΚΑ} \in \textit{NP}$$

Η κλίκα είναι το πιστοποιητικό.

Ένας επαληθευτής V: σε είσοδο $\langle G, k, c\rangle$

- Αν c δεν είναι k-κλίκα, απορρίπτουμε
- Αν ο G δεν περιέχει όλες τις κορυφές του c, απορρίπτουμε
- Αποδεχόμαστε

Κλίκα ∈ NP

Εναλλακτική Απόδειξη:

Θα φτιάξουμε έναν ανταιτιοκρατικό αλγόριθμο N που να επιλύει το συγκεκριμένο πρόβλημα.

Ομοιότητα με την προηγούμενη απόδειξη;;;;

N: για είσοδο $\langle G,k \rangle$

1. Επιλέγουμε ανταιτιοκρατικά ένα σύνολο k κόμβων του G, έστω c
2. Ελέγχουμε αν το G περιέχει όλες τις ακμές που συνδέουν κόμβους του c
3. Αν ναι, αποδεχόμαστε αλλιώς απορρίπτουμε.

Άθροισμα Υποακολουθίας

Στιγμιότυπο του προβλήματος:

Μια συλλογή από αριθμούς $x_1, \ldots, x_k$

Αριθμός στόχος: t

Ερώτηση: Υπάρχει υποακολουθία της οποίας το άθροισμα να είναι ακριβώς t;

$$\text{ΑΘ\_ΥΠ} = \{\langle S, t\rangle \mid S = \langle x_1, \ldots, x_k\rangle, \exists\, y_1, \ldots, y_\lambda \subseteq x_1, \ldots, x_k: \Sigma y_i = t\}$$

Άθροισμα Υποακολουθίας

Παράδειγμα:

- $(\{4, 11, 16, 21, 27\}, 25) \in$ ΑΘ_ΥΠ αφού $4 + 21 = 25$.
- $(\{4, 11, 16, 21, 27\}, 26) \notin$ ΑΘ_ΥΠ (γιατί;)

Θεώρημα:

$$\text{ΑΘ\_ΥΠ} \in NP$$

Η υποακολουθία είναι το πιστοποιητικό.

Ο επαληθευτής: V σε είσοδο $\langle S, t, c\rangle$

- Έλεγξε αν c είναι μία συλλογή αριθμών με άθροισμα t
- Έλεγξε αν το c είναι υποακολουθία του S
- Αν αποτύχουμε σε (1) ή (2) τότε απόρριψη αλλιώς αποδοχή

Συμπληρωματικά Προβλήματα

Η *co-ΚΛΙΚΑ* και *co-ΑΘ-ΥΠ* φαίνεται ότι δεν είναι μέλη της κλάσης *NP*.

Είναι πιο δύσκολη η αποδοτική επαλήθευση ότι κάτι δεν υπάρχει παρά η αποδοτική επαλήθευση ότι κάτι υπάρχει.

Κλάση προβλημάτων για τα οποία υπάρχουν αποδοτικώς επαληθεύσιμα αντιπαραδείγματα

Ορισμός: Η κλάση co-NP:

$$L \in \text{co-NP} \text{ αν } \text{co-}L \in \text{NP}$$

Μέχρι τώρα δεν ξέρουμε αν οι κλάσεις co-NP και NP είναι πράγματι διαφορετικές.

co-NP

Έστω το *co-ΑΘ-ΥΠ*: δοθέντος ενός συνόλου ακεραίων, κάθε υποσύνολο να έχει άθροισμα που να μην είναι ίσο με το στόχο; έχουμε μία απόδειξη για αρνητική απάντηση (*αντιπαράδειγμα*) που είναι αποδοτικά επαληθεύσιμη, απλά ένα σύνολο που να έχει άθροισμα ίσο με το στόχο.

Παράδειγμα:

({4, 11, 16, 21, 27}, 25) ∉ co-ΑΘ_ΥΠ αφού 4 + 21 = 25

({4, 11, 16, 21, 27}, 26) ∈ co-ΑΘ_ΥΠ αφού ?????

Ασυμμετρία σε NP και coNP

Η κλάση NP είναι κλειστή ως προς ένωση, τομή, και σώρευση.

- Πιστεύουμε ότι κλάση NP δεν είναι κλειστή ως προς συμπλήρωμα (ασυμμετρία υπέρ αποδοχής).
- co-NP: αντίστοιχη κλάση με ασυμμετρία υπέρ απόρριψης.

Άσκηση 7.6: Δείξτε ότι η κλάση P είναι κλειστή ως προς την ένωση

Για γλώσσες $L_1 \in P$ και $L_2 \in P$, υπάρχει ΤΜ Μ΄ που επιλύει την $L_1 \cup L_2$ σε πολυωνυμικό χρόνο. Έστω M_1 η ΤΜ για L_1 και M_2 η ΤΜ για την L_2.

