ΘΕΩΡΙΑ ΥΠΟΛΟΓΙΣΜΩΝ ΚΑΙ ΑΥΤΟΜΑΤΩΝ

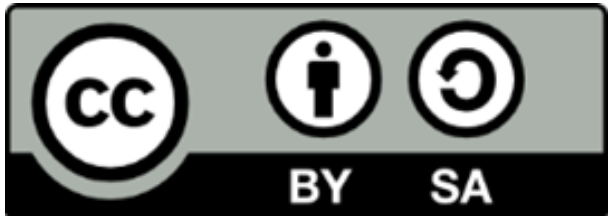
Ενότητα 12: Μη ντετερμινιστικές μηχανές Turing

Ρεφανίδης Ιωάννης

Τμήμα Εφαρμοσμένης Πληροφορικής

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Μη Ντετερμινιστικές Μηχανές Turing

Ορισμός

- Μια μη-ντετερμινιστική μηχανή Turing ορίζεται όμοια με μια ντετερμινιστική, με την εξής διαφορά:
  - Για κάθε συνολική κατάσταση της μηχανής , μπορεί να ορίζονται περισσότερες από μια επόμενες καταστάσεις.
- Δημιουργείται το ερώτημα, πώς λειτουργεί.

Μη-ντετερμινισμός και ημι-αποφασίσιμες γλώσσες

- Μια μη-ντετερμινιστική μηχανή Turing **δέχεται** μια είσοδο w, αν υπάρχει τρόπος ξεκινώντας με είσοδο το w να καταλήξουμε σε τελική κατάσταση.
- Η μη-ντετερμινιστική μηχανή Turing **ημι-αποφασίζει** μια γλώσσα L, αν δέχεται κάθε λέξη w της L.

Μη-ντετερμινισμός και αποφασίσιμες γλώσσες

- Μια μη-ντετερμινιστική μηχανή Turing M **αποφασίζει** μια γλώσσα L, αν για κάθε λέξη $w \in \Sigma^*$ ισχύουν τα εξής:
  - Υπάρχει φυσικός αριθμός N που εξαρτάται από την M και την w, τέτοιος ώστε να μην υπάρχει κατάσταση C στην οποία να καταλήγει η μηχανή μετά από N μη-ντετερμινιστικά βήματα.
  - Η w ανήκει στην L αν και μόνο αν η M με αρχική είσοδο την w καταλήγει στην «**θετική**» κατάσταση τερματισμού της.

Μη-ντετερμινισμός και υπολογίσιμες συναρτήσεις

- Μια μη-ντετερμινιστική μηχανή Turing υπολογίζει μια συνάρτηση $f: \Sigma^* \rightarrow \Sigma^*$, αν ισχύουν τα εξής για κάθε λέξη w:
  - Υπάρχει N που εξαρτάται από την f και την w, τέτοιος ώστε να μην υπάρχει συνολική κατάσταση C προσβάσιμη από την $(s, \#w\underline{\#})$ σε N βήματα.
  - $(s,\#w\underline{\#}) \vdash^* (h,\#u\underline{\#})$ αν και μόνο αν $f(w)=u$.
    - Όλοι οι δυνατοί υπολογισμοί πρέπει να συμφωνούν.

Παράδειγμα: Σύνθετοι αριθμοί (1/2)

- Ένας σύνθετος αριθμός είναι το γινόμενο δύο μεγαλύτερων της μονάδας φυσικών αριθμών.
- Έστω C το σύνολο όλων σύνθετων αριθμών, σε δυαδική αναπαράσταση:
  - C={100, 110, 1000, 1001, 1010, …, 1011011, …}
- Για να ελέγξει αν ένας αριθμός n είναι σύνθετος, μια ντετερμινιστική μηχανή θα έπρεπε να ελέγχει όλους τους μικρότερους αριθμούς...

Παράδειγμα: Σύνθετοι αριθμοί (2/2)

- Για να ελέγξει αν ένας αριθμός n είναι σύνθετος, μια μη-ντετερμινιστική μηχανή:
  - Θα επέλεγε μη-ντετερμινιστικά δύο αριθμούς p και q, μεγαλύτερους της μονάδας και μικρότερους από τον n.
  - Θα τους πολλαπλασίαζε.
  - Εάν $n=p \cdot q$, θα τερματίζει «θετικά».
  - Εάν $n \neq p \cdot q$, θα τερματίζει «αρνητικά».

Σύγκριση ντετερμινιστικών και μη-ντετερμινιστικών μηχανών Turing

- Αν μια μη-ντετερμινιστική μηχανή Turing M αποφασίζει ή ημι-αποφασίζει μια γλώσσα ή υπολογίζει μια συνάρτηση, τότε υπάρχει μια ντετερμινιστική μηχανή Turing M' που αποφασίζει ή ημι-αποφασίζει την ίδια γλώσσα ή υπολογίζει την ίδια συνάρτηση.
  - Η M' θα προσομοιώσει συστηματικά **όλους** τους υπολογισμούς της M.
  - Η M' απαιτεί εκθετικά περισσότερο αριθμό βημάτων για να προσομοιώσει έναν υπολογισμο της M.

Αναγωγές

- Έστω $L_1, L_2 \subseteq \Sigma^*$. Μια αναγωγή από την L_1 στην L_2 είναι μια συνάρτηση $\tau : \Sigma^* \to \Sigma^*$, τέτοια ώστε $x \in L_1$ αν και μόνο αν $\tau(x) \in L_2$.
  - Κατεύθυνση αναγωγής: Από την L_1 στην L_2.

- Αν η L_1 δεν είναι αποφασίσιμη, και υπάρχει αναγωγή τ από την L_1 στην L_2, τότε ούτε η L_2 είναι αποφασίσιμη.

Κατεύθυνση αναγωγής

- Η συνάρτηση τ(x) από την L_1 στην L_2:
  - Ορίζεται για όλες τις λέξεις της L_1
  - Δεν έχει ως τιμές της όλες τις λέξεις της L_2
- Γενικά η συνάρτηση τ(x) δεν είναι αντιστρέψιμη.
  - Αν είναι, τότε ορίζεται και η αντίστροφη αναγωγή.
- Αν λοιπόν η L_1 δεν είναι αποφασίσιμη, τότε για τα αντίστοιχα προβλήματα δεν είναι ούτε η L_2.

Παράδειγμα αναγωγής (1/3)

- Έστω η γλώσσα:
- Η={«Μ»«w» : Η μηχανή Turing Μ τερματίζει με συμβολοσειρά εισόδου το w}
- Η γλώσσα αυτή είναι ημι-αποφασίσιμη
  - Πρόκειται για το πρόβλημα του τερματισμού

- Θα βρούμε συναρτήσεις αναγωγής τ από την Η σε άλλες γλώσσες.

Παράδειγμα αναγωγής (2/3)

- Δεδομένης μιας μηχανής Turing M, τερματίζει η M με είσοδο κενή ταινία;
- Περιγράφουμε μια αναγωγή από την H στην:
  - L={«M» : Η M τερματίζει με είσοδο ε}
- Για κάθε λέξη «M»«w» της H, όπου $w=a_1a_2\ldots a_n$, κατασκευάζουμε μια λέξη «M_w» της L ως εξής:
  - $M_w=Ra_1Ra_2\ldots Ra_nM$

Παράδειγμα αναγωγής (3/3)

- Δεδομένης μιας μηχανής Turing M, υπάρχει έστω και μια συμβολοσειρά για την οποία η M τερματίζει;
- Θα ανάγουμε την L στην L':
  - L' = {«M» : Η M τερματίζει για κάποια είσοδο}
- Έχοντας μια μηχανή M (για την οποία δεν μπορούμε να αποφασίσουμε αν τερματίζει με κενή είσοδο), κατασκευάζουμε μια μηχανή M', η οποία στην αρχή της λειτουργίας της διαγράφει την είσοδό της και μετά συνεχίζει σαν την M.

Μερικά ακόμη μη-αποφασίσιμα προβλήματα

- Πρόβλημα Thue
- Πρόβλημα αντιστοίχησης του Post
- Πρόβλημα πλακόστρωσης

Πρόβλημα Thue (1/2)

- Έστω ένα πεπερασμένο αταξινόμητο σύνολο ζευγών λέξεων:
  - $\{w_1,u_1\}, \{w_2, u_2\}, ..., \{w_n, u_n\}$
- Έστω δύο λέξεις w και u, τέτοιες ώστε:
  - $w=w_{i1}w_{i2}...w_{ik}$
  - $u=u_{i1}u_{i2}...u_{ik}$

    όπου $i_1, i_2, ..., i_k \in \{1, 2, ... ,n\}$
- Οι λέξεις w και u λέγονται ισοδύναμες.

Πρόβλημα Thue (2/2)

- Παράδειγμα:
  - Έστω {ab, a}, {bc, b}, {abc, c}.
  - Έστω w=abbcabc
  - Τότε η w είναι ισοδύναμη με την u=ababc
  - Πράγματι, μπορούμε να τις γράψουμε:
    - w=ab-bc-abc
    - u=a-b-c
- Το πρόβλημα που τίθεται είναι εάν μπορεί να κατασκευασθεί ένα πρόγραμμα που να μας λέει εάν για τυχαίο σύστημα Thue υπάρχουν δύο λέξεις w και u που να είναι ισοδύναμες. Το πρόβλημα αυτό είναι μη-αποφασίσιμο.

Πρόβλημα αντιστοίχησης του Post (παραλλαγή του προβλήματος Thue) (1/2)

- Έστω και πάλι ένα πεπερασμένο αταξινόμητο σύνολο ζευγών λέξεων:
  - $\{w_1,u_1\}, \{w_2, u_2\}, ..., \{w_n, u_n\}$
- Έστω μια λέξη w τέτοια ώστε:
  - $w=w_{i1}w_{i2}...w_{ik}=u_{i1}u_{i2}...u_{ik}$

    όπου $i_1, i_2, ..., i_k \in \{1, 2, ... ,n\}$
- Η λέξη w λέγεται ταίριασμα.

Πρόβλημα αντιστοίχησης του Post (2/2)

- Παράδειγμα:
  - Έστω {a, aaa}, {abaaa, ab}, {ab, b}
  - Έστω w=abaaaaaab
  - Τότε η w είναι ένα ταίριασμα, αφού:
  - abaaa-a-a-ab = ab-aaa-aaa-b
- Το πρόβλημα που τίθεται εάν για τυχαίο σύστημα αντιστοίχησης υπάρχει ένα ταίριασμα. Το πρόβλημα αυτό είναι μη-αποφασίσιμο.

Πρόβλημα πλακόστρωσης (1/2)

- Έστω ένα πεπερασμένο σύνολο από τετράγωνα πλακάκια.
- Κάθε τύπος από πλακάκι επιτρέπεται να συνορεύει προς κάθε κατεύθυνση με συγκεκριμένους τύπους από άλλα πλακάκια.
- Τα πλακάκια δεν επιτρέπεται να περιστραφούν.
- Έχουμε άπειρα πλακάκια από κάθε τύπο.