M' : σε είσοδο <w>

1. Εξομοιώνουμε την M_1 σε w.
2. Αν η M_1 αποδέχεται τότε ΑΠΟΔΟΧΗ
3. Εξομοιώνουμε την M_2 σε w.
4. Αν η M_2 αποδέχεται τότε ΑΠΟΔΟΧΗ
5. ΑΠΟΡΡΙΨΗ

Προφανώς η γλώσσα της M' είναι η ένωση των γλωσσών. Η M' τρέχει σε πολυωνυμικό χρόνο αφού και οι δύο μηχανές M_1 και M_2 τρέχουν σε πολυωνυμικό χρόνο. Άρα η P είναι κλειστή ως προς την ένωση.

Άσκηση 7.6: Δείξτε ότι η κλάση P είναι κλειστή ως προς τη συναρμογή

Για δοθείσες γλώσσες $L_1 \in P$ και $L_2 \in P$, υπάρχει ΤΜ M' που επιλύει την L_1 ο L_2 σε πολυωνυμικό χρόνο. Έστω M_1 η ΤΜ για L_1 και M_2 η ΤΜ για την L_2. Η Μ΄ είναι η εξής:

M' : σε είσοδο $<w>$

1. Για $i = 0$ μέχρι $|w|$
    1. Τρέξε την M_1 στους πρώτους i χαρακτήρες του w
    2. Τρέξε την M_2 στους χαρακτήρες από $i+1$ μέχρι $|w|$ του w
    3. Αν και οι δύο ΤΜ αποδεχτούμε τότε ΑΠΟΔΟΧΗ
2. ΑΠΟΡΡΙΨΗ

Ο αλγόριθμος είναι πολυωνυμικός και έχει χρονική πολυπλοκότητα $O(n)$ (πλέον των πολυπλοκοτήτων των μηχανών). Η γλώσσα της M' είναι η συναρμογή των γλωσσών. Η M' τρέχει σε πολυωνυμικό χρόνο αφού και οι δύο μηχανές M_1 και M_2 τρέχουν σε πολυωνυμικό χρόνο. Άρα η P είναι κλειστή ως προς τη συναρμογή.

Άσκηση 7.6: Δείξτε ότι η κλάση *P* είναι κλειστή ως προς το συμπλήρωμα

Αν μία γλώσσα *L* ανήκει στο *P* τότε η αντίστοιχη ΤΜ *A* την επιλύει σε πολυωνυμικό χρόνο. Η συμπληρωματική της μπορεί επίσης να επιλυθεί σε πολυωνυμικό χρόνο με αντιστροφή των εξόδων της *A*.

Άρα και η L' ανήκει στο *P*.

Άρα η *P* είναι κλειστή ως προς το συμπλήρωμα.

Άσκηση 7.6: Δείξτε ότι η κλάση P είναι κλειστή ως προς τη σώρευση (εκτός ύλης)

Έστω μία ΤΜ A που ανήκει στο P για τη γλώσσα L. Κατασκευάζουμε μία ΤΜ A^* που ανήκει στο P που αποδέχεται το L^*. Η λύση θα βασιστεί σε δυναμικό προγραμματισμό και θα φτιάξει έναν boolean πίνακα S όπου $S[i,j]$ αναπαριστά αν η υποακολουθία $w_i...w_j$ της εισόδου $w=w_1...w_n$ ανήκει στη L.

Η ΤΜ A^* θα κάνει τα εξής:

1. Αν $w = \varepsilon$, ΑΠΟΔΕΧΟΜΑΣΤΕ
2. Για $i = 1$ μέχρι n,
    1. $S[i,i] = 1$ αν η A αποδέχεται το w_i
3. Για $k = 2$ μέχρι n,
    1. Για $i = 1$ μέχρι $n - k + 1$
        1. $j = i + k – 1$
        2. Αν η A αποδέχεται το $w_i...w_j$ τότε $S[i,j] = 1$
        3. Αλλιώς Για $m = i$ μέχρι $j – 1$ //Περίπτωση η $w_i...w_j$ να προκύπτει από συναρμογή.
            1. Αν $S[i,m]=1$ και $S[m,j]=1$ τότε $S[i,j] = 1$
4. Αν $S[1,n] = 1$, ΑΠΟΔΕΧΟΜΑΣΤΕ.

Ο αλγόριθμος είναι πολυωνυμικός και έχει χρονική πολυπλοκότητα $O(n^3)$. Άρα η P είναι κλειστή ως προς τη σώρευση.