Πρόβλημα πλακόστρωσης (2/2)

- Θέλουμε να πλακοστρώσουμε το πρώτο τεταρτημόριο του επιπέδου, τοποθετώντας στην κάτω αριστερή του γωνία ένα συγκεκριμένο πλακάκι.
- Το πρόβλημα που τίθεται είναι εάν, για τυχαίο σύστημα πλακόστρωσης, είναι δυνατή η πλακόστρωση του πρώτου τεταρτημόριου.
- Το πρόβλημα αυτό είναι μη-αποφασίσιμο.

Ιδιότητες των αποφασίσιμων γλωσσών

- Μια γλώσσα είναι αποφασίσιμη, αν και μόνο αν το συμπλήρωμά της είναι επίσης αποφασίσιμο.
- Μια γλώσσα είναι αποφασίσιμη, αν και μόνο αν αυτή και το συμπλήρωμά της είναι ημι-αποφασίσιμες.

Απαριθμήσιμες γλώσσες

- Μια γλώσσα L είναι απαριθμίσιμη κατά Turing, αν και μόνο αν υπάρχει μηχανή Turing τέτοια ώστε:
  - $L=\{w : (s,\underline{\#}) \vdash^* (q,\#w\underline{\#}) \}$
- όπου q μια προκαθορισμένη «κατάσταση παρουσίασης» της M.

- Μια γλώσσα είναι ημι-αποφασίσιμη αν και μόνο αν είναι απαριθμήσιμη κατά Turing.

Λεξικογραφικά απαριθμήσιμες γλώσσες

- Μια μηχανή Turing M λέμε ότι απαριθμεί λεξικογραφικά τη γλώσσα L, αν:
  - Η M απαριθμεί την L.
  - Όποτε συμβαίνει να ισχύει:
    - $(q,\#w\underline{\#}) \vdash^* (q,\#w'\underline{\#})$
  - τότε η w προηγείται λεξικογραφικά της w'.
- Μια γλώσσα είναι αποφασίσιμη, αν και μόνο αν είναι λεξικογραφικά απαριθμήσιμη.

Θεώρημα του Rice

- Έστω ότι C είναι ένα γνήσιο μη-κενό υποσύνολο της κλάσης όλων των ημι-αποφασίσιμων γλωσσών. Τότε το ακόλουθο πρόβλημα είναι μη-αποφασίσιμο:
  - Δεδομένης μιας μηχανής Turing M, ισχύει ότι $L(M) \in C$;
- Δεν μπορούμε να αποδείξουμε στη γενική περίπτωση ότι η γλώσσα μιας μηχανής Turing είναι κανονική, χωρίς συμφραζόμενα, κλπ.

Υπολογιστική Πολυπλοκότητα

Πρακτικά εφικτοί αλγόριθμοι

- Μια μηχανή Turing M ονομάζεται πολυωνυμικά φραγμένη, αν υπάρχει πολυώνυμο p(n) τέτοιο ώστε να ισχύει το εξής:
  - Για κάθε είσοδο x, δεν υπάρχει κατάσταση C, τέτοια ώστε $(s,\#x\underline{\#}) \vdash^{p(|x|)+1} C$
- Μια γλώσσα λέγεται **πολυωνυμικά αποφασίσιμη**, αν υπάρχει μια πολυωνυμικά φραγμένη μηχανή Turing που την αποφασίζει.
- Η κλάση όλων των πολυωνυμικά αποφασίσιμων γλωσσών συμβολίζεται με $\mathcal{P}$.

Θέση του Church (revisited)

- Οι πολυωνυμικά φραγμένες μηχανές Turing και η κλάση $\mathcal{P}$ εκφράζουν ικανοποιητικά τις διαισθητικές έννοιες, αντίστοιχα, των πρακτικά εφικτών αλγορίθμων και των ρεαλιστικά επιλύσιμων προβλημάτων.

- Η κλάση $\mathcal{P}$ είναι κλειστή ως προς το συμπλήρωμα.

Προβλήματα

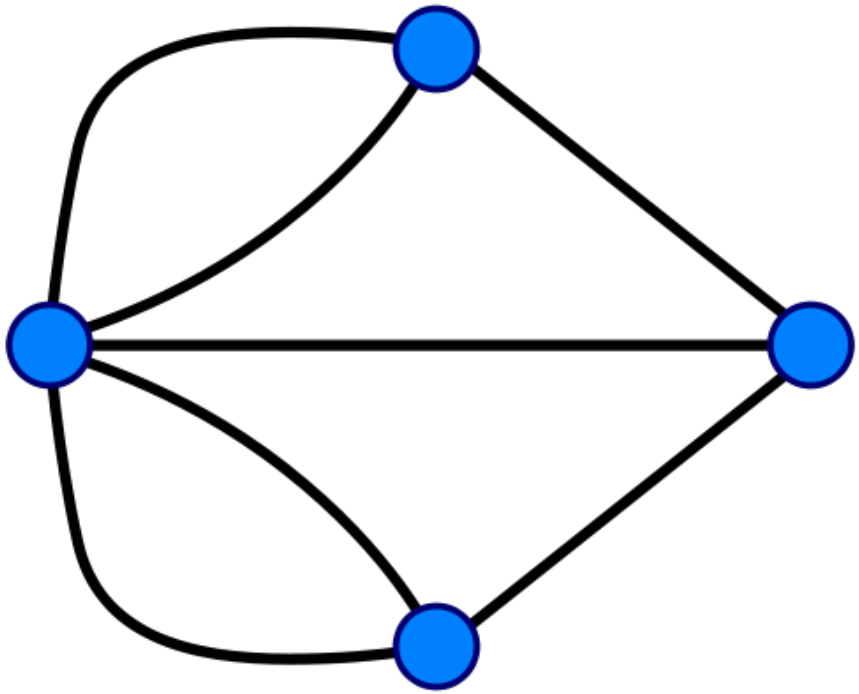
Το πρόβλημα της συνεκτικότητας

- Δεδομένων ενός κατευθυνόμενου γραφήματος $G \subseteq VxV$, όπου $V=\{v_1,v_2, \ldots, v_n\}$ και δύο κόμβων $v_i,v_j \in V$, υπάρχει μονοπάτι από τον v_i στον v_j ;
- Είναι πρόβλημα, δεν είναι γλώσσα.
- Μπορεί να μετατραπεί σε γλώσσα ως εξής:
  - $L=\{(«G»,«v_i»,«v_j») :$ Υπάρχει μονοπάτι από τον v_i στον v_j στο γράφημα G.
- Οι γλώσσες κωδικοποιούν προβλήματα!
- Ανήκει στο $\mathcal{P}$.

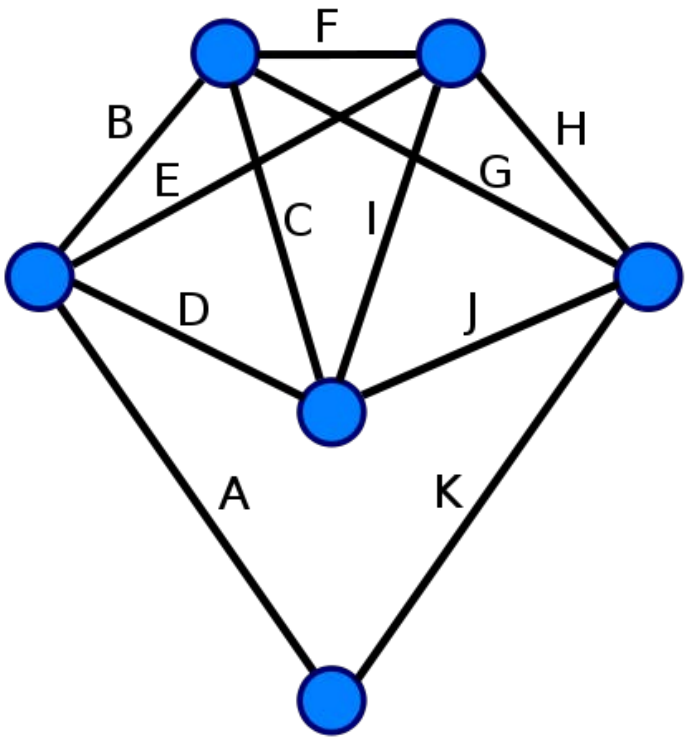
Γράφημα Euler

- Δεδομένου ενός κατευθυνόμενου γραφήματος G, υπάρχει κλειστό μονοπάτι στο G το οποίο χρησιμοποιεί κάθε ακμή ακριβώς μία φορά;
  - Γράφημα Euler ή γράφημα μοναδικής διάσχισης.
  - L = { «G» : Το G είναι γράφημα Euler }
- Λύση:
  - Υπάρχει μονοπάτι μεταξύ κάθε δύο κόμβων.
  - Για κάθε κόμβο, το πλήθος των εισερχόμενων και εξερχόμων ακμών ταυτίζονται.
- Ανήκει στο $\mathcal{P}$ (μπορεί να αποδειχθεί και με αναγωγή στο πρόβλημα της συνεκτικότητας).