Άσκηση 7.7: Δείξτε ότι η κλάση *NP* είναι κλειστή ως προς την ένωση

Για γλώσσες $L_1 \in NP$ και $L_2 \in NP$, υπάρχει NTM N΄ που επιλύει την $L_1 \cup L_2$ σε ανταιτιοκρατικό πολυωνυμικό χρόνο. Έστω N_1 η TM για L_1 και N_2 η TM για την L_2.

N' : σε είσοδο <w>

1. Εξομοιώνουμε την N_1 σε w.
2. Αν η N_1 αποδέχεται τότε ΑΠΟΔΟΧΗ
3. Εξομοιώνουμε την N_2 σε w.
4. Αν η N_2 αποδέχεται τότε ΑΠΟΔΟΧΗ
5. ΑΠΟΡΡΙΨΗ

Η γλώσσα της N' είναι η ένωση των γλωσσών. Η N' τρέχει σε ανταιτιοκρατικό πολυωνυμικό χρόνο αφού και οι δύο μηχανές N_1 και N_2 τρέχουν σε ανταιτιοκρατικό πολυωνυμικό χρόνο. Άρα η *NP* είναι κλειστή ως προς την ένωση.

NP = co-NP ;;;;;

Έχουν τα αποδεκτικά στιγμιότυπα αποδοτικούς επαληθευτές αν έχουν και τα απορριπτικά στιγμιότυπα;

Μάλλον ΟΧΙ.

Λήμμα: Αν NP ≠ co-NP, τότε P ≠ NP.

Ισοδύναμα: Αν P = NP, τότε NP = co-NP.

Ιδέα απόδειξης:

- Το P είναι κλειστό ως προς το συμπλήρωμα.
- Αν P = NP, τότε και το NP είναι κλειστό ως προς το συμπλήρωμα.
- Με άλλα λόγια, NP = co-NP.

Αποδείχτηκε

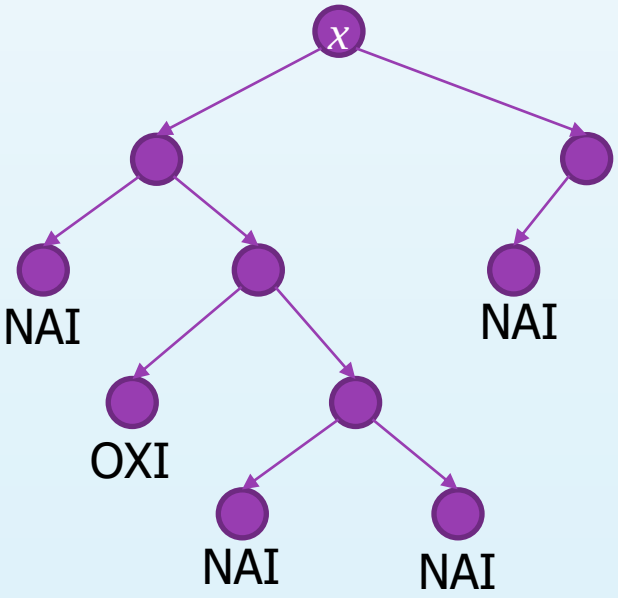
Συμπληρώνοντας τις Εξόδους

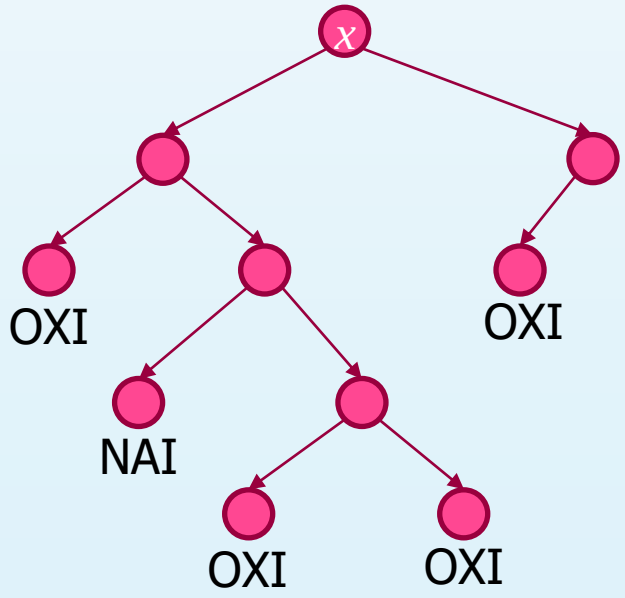
Έστω M διαγιγνώσκει την L, και M' είναι η M μετά την αντιστροφή εξόδου.