Οι γέφυρες του Königsberg



Πηγή:
http://en.wikipedia.org/wiki/File:Konigsburg_graph.svg

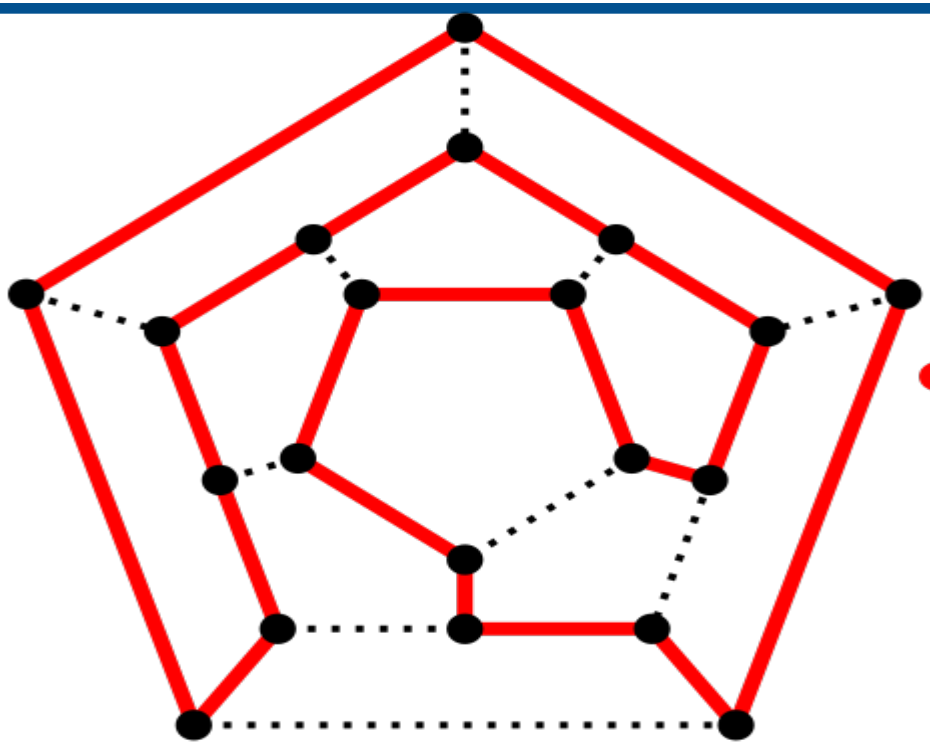


Πηγή:
http://en.wikipedia.org/wiki/File:Labelled_Eulergraph.svg

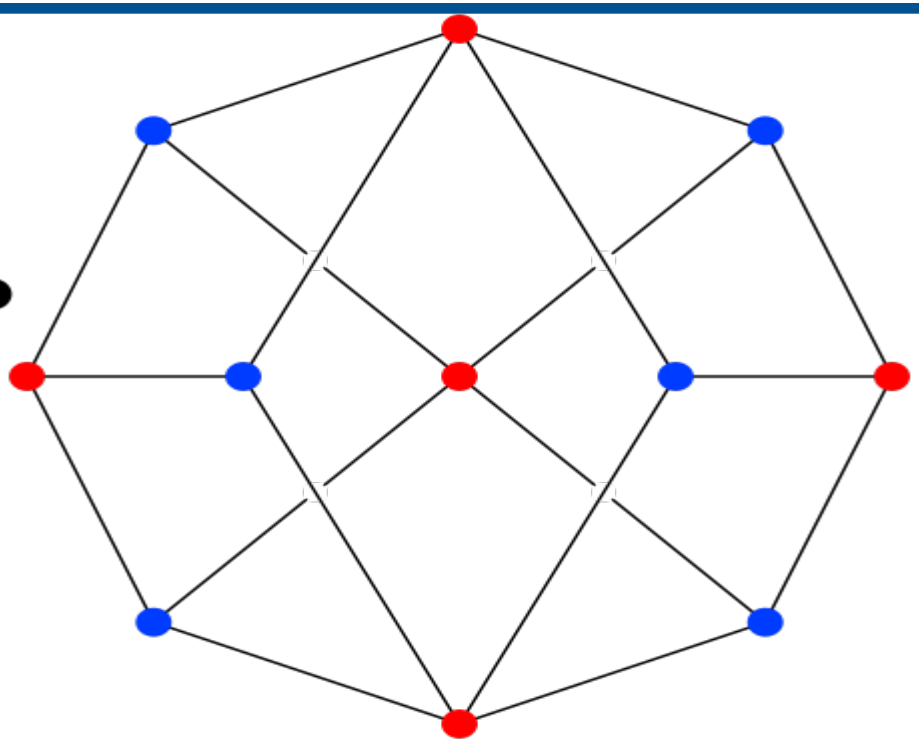
Γράφημα Hamilton (1/2)

- Δεδομένου ενός γραφήματος G, υπάρχει κύκλος που διέρχεται από κάθε κόμβο του G ακριβώς μια φορά;
  - Κύκλος Hamilton, γράφημα Hamilton.
- Δεν έχει βρεθεί κανείς πολυωνυμικός αλγόριθμος για αυτό το πρόβλημα.
- Μη-πολυωνυμική λύση:
  - Εξέτασε όλες τις μεταθέσεις κόμβων του γραφήματος.

Γράφημα Hamilton (2/2)



Πηγή:
http://upload.wikimedia.org/wikipedia/commons/6/60/Hamiltonian_path.svg



Πηγή:
http://upload.wikimedia.org/wikipedia/commons/c/cf/Herschel_graph.svg

Πλανώδιος πωλητής

- Δοθέντος ενός πλήρους, μη κατευθυνόμενου γραφήματος G=VxV με κόμβους $V=\{v_1,v_2,\ldots,v_n\}$, καθώς και ενός συμμετρικού μη-αρνητικού πίνακα D διαστάσεων nxn, με τα στοιχεία του d_{ij} να εκφράζουν το βάρος της ακμής (v_i,v_j), ψάχνουμε μια μετάθεση π των κορυφών V, έτσι ώστε να ελαχιστοποιείται το παρακάτω άθροισμα:
  - $c(\pi)=d_{\pi(1)\pi(2)}+d_{\pi(2)\pi(3)}+\ldots+d_{\pi(n-1)\pi(n)}+d_{\pi(n)\pi(1)}$
- Πρόβλημα βελτιστοποίησης

Μετατροπή προβλημάτων βελτιστοποίησης σε γλώσσες

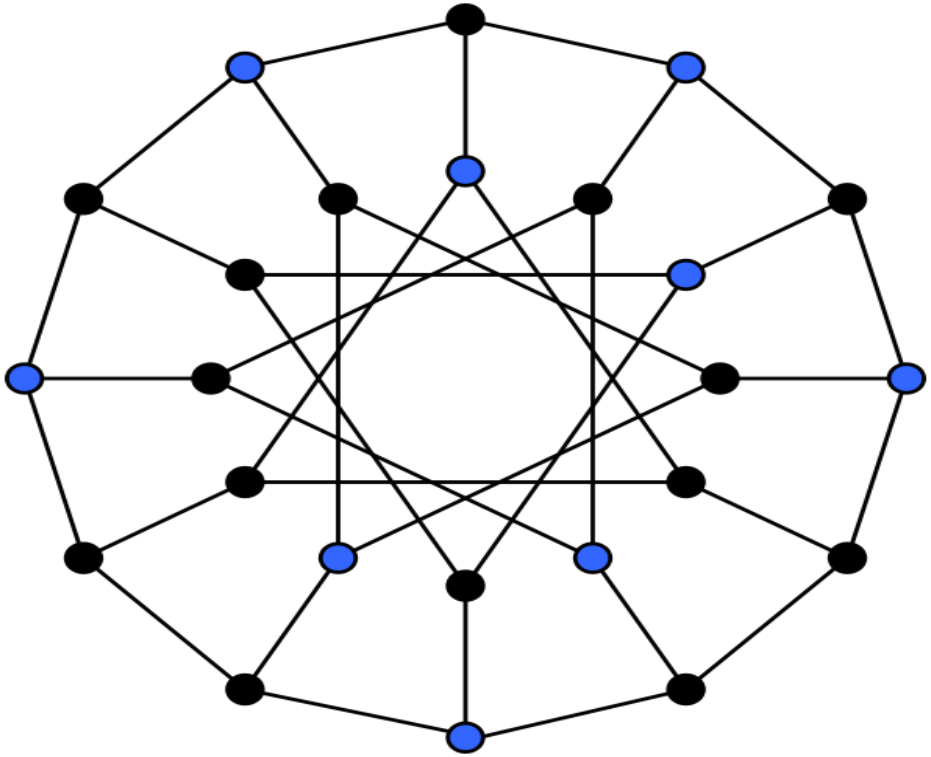
- Ορίζουμε έναν περιορισμό στο κόστος της κάθε λύσης.
- Οι λύσεις που ικανοποιούν τον περιορισμό είναι αποδεκτές (θεωρούνται λέξεις της γλώσσας).
- Θέτουμε ένα ανώτατο όριο Β στο κόστος της λύσης και ψάχνουμε να βρούμε αν υπάρχει λύση με κόστος το πολύ Β.
- Αν το πρόβλημα βελτιστοποίησης ανήκει στο $\mathcal{P}$, τότε και το πρόβλημα απόφασης ανήκει στο $\mathcal{P}$.

Ανεξάρτητο Σύνολο (1/2)

- Δεδομένων ενός μη κατευθυνόμενου γραφήματος G και ενός ακεραίου $K \geq 2$, υπάρχει υποσύνολο του C του V με $|C| \geq K$, τέτοιο ώστε για κάθε $v_i, v_j \in C$, **να μην υπάρχει** ακμή μεταξύ των v_i και v_j;

- Δεν έχει βρεθεί πολυωνυμικός αλγόριθμος.

Ανεξάρτητο Σύνολο (2/2)



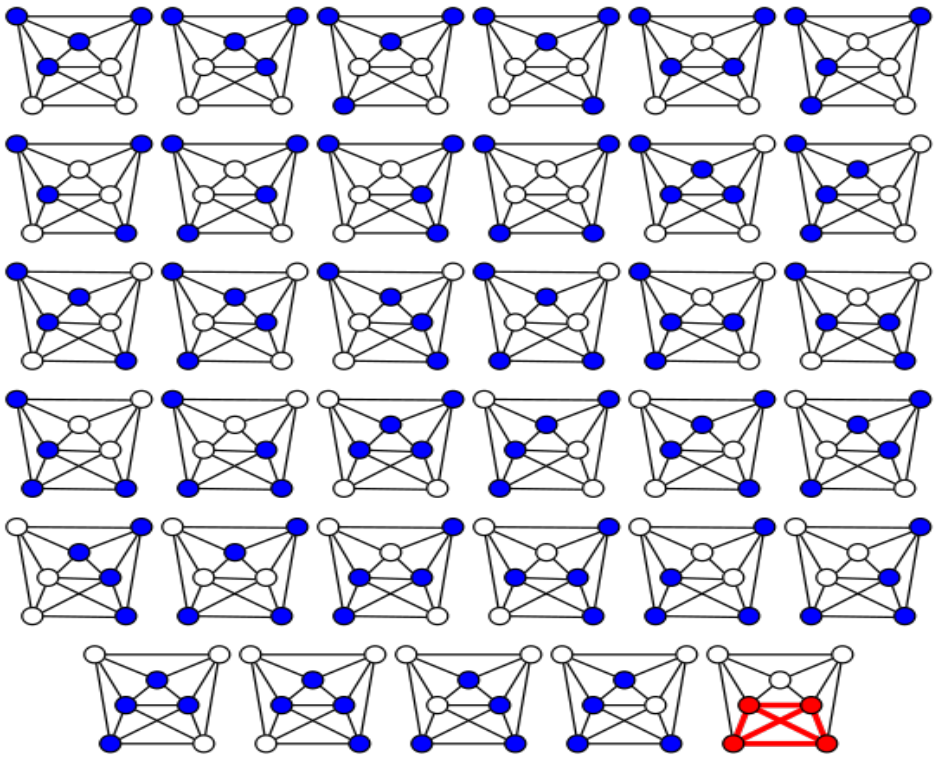
Πηγή:http://upload.wikimedia.org/wikipedia/commons/3/34/Independent_set_graph.svg

Κλίκα

- Δεδομένων ενός μη κατευθυνόμενου γραφήματος G και ενός ακεραίου $K \geq 2$, υπάρχει υποσύνολο C του V με $|C| \geq K$, τέτοιο ώστε για κάθε $v_i, v_j \in C$, **να υπάρχει** ακμή μεταξύ των v_i και v_j;

- Δεν έχει βρεθεί πολυωνυμικός αλγόριθμος.