- Αν η M είναι μία αιτιοκρατική ΤΜ τότε η M' αποφασίζει την L'.
- Αν η M είναι μία ανταιτιοκρατική ΤΜ, τότε η M' μπορεί να μην αποφασίζει την L'.

Είναι πιθανό οι M και M' να δέχονται και οι δύο μία είσοδο x και άρα δεν είναι συμπληρωματικές οι γλώσσες τους

Συμπληρώνοντας τις Εξόδους





$x \in L$

$x \in L'$

Άρα $L' \neq co\text{-}L$

$NP \cap co\text{-}NP$

$IF \in P;;;;$

- Μπορείτε να σκεφτείτε προβλήματα που ανήκουν στο $NP \cap co\text{-}NP;;;$

Η κλάση προβλημάτων P

- Το πρόβλημα παραγοντοποίησης ακεραίων:

$$IF = \{\langle m, n\rangle \mid m = x \times q, x \in (1, n], q \in N\}$$

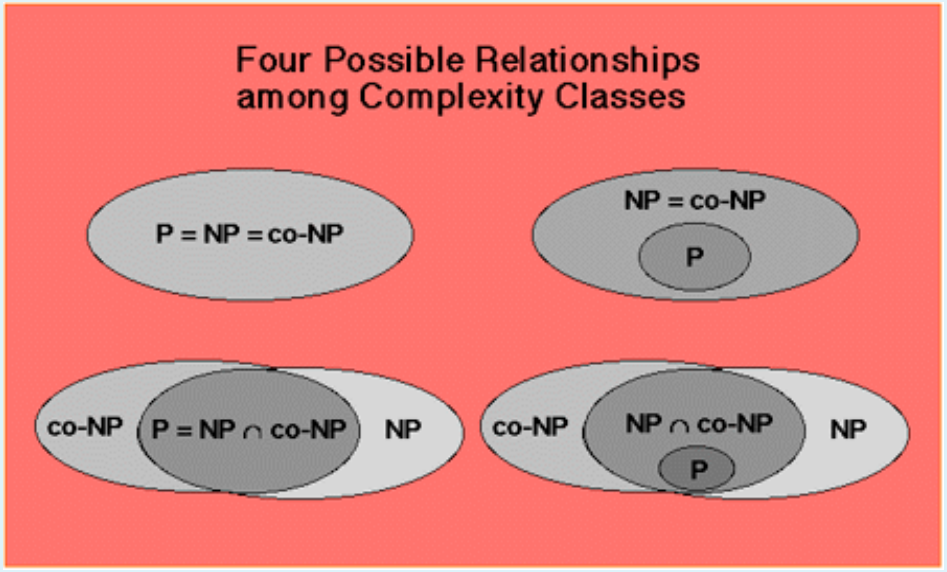
$IF \in NP$: το πιστοποιητικό είναι το x

$IF \in$ co-NP: όλοι οι πρώτοι παράγοντες του m μαζί με ένα πιστοποιητικό για τον καθένα ότι είναι πρώτοι

P vs. NP
Ή Τρόπος vs Κόπος

- Το *P* είναι υποσύνολο του *NP*

- Είναι *P=NP*; Αν ναι, τότε κάθε απλοϊκό πρόβλημα εξαντλητικής αναζήτησης θα είχε ένα πολυωνυμικού χρόνου αλγόριθμο



Clay Mathematics Institute

| [home] | [index] |

- Annual Meeting - Research - Students - Awards - Summer School - Workshops - About CMI - Millennium Prize Problems - News -

HOME / MILLENNIUM PRIZE PROBLEMS

MILLENNIUM PRIZE PROBLEMS

P versus NP

The Hodge Conjecture

The Poincaré Conjecture

The Riemann Hypothesis

Yang-Mills Existence and Mass Gap

Navier-Stokes Existence and Smoothness

The Birch and Swinnerton-Dyer Conjecture

Announced 16:00, on Wednesday, May 24, 2000
Collège de France

Λύθηκε (Perelman)!

P vs. NP και Μαθηματικά

- Αν *P=NP*, τότε θα αντικαθιστούσαμε τους μαθηματικούς από (πολύ πιο αξιόπιστους) υπολογιστές:

> *P=NP*: Υπάρχει αλγοριθμική διαδικασία που παίρνει ως είσοδο οποιαδήποτε τυπική μαθηματική πρόταση και πάντα παράγει την μικρότερη δυνατή απόδειξη σε χρόνο ανάλογο με το μήκος της απόδειξης.

- Αυτός είναι ένα λόγος που συνήθως θεωρούμε (ιδιαίτερα οι μαθηματικοί!) ότι οι κλάσεις *P* και *NP* είναι διαφορετικές.