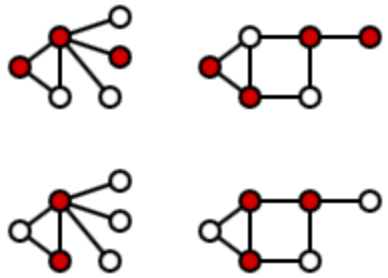
Κλίκα



Πηγή: http://en.wikipedia.org/wiki/File:Brute_force_Clique_algorithm.svg

Κάλυμμα κόμβων

- Ένα σύνολο κόμβων καλύπτει μια ακμή, αν περιλαμβάνει μια τουλάχιστον το ένα άκρο της.
- Δεδομένων ενός μη κατευθυνόμενου γραφήματος G και ενός ακεραίου Β ≥ 2, υπάρχει υποσύνολο του C του V με |C| ≤ K, τέτοιο ώστε το C να καλύπτει όλες τις ακμές του G ;
  - Σκεφτείτε το πρόβλημα της φρούρησης των διαδρόμων ενός μουσείου.



Διαμέριση ακεραίων

- Μας δίνεται ένα σύνολο n μη-αρνητικών ακεραίων, a_1, a_2, …, a_n. Μπορούμε να τους χωρίσουμε σε δύο ξένα υποσύνολα, έτσι ώστε οι ακέραιοι κάθε υποσυνόλου να έχουν το ίδιο άθροισμα;
  - Π.χ.: Έστω A={38,17,52,61,21,88,25}.
  - 38+52+61 = 17+21+88+25 = 151

Διαμέριση ακεραίων: Αλγόριθμος

- Έστω Η το ημιάθροισμα όλων των ακεραίων. Ψάχνουμε να βρούμε ένα υποσύνολο των ακεραίων που να αθροίζεται στο Η.
- Για $1 \leq i \leq n$, ορίζουμε το εξής σύνολο αριθμών:
  - $B(i)=\{b \leq H$: b είναι το άθροισμα ενός υποσυνόλου των αριθμών $\{a_1,\ldots,a_i\}\}$
- Υπολογίζουμε τα διάφορα b(i), από i=1 μέχρι n, μέχρι να εμφανιστεί ο αριθμός Η μέσα σε κάποιο b(i).

Παράδειγμα

- A = {38, 17, 52, 61, 21, 88, 25}
- H = 151
- B(0) = {0}
- B(1) = {0,38}
- B(2) = {0,17,38,55}
- B(3) = {0, 17, 38, 52, 55, 69, 90, 107}
- …
- B(7) = {0, 17, 21, …, 151}

Πολυπλοκότητα αλγορίθμου διαμέρισης

- Είναι εύκολο να αποδείξουμε ότι η πολυπλοκότητα του αλγορίθμου είναι O(nH).
- Ανήκει ο αλγόριθμος στο $\mathcal{P}$;
- Όχι, γιατί το μήκος της εισόδου είναι τάξης μεγέθους x=nlg(H), με αποτέλεσμα η πολυπλοκότητα να είναι εκθετική σε σχέση με το μήκος της εισόδου: $O(ne^{x/n})$.
- Αν ωστόσο υιοθετούσαμε μοναδιαία αναπαράσταση, η πολυπλοκότητα θα ήταν γραμμική ως προς το μέγεθος της εισόδου.

Τύποι Bool

- Έστω $X=\{x_1,x_2,\ldots,x_n\}$ ένα πεπερασμένο σύνολο από μεταβλητές Bool, και έστω $X'=\{x'_1, x'_2,\ldots, x'_n\}$ οι αρνήσεις τους.
- Ονομάζουμε τα μέλη του $X\cup X'$ στοιχεία.
  - Θετικά στοιχεία και αρνητικά στοιχεία.
- Μια συνθήκη C είναι ένα μη κενό σύνολο στοιχείων $C\subseteq X\cup X'$.
- Ένας τύπος Bool σε κανονική συζευκτική μορφή είναι ένα σύνολο συνθηκών.

Παράδειγμα

- Έστω $X=\{x_1,x_2,x_3\}$ και άρα $X'=\{x'_1,x'_2,x'_3\}$.
- Μια συνθήκη είναι η:
  - $C=\{x_1 \vee x'_2\}$
- Ένας τύπος Bool είναι ο:
  - $F=\{(x_1 \vee x'_2 \vee x_3), (x'_1), (x_2 \vee x'_2)\}$
- Απόδοση τιμών αληθείας είναι μια απεικόνιση από το X στο σύνολο {T,F} (T=true, F=false).
- **Ικανοποιήσιμος τύπος**.
  - x_1=F, x_2=T, x_3=T

Το πρόβλημα της ικανοποιησιμότητας

- Μη ικανοποιήσιμος τύπος:
  - $F = \{(x_1 \vee x_2 \vee x_3),(x'_1 \vee x_2),(x'_2 \vee x_3),(x'_3 \vee x_1),(x'_1 \vee x'_2 \vee x'_3)\}$

- Το πρόβλημα της ικανοποιησιμότητας:
  - Δεδομένου ενός τύπου Bool, είναι αυτός ικανοποιήσιμος;

2-SAT

- Ειδική περίπτωση του προβλήματος της ικανοποιησιμότητας:
  - Οι συνθήκες έχουν το πολύ δύο στοιχεία
- $F=\{(x_1 \vee x_2),(x_3 \vee x'_2),(x_1),(x'_1 \vee x'_2),(x_3 \vee x_4),(x'_3 \vee x_5),$
  $(x'_4 \vee x'_5),(x_4 \vee x'_3)\}$

- Το πρόβλημα 2-SAT ανήκει στο $\mathcal{P}$.

Η Κλάση $\mathcal{NP}$

Προβλήματα που δεν ανήκουν στην $\mathcal{P}$

- Αποφασίσιμη εκδοχή του προβλήματος του τερματισμού:
  - E={«M»«w» : Η M δέχεται την είσοδο w μετά από το πολύ $2^{|w|}$ βήματα}
- Η E δεν ανήκει στην $\mathcal{P}$.
- Άλλα προβλήματα που δεν ανήκουν στο $\mathcal{P}$:
  - Κύκλος Hamilton, περιοδεύων πωλητής, ανεξάρτητο σύνολο, διαμέριση, ικανοποιησιμότητα, ...

Η κλάση $\mathcal{NP}$

- Μια μη-ντετερμινιστική μηχανή Turing M λέγεται πολυωνυμικά φραγμένη αν υπάρχει πολυώνυμο p(n) τέτοιο ώστε για κάθε είσοδο x να μην υπάρχει συνολική κατάσταση C της M, τέτοια ώστε:
  - $(s,\#x\underline{\#}) \vdash^{p(|x|)+1} C$
- Ορίζουμε ως $\mathcal{NP}$ (non-deterministic polynomial) την κλάση όλων των γλωσσών που αποφασίζονται από μια πολυωνυμικά φραγμένη μη-ντετερμινιστική μηχανή Turing.

Ικανοποιησιμότητα

- Έστω μια μηχανή Μ που εκτελεί τους εξής υπολογισμούς:
  - Γράφει στην ταινία μη-ντετερμινιστικά μια ανάθεση τιμών στις μεταβλητές Bool.
  - Ελέγχει την ανάθεση.
- Κάθε ακολουθία υπολογισμών είναι φραγμένη.
- Το πρόβλημα της ικανοποιησιμότητας ανήκει στην $\mathcal{NP}$.

Περιοδεύων πωλητής

- Με δεδομένο «προϋπολογισμό» Β.
- Έστω μια μηχανή Μ που εκτελεί τους εξής υπολογισμούς:
  - Γράφει στην ταινία μη-ντετερμινιστικά μια μετάθεση των πόλεων.
  - Ελέγχει την μετάθεση.
- Κάθε ακολουθία υπολογισμών είναι φραγμένη.
- Το πρόβλημα του περιοδεύοντος πωλητή ανήκει στην $\mathcal{NP}$.

Ιδιότητες της $\mathcal{NP}$

- $\mathcal{P} \subseteq \mathcal{NP}$
- Τα δένδρα που αναπαριστούν το σύνολο των υπολογισμών μιας πολυωνυμικά φραγμένης μη-ντετερμινιστικής μηχανής Turing μπορεί να έχουν εκθετικά πολλά κλαδιά, αλλά όλα με μέτριο βάθος.
- Η προσομοίωση μιας πολυωνυμικά φραγμένης μη-ντετερμινιστικής μηχανής Turing από μια ντετερμινιστική μηχανή Turing απαιτεί εκθετικά μεγάλο αριθμό βημάτων.

Η κλάση $\mathcal{EXP}$

- Μια ντετερμινιστική μηχανή Turing M ονομάζεται εκθετικά φραγμένη αν υπάρχει πολυώνυμο p(n) τέτοιο ώστε για κάθε είσοδο x να μην υπάρχει κατάσταση C τέτοια ώστε:
  - $(s,\#x\underline{\#}) \vdash^{2^{p(|x|)}+1} C$
- Ορίζουμε ως $\mathcal{EXP}$ την κλάση όλων των γλωσσών που αποφασίζονται από μια εκθετικά φραγμένη ντερμινιστική μηχανή Turing.

Ιεραρχία κλάσεων

- Αν μια γλώσσα ανήκει στην $\mathcal{NP}$, τότε ανήκει και στην $\mathcal{EXP}$.
- Γενικότερα ισχύει:
  - $\mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{EXP}$
- Γνωρίζουμε ωστόσο πως:
  - $\mathcal{P} \subset \mathcal{EXP}$
- Δεν έχει αποδειχθεί κάποιο από τα :
  - $\mathcal{P} \subset \mathcal{NP}$
  - $\mathcal{NP} \subset \mathcal{EXP}$

Πιστοποιητικά

- Οι μη-ντετερμινιστικές πολυωνυμικά φραγμένες μηχανές Turing της κλάσης $\mathcal{NP}$ λειτουργούν ως εξής:
  - Δημιουργούν υποψήφιες λύσεις.
  - Τις ελέγχουν.
- Ονομάζουμε «πιστοποιητικό» (certificate) μια τέτοια συμβολοσειρά που **είναι λύση**.
- Ένα πιστοποιητικό πρέπει να είναι πολυωνυμικά σύντομο και να μπορεί να ελεγχθεί σε πολυωνυμικό χρόνο.
- Όλα τα προβλήματα του $\mathcal{NP}$ έχουν πιστοποιητικά και μόνο αυτά.

ανοικτάμαθήματα
opencourses

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης