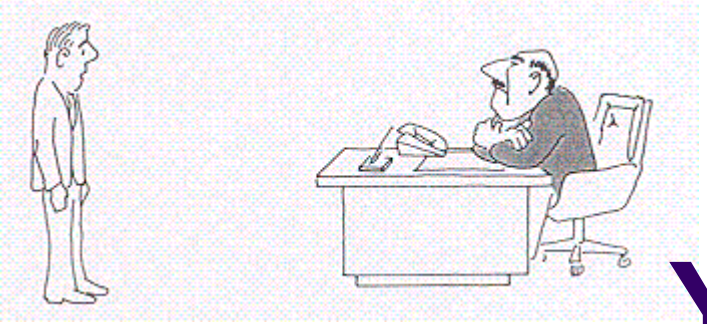
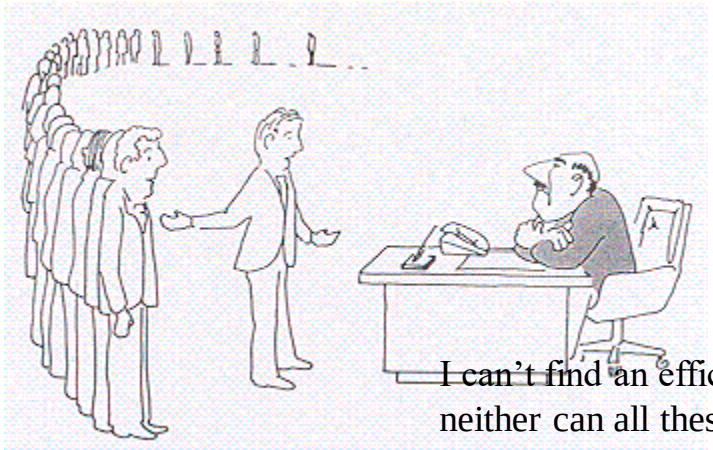


I can’t find an efficient algorithm, I guess I am just too dumb

Υπολογιστική Πολυπλοκότητα

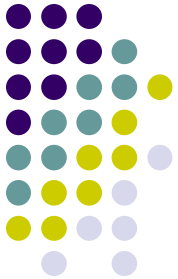
NP-Πληρότητα

I can’t find an efficient algorithm, because no such algorithm is possible



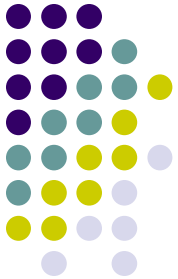
I can’t find an efficient algorithm, but neither can all these famous people

Ανακεφαλαίωση: *P*



- Μερικά προβλήματα είναι αποδεδειγμένα επιλύσιμα σε πολυωνυμικό χρόνο σε έναν κανονικό υπολογιστή.
  - Αυτά τα προβλήματα ανήκουν στην κλάση ***P***
  - Στην ουσία είναι ένας Η/Υ με άπειρη μνήμη
  - *Πώς αποδεικνύουμε ότι ένα πρόβλημα είναι στο* ***P****?*

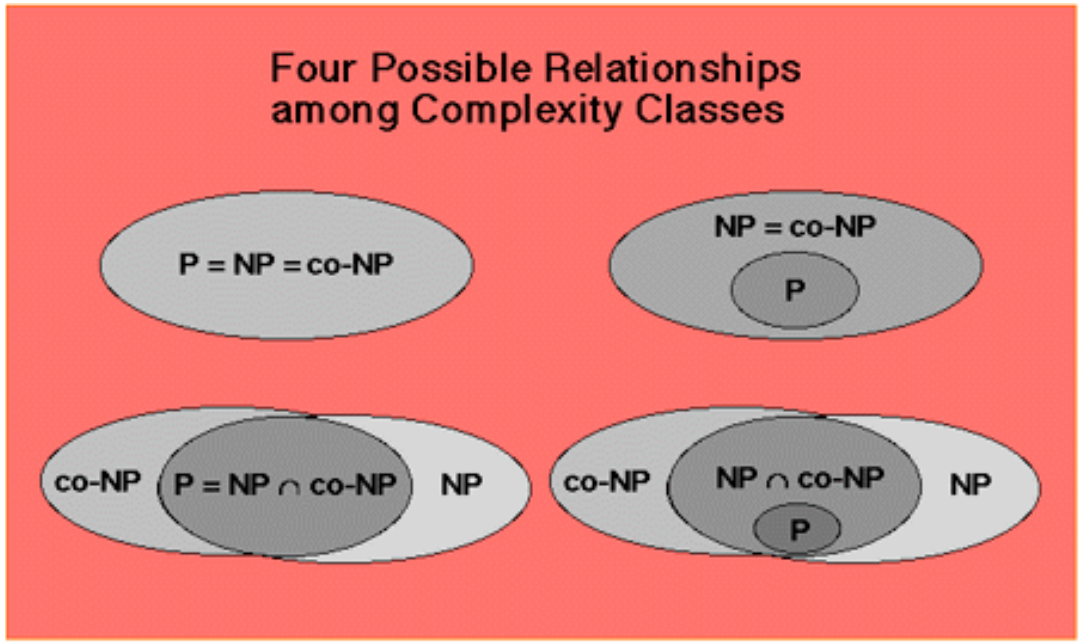
Ανακεφαλαίωση: *NP*



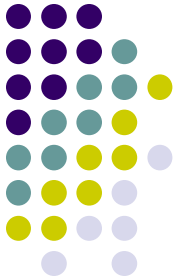
- Μερικά προβλήματα είναι αποδεδειγμένα επιλύσιμα σε πολυωνυμικό χρόνο σε έναν ανταιτιοκρατικό Η/Υ
  - Αυτά τα προβλήματα ανήκουν στην κλάση ***NP***
  - Μπορούμε να φανταστούμε έναν ανταιτιοκρατικό Η/Υ σαν μία παράλληλη μηχανή που μπορεί να τρέχει παράλληλα άπειρες διεργασίες
  - *Πώς αποδεικνύουμε ότι ένα πρόβλημα είναι στο* ***NP;***

Ανακεφαλαίωση: *P* και *NP*

- ***P*** = επίλυση σε πολυωνυμικό χρόνο
- ***NP*** = επαλήθευση σε πολυωνυμικό χρόνο
- ***co-NP*** = επαλήθευση αντιπαραδείγματος σε πολυωνυμικό χρόνο



Αναγωγιμότητα Πολυωνυμικού Χρόνου



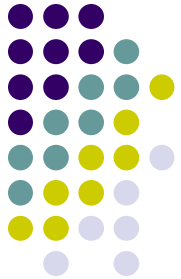
Ορισμός: Μία συνάρτηση

$$f : \Sigma^* \to \Sigma^*$$

Είναι υπολογίσιμη σε πολυωνυμικό χρόνο αν υπάρχει αιτιοκρατική TM που

- ξεκινά με είσοδο w, και
- τερματίζει έπειτα από ***πολυωνυμικό*** πλήθος βημάτων με έξοδο $f(w)$ στην ταινία.

Πολυωνυμικού Χρόνου Αναγωγή



Ορισμός: Ένα πρόβλημα A είναι απεικονιστικά αναγώγιμο σε πολυωνυμικό χρόνο στο B:

$$A \leq_P B$$

αν υπάρχει συνάρτηση πολυωνυμικού χρόνου

$$f : \Sigma^* \to \Sigma^*$$

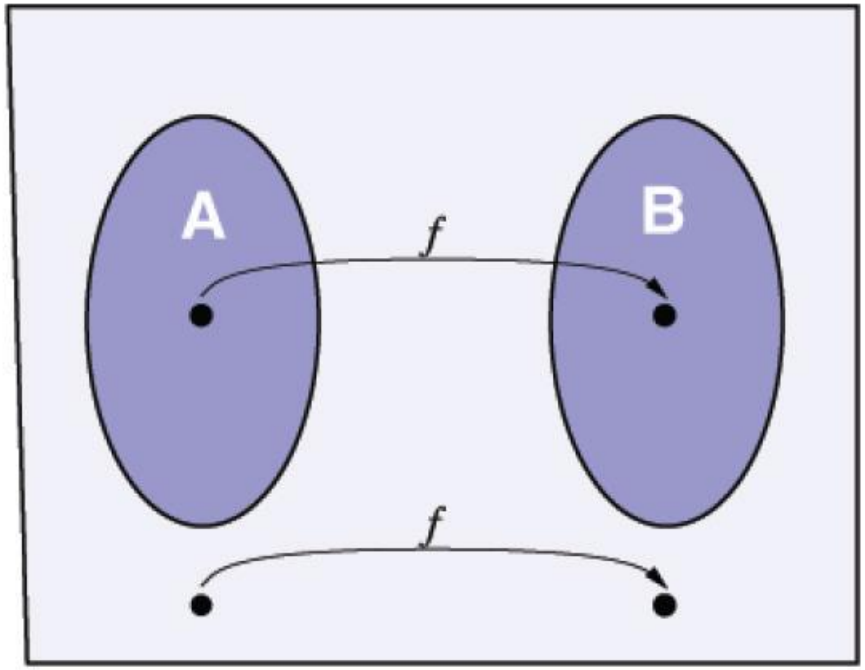
έτσι ώστε για κάθε w,

$$w \in A \Leftrightarrow f(w) \in B.$$

Η συνάρτηση f καλείται πολυωνυμικού χρόνου αναγωγή της A στο B.

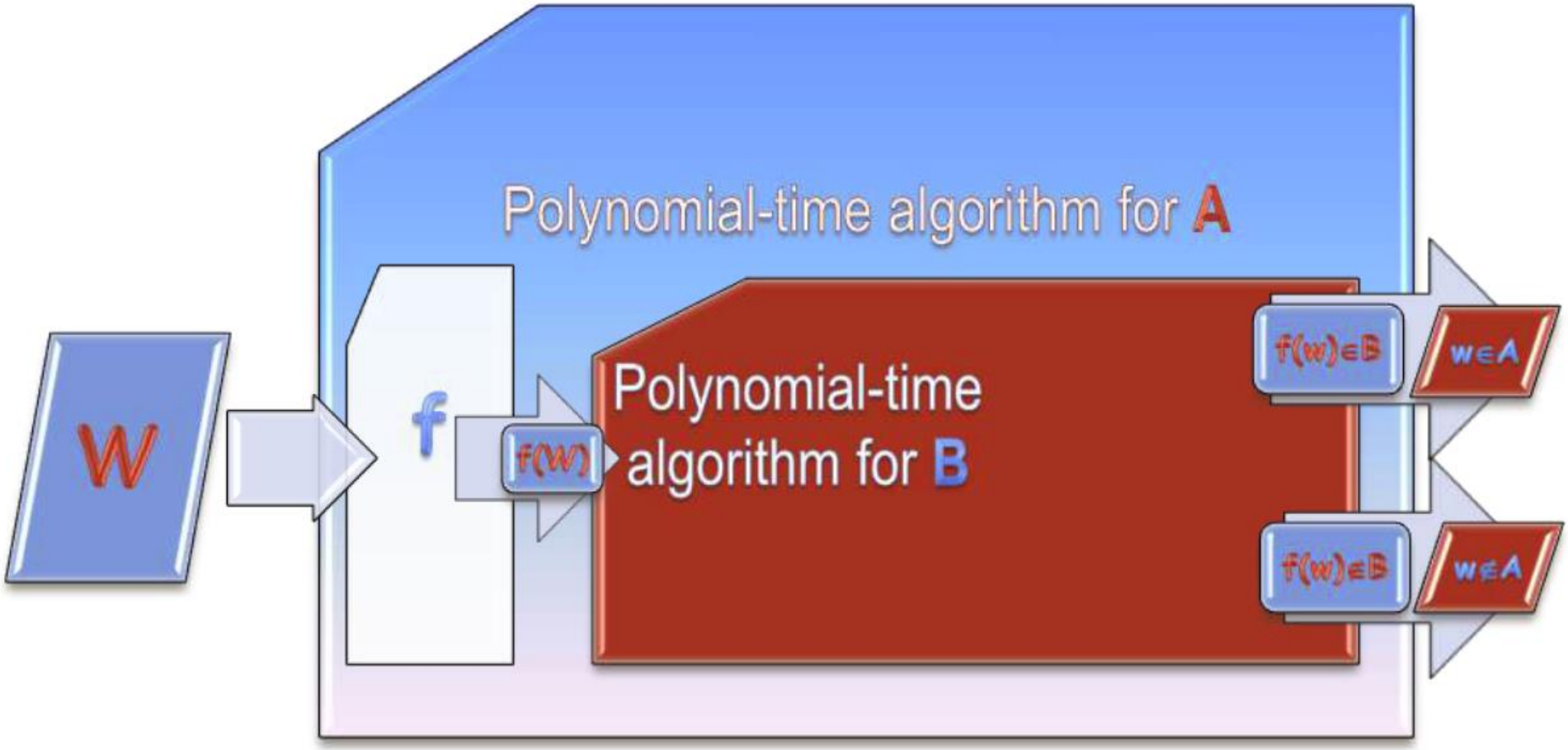
Πολυωνυμικού Χρόνου Αναγωγή

Μετατρέπει ερωτήσεις συμμετοχής στο A σε ερωτήσεις συμμετοχής στο B, με ***αποδοτικό*** τρόπο.



Αναγωγή για την Κλάση *P*

Θεώρημα: Αν $A \leq_P B$ και $B \in P$ τότε $A \in P$.



Αναγωγή για την Κλάση P

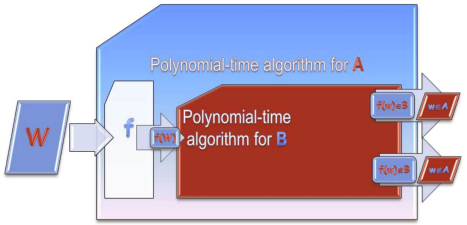
Θεώρημα: Αν $A \leq_P B$ και $B \in P$ τότε $A \in P$.

Απόδειξη:

- Έστω f η αναγωγή από το A στο B, που υπολογίζεται από την ΤΜ M_f .
  - Σε είσοδο w μήκους n, η M_f απαιτεί το πολύ $c_1 n^{a1}$ βήματα.
- M μία ΤΜ πολυωνυμικού χρόνου για το B.
  - Σε είσοδο y μήκους m, η M απαιτεί το πολύ $c_2 m^{a2}$ βήματα.

Αναγωγή για την Κλάση *P*

Ορίζουμε την N: σε είσοδο w



1. Υπολόγισε $f(w)$
2. Τρέξε την M σε είσοδο $f(w)$ και η έξοδος είναι αυτή της M

Ανάλυση:

- Σε είσοδο w μήκους n, ο υπολογισμός $y = f(w)$ απαιτεί το πολύ $c_1 n^{a1}$ βήματα.
- Σε είσοδο y μήκους $m = c_1 n^{a1}$, η M απαιτεί το πολύ $c_2 m^{a2} = c_2 (c_1 n^{a1})^{a2} = (c_2 {c_1}^{a2}) n^{a1 \cdot a2}$ βήματα.
- Και τα δύο στάδια απαιτούν πολυωνυμικό χρόνο ως προς n.
- Άρα $A \in P$.

Αληθευσιμότητα

Μία λογική μεταβλητή παίρνει τιμές:

- ΑΛΗΘΕΣ (1), και ΨΕΥΔΕΣ (0).

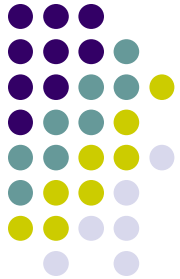
Λογικές Πράξεις:

- ΚΑΙ: $\wedge$
- Η: $\vee$
- ΟΧΙ: $\neg$

Παραδείγματα:

- $0 \wedge 1 = 0$
- $0 \vee 1 = 1$
- $\neg 0 = 1$

Αληθευσιμότητα



Ένας λογικός τύπος είναι μία έκφραση των λογικών μεταβλητών και πράξεων.

$$\varphi = (x \wedge y) \vee (x \wedge z)$$

Ορισμός: Ένας λογικός τύπος είναι αληθεύσιμος αν υπάρχει κάποιος συνδυασμός από 0 και 1 έτσι ώστε η έκφραση να είναι 1.

Αληθευσιμότητα

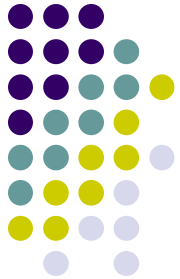
$\varphi = (x \wedge y) \vee (x \wedge \neg z)$

Είναι αληθεύσιμος από την τιμοδοσία:

- $x = 0$
- $y = 1$
- $z = 0$

Αυτή η τιμοδοσία είναι αληθοποιός για την έκφραση φ.

Το Πρόβλημα της Αληθευσιμότητας

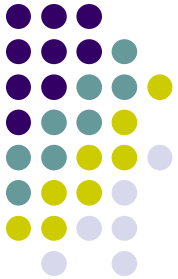


SAT = {⟨φ⟩ | φ είναι ένας αληθεύσιμος λογικός τύπος}

Ασχολούμαστε με συγκεκριμένη μορφή:

- Ένα λεξίγραμμα είναι μία μεταβλητή ή η συμπληρωματική της: x ή $\neg x$.
- Μία φράση είναι λεξιγράμματα που συνδέονται με διάζευξη ($\vee$): $(x_1 \vee x_2 \vee x_3)$
- Ένας λογικός τύπος είναι σε Κανονική Συζευκτική Μορφή (CNF) αν αποτελείται από φράσεις συνδεόμενες με συζεύξεις ($\wedge$).
- Παράδειγμα: $(x_1 \vee x_2 \vee x_3 \vee x_4) \wedge (x_3 \vee x_5 \vee x_6) \wedge (x_3 \vee x_6)$

Αληθευσιμότητα



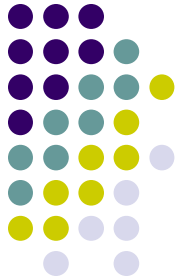
Ορισμός: Ένας λογικός τύπος είναι σε μορφή $_3$CNF αν είναι CNF μορφή, και όλες οι φράσεις έχουν ακριβώς 3 λεξιγράμματα.

$$(x_1 \vee x_2 \vee x_3) \wedge (x_3 \vee x_5 \vee x_6) \wedge (x_3 \vee x_6 \vee x_4)$$

$_3$SAT = $\{\langle \varphi \rangle \mid \varphi$ είναι αληθεύσιμος λογικός τύπος $_3$CNF$\}$

Αν ο φ είναι αληθεύσιμος $_3$CNF τύπος, τότε για κάθε τέτοια τιμοδοσία του φ, κάθε φράση θα περιέχει τουλάχιστον ένα λεξίγραμμα που είναι 1.

Αναγωγή



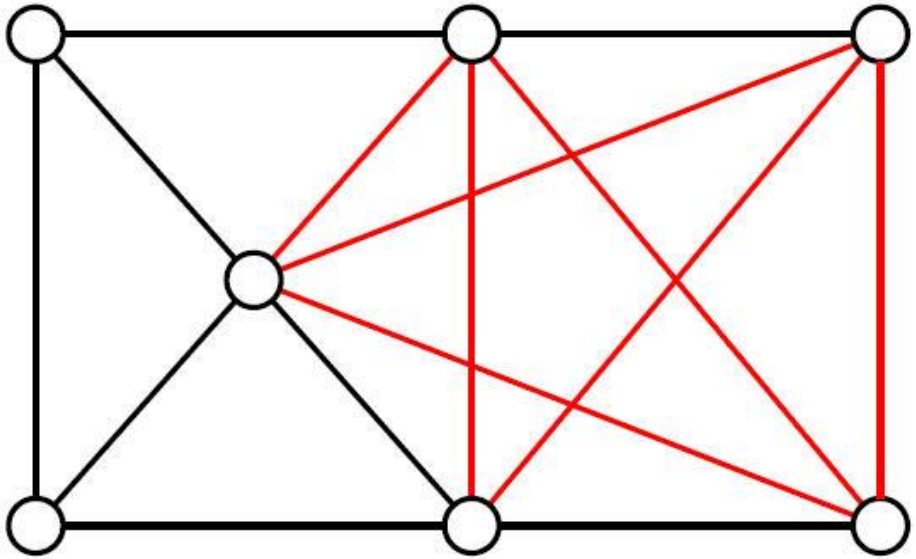
Ισχυρισμός: Υπάρχει πολυωνυμική αναγωγή από το ${}_3$SAT στην ΚΛΙΚΑ. Με άλλα λόγια:

$$ {}_3\text{SAT} \leq_P \text{CLIQUE} $$

Θα κατασκευάσουμε μία πολυωνυμική αναγωγή f που απεικονίζει έναν ${}_3$CNF λογικό τύπο φ σε ένα γράφημα G και έναν αριθμό k.

Η συνάρτηση f έχει τη ιδιότητα ότι η φ είναι αληθεύσιμη αν και μόνο αν το γράφημα G έχει κλίκα μεγέθους k.

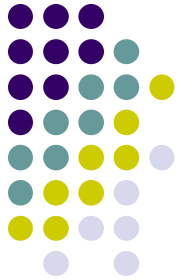
Παράδειγμα: Κλίκα



Η κλίκα σε ένα γράφημα είναι ένα υπογράφημα όπου μεταξύ κάθε ζευγαριού κόμβων υπάρχει μία ακμή.

Μία k-κλίκα είναι μία κλίκα μεγέθους k. Για παράδειγμα, το γράφημα παραπάνω έχει μία 5-κλίκα.

${}_3SAT \leq_P$ ΚΛΙΚΑ



Έστω φ ένας ${}_3CNF$ λογικός τύπος με k φράσεις.

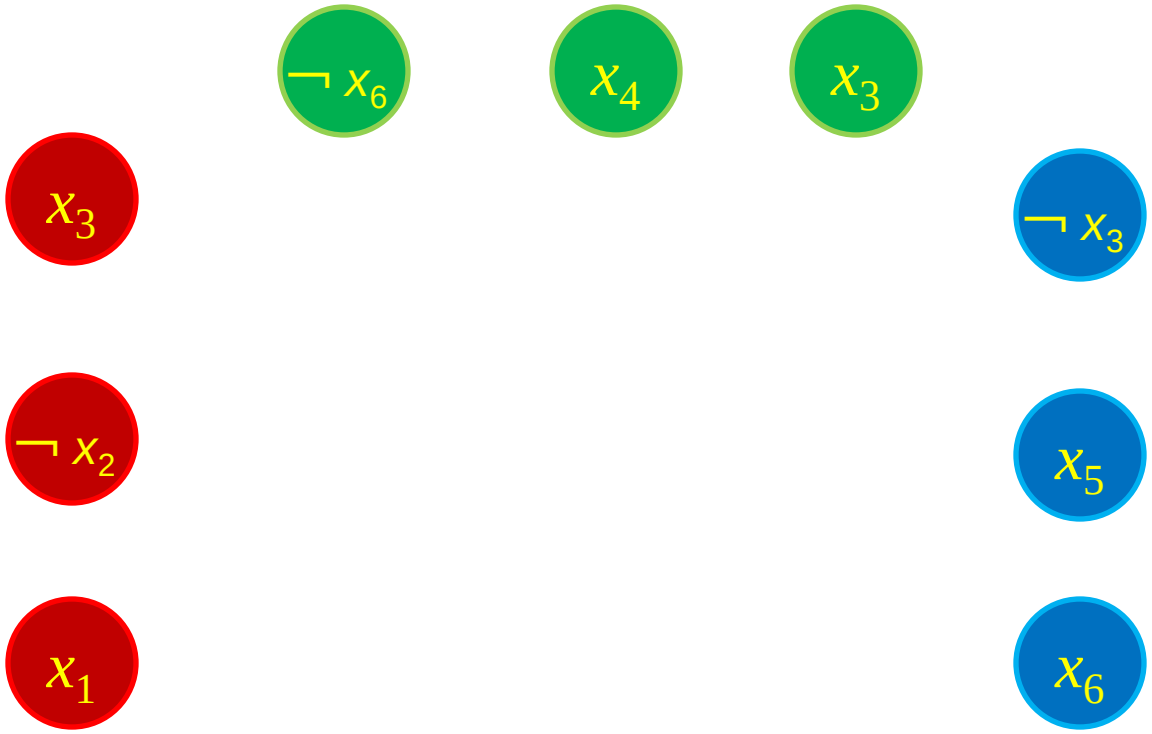
$$(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_3 \vee x_5 \vee x_6) \wedge (x_3 \vee \neg x_6 \vee x_4)$$

Ορίζουμε το γράφημα ως εξής:

- Οι κόμβοι του G οργανώνονται σε τριάδες $t_1, \ldots, t_k$.
- Κάθε τριάδα αντιστοιχεί σε μία φράση
- Κάθε κόμβος σε μία τριάδα αντιστοιχεί σε ένα λεξίγραμμα.

Παράδειγμα

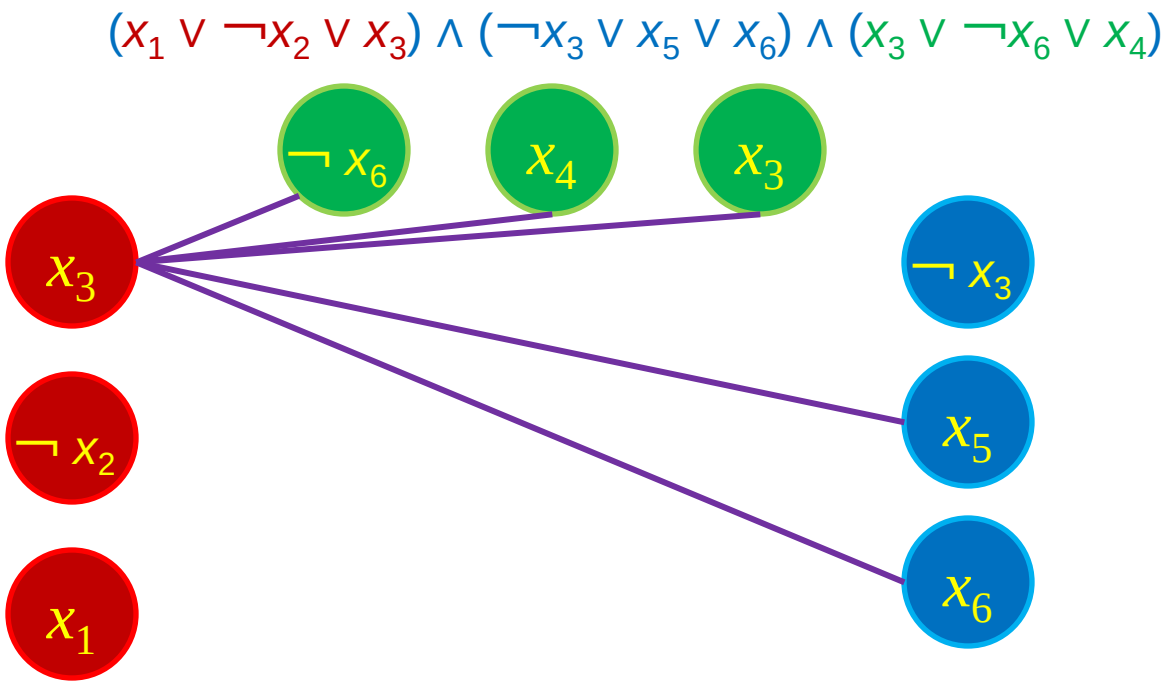
$(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_3 \vee x_5 \vee x_6) \wedge (x_3 \vee \neg x_6 \vee x_4)$



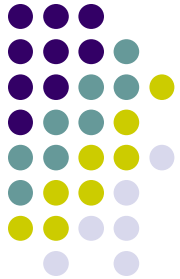
$_3$SAT $\leq_P$ ΚΛΙΚΑ

Πρόσθεσε ακμές μεταξύ όλων των ζευγαριών κορυφών εκτός:

- Αν ανήκουν στην ίδια τριάδα
- Μεταξύ αντίθετων λεξιγραμμάτων



${}_3SAT \leq_P$ ΚΛΙΚΑ



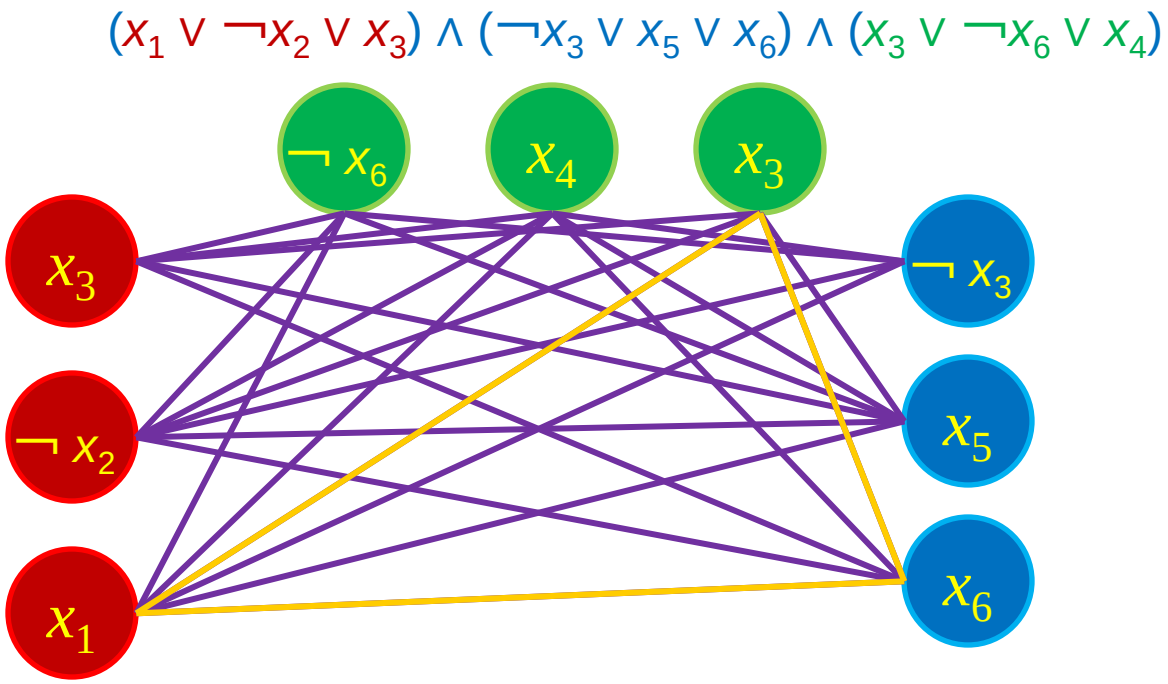
Αν η φ είναι αληθεύσιμη, τότε η G έχει μία k-κλίκα.

Έστω ότι η φ είναι αληθεύσιμη.

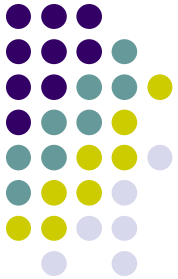
- Τουλάχιστον ένα λεξίγραμμα είναι ΑΛΗΘΕΣ σε κάθε φράση
- σε κάθε τριάδα επέλεξε ένα κόμβο με ΑΛΗΘΕΣ λεξίγραμμα
- Αυτές συνδέονται με ακμές που αποδίδουν μία k-κλίκα

$_3$SAT $\leq_P$ ΚΛΙΚΑ

Αν η φ είναι αληθεύσιμη τότε ο G έχει k-κλίκα.



$_3$SAT $\leq_P$ ΚΛΙΚΑ

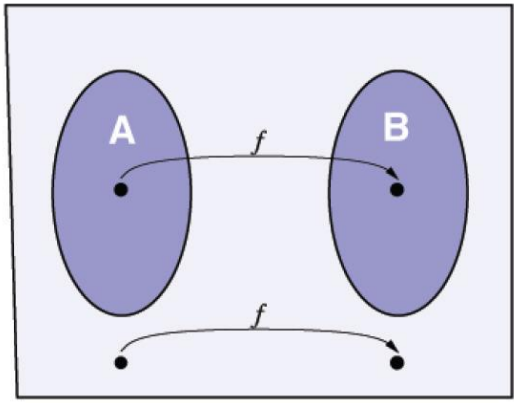


Αν η G έχει μία k-κλίκα, η φ είναι αληθεύσιμη.

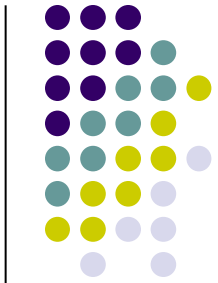
- Κανένα ζευγάρι κόμβων δεν είναι στην ίδια τριάδα.
- Έχει k κορυφές και k φράσεις, και άρα
- κάθε τριάδα έχει ακριβώς ένα κόμβο κλίκας
- Δίνουμε 1 σε κάθε κόμβο της κλίκας
- Δεν υπάρχει αντίφαση

${}_3SAT \leq_P$ ΚΛΙΚΑ

- Κατασκευάσαμε μία υπολογίσιμη σε πολυωνυμικό χρόνο συνάρτηση f.
- Δείξαμε ότι η συνάρτηση f έχει την ιδιότητα ότι ο $\varphi \in {}_3SAT$ αν και μόνο αν $f(\varphi) \in$ ΚΛΙΚΑ.
- Άρα η f είναι μία αναγωγή από το ${}_3SAT$ στην ΚΛΙΚΑ και άρα ${}_3SAT \leq_P$ ΚΛΙΚΑ



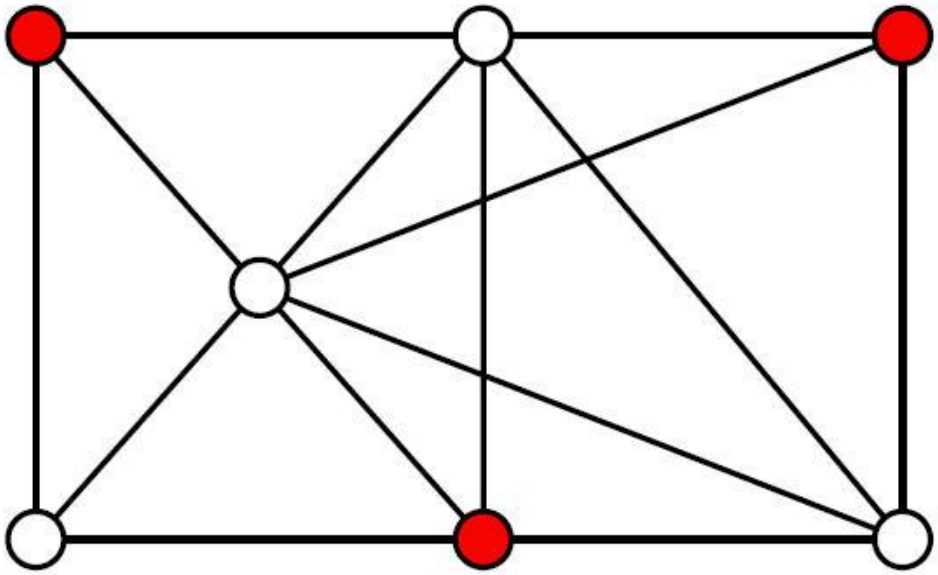
Αναγωγές



- Σκέψη για κατανόηση της δομής και των δύο προβλημάτων
- Εύρεση «εξαρτήματος» που εκμεταλλεύεται αυτή τη δομή (δομές που μπορούν να προσομοιώσουν τις φράσεις και μεταβλητές του $_3$SAT αν κάνω από εκεί αναγωγή)
- Γενικά είναι δύσκολα προβλήματα

Ανεξάρτητο Σύνολο

- Ένα ανεξάρτητο σύνολο σε ένα γράφημα είναι ένα σύνολο κορυφών έτσι ώστε κανένα ζευγάρι κορυφών να μην είναι γειτονικές
- Υπάρχει ανεξάρτητο σύνολο μεγέθους k;



Ανεξάρτητο Σύνολο

ΑΝΕΞΑΡΤΗΤΟ_ΣΥΝ = $\{\langle G,k\rangle \mid G$ περιέχει ανεξάρτητο σύνολο μεγέθους $k\}$

Το ΑΝΕΞΑΡΤΗΤΟ_ΣΥΝ είναι πολυωνυμικά αναγώγιμο στην ΚΛΙΚΑ

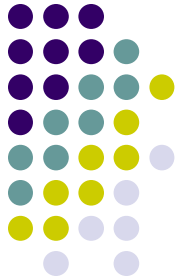
ΑΝΕΞΑΡΤΗΤΟ-ΣΥΝ $\leq_P$ ΚΛΙΚΑ

και αντίστροφα :

ΚΛΙΚΑ $\leq_P$ ΑΝΕΞΑΡΤΗΤΟ-ΣΥΝ

Ισχύει πάντα αυτό;

Ανεξάρτητο Σύνολο



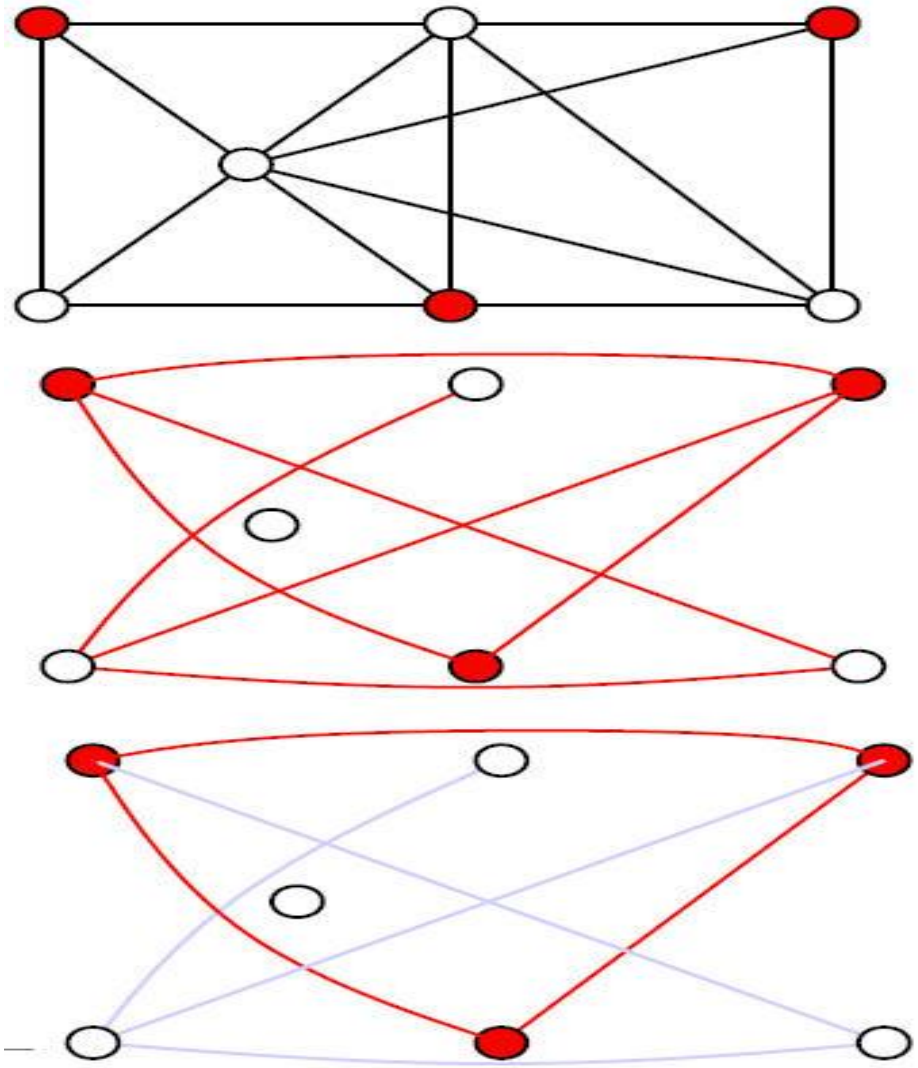
Το συμπλήρωμα του γραφήματος $G = (V,E)$ είναι ένα γράφημα:

$G^c = (V,E^c)$, όπου:

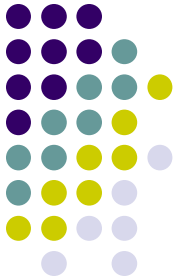
$$E^c = \{(v_1, v_2) | v_1, v_2 \in V \text{ και } (v_1, v_2) \notin E\}$$

Αν το V είναι ένα ανεξάρτητο σύνολο στο G, τότε ο V είναι κλίκα στο G^c. (και αντίστροφα)

Παράδειγμα



ΑΝΕΞΑΡΤΗΤΟ-ΣΥΝ $\leq_p$ ΚΛΙΚΑ



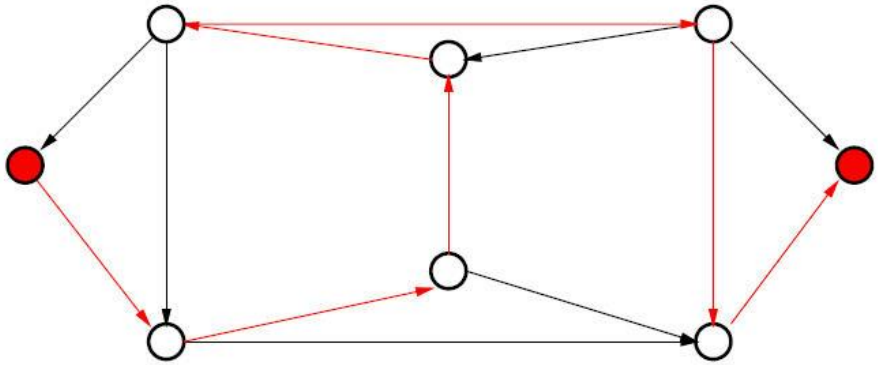
Αναγωγή: Έστω ζεύγος $\langle G,k\rangle$. Κατασκευάζουμε το $\langle G^c,k\rangle$ σε πολυωνυμικό χρόνο.

$\Rightarrow$ Αν $\langle G,k\rangle \in$ ΑΣ τότε υπάρχει ανεξάρτητο σύνολο μεγέθους k στο γράφημα G. Αυτοί οι κόμβοι ανά δύο δεν συνδέονται μεταξύ τους και άρα στο G^c θα συνδέονται ανά δύο μεταξύ τους. Άρα κλίκα μεγέθους k και άρα $\langle G^c,k\rangle \in$ ΚΛΙΚΑ.

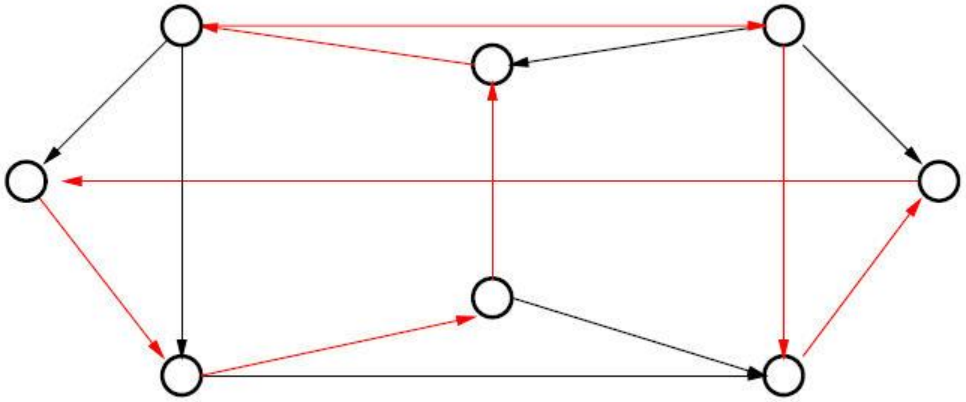
$\Leftarrow$ Αν $\langle G^c,k\rangle \in$ ΚΛΙΚΑ τότε υπάρχει κλίκα μεγέθους k στο γράφημα G^c. Αυτοί οι κόμβοι ανά δύο συνδέονται μεταξύ τους και άρα στο G δεν θα συνδέονται ανά δύο μεταξύ τους. Άρα έχουμε ανεξάρτητο σύνολο μεγέθους k και άρα $\langle G,k\rangle \in$ ΑΣ.

Hamiltonian Μονοπάτι - Κύκλος

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



Ένας Hamiltonian κύκλος είναι ένα Hamiltonian μονοπάτι που η αρχή και το τέλος συμπίπτουν.



Hamiltonians

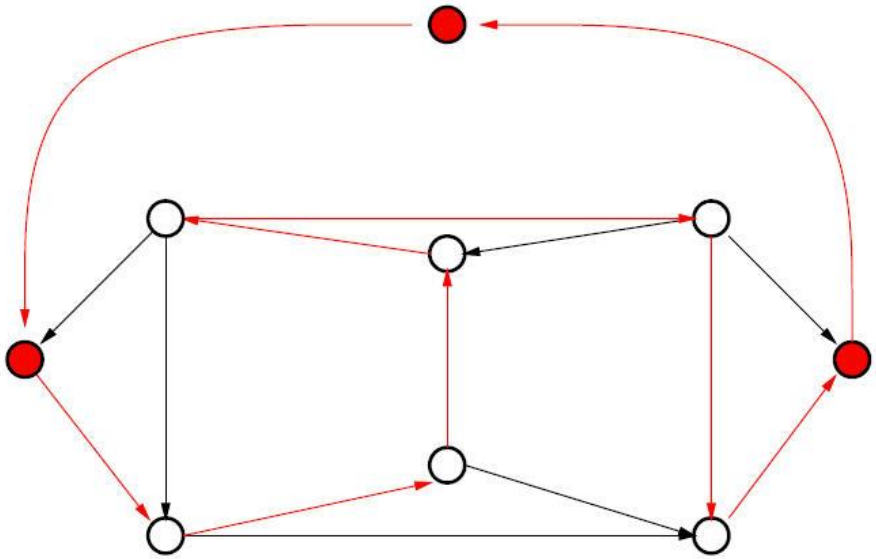
HAMPATH = {⟨*G*, *s*, *t*⟩ |ο *G* έχει Hamiltonian μονοπάτι από τον *s* στο *t*}

HAMCIRCUIT = {⟨*G*⟩ | ο *G* έχει Hamiltonian κύκλο}

Θεώρημα:

HAMPATH $\leq_P$ HAMCIRCUIT

HAMCIRCUIT $\leq_P$ HAMPATH



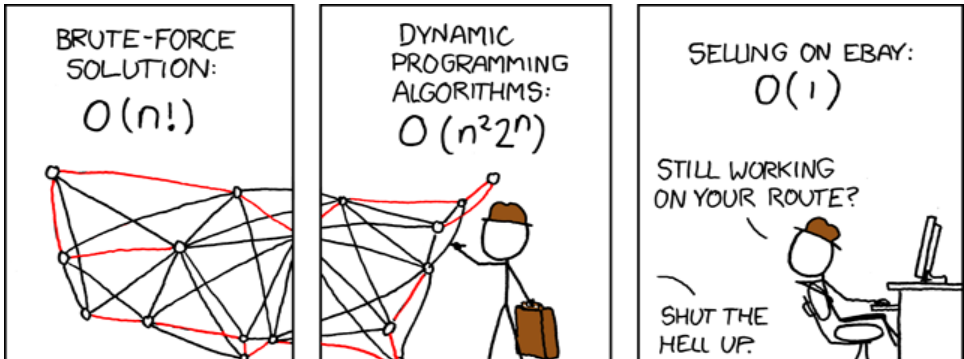
Πρόβλημα Περιοδεύοντος Πωλητή (TSP)

Παράμετροι:

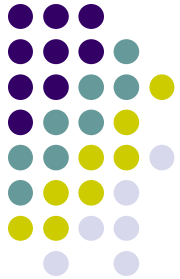
- Σύνολο πόλεων C
- Σύνολο αποστάσεων μεταξύ πόλεων D
- Στόχος k

Τυπικά:

- Κατευθυντό γράφημα $G=(C,D)$
- Οι ακμές έχουν βάρη
- Πλήρες γράφημα G
- Στόχος k



Πρόβλημα Περιοδεύοντος Πωλητή (TSP)



TSP = {⟨C, D, k⟩ | το (C,D) έχει πορεία από όλες τις πόλεις μία και μόνο μία φορά συνολικής απόστασης ≤ k}

HAMCIRCUIT = {⟨G⟩ | ο G έχει ένα Hamiltonian κύκλο}

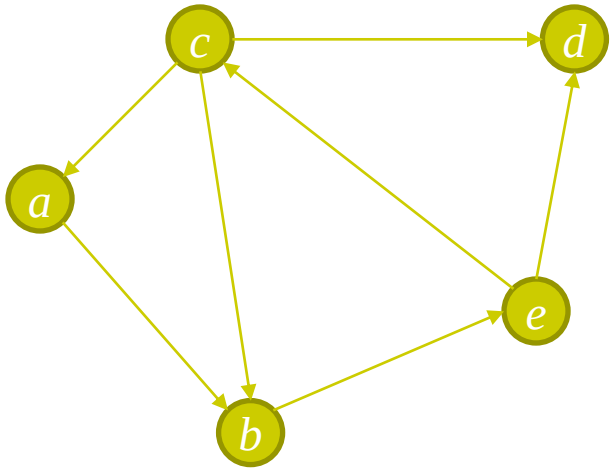
$$\text{HAMCIRCUIT} \leq_P \text{TSP}$$

Αναγωγή: Δοθέντος ενός κατευθυντού γραφήματος G=(V,E) κατασκευάζουμε στιγμιότυπο TSP. Οι πόλεις είναι ίδιες με τους κόμβους του G, $C = V$.

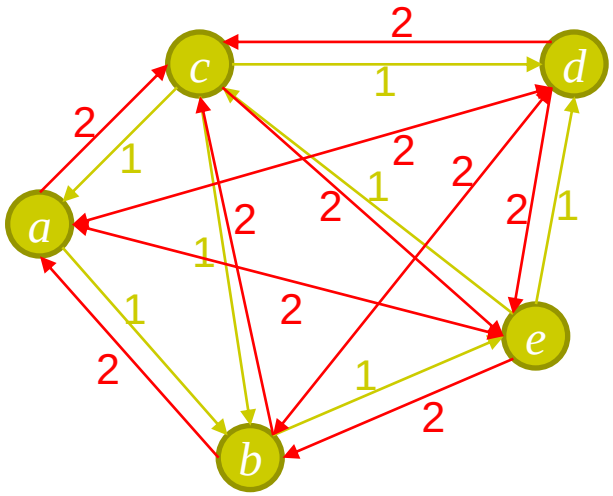
Η απόσταση από το v_1 στο v_2 είναι 1 αν $(v_1, v_2) \in E$, και 2 διαφορετικά.

Το φράγμα για την συνολική απόσταση είναι $k = |V|$.

Η Αναγωγή (1)



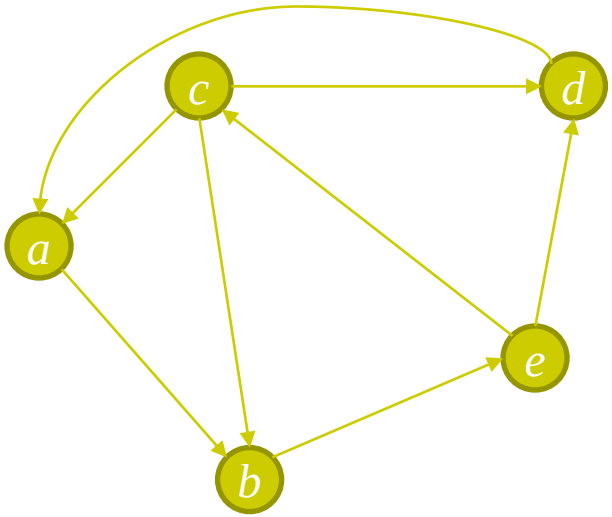
Αναγωγή



Δεν έχει Hamiltonian Κύκλο

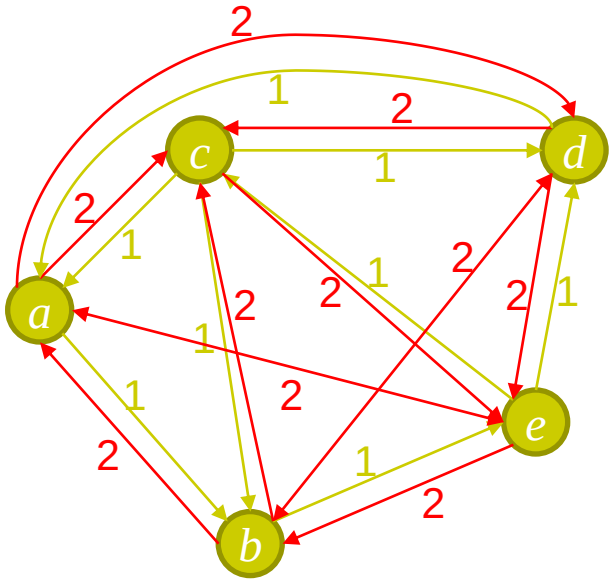
Δεν υπάρχει πορεία απόστασης ≤5

Η Αναγωγή (2)



Έχει Hamiltonian Κύκλο

Αναγωγή



Υπάρχει πορεία απόστασης ≤5

HAMCIRCUIT $\leq_p$ TSP

Ορθότητα Αναγωγής

$\Rightarrow$ Έστω ότι ο G έχει ένα Hamiltonian κύκλο.

Η απόσταση που δίνεται λόγω της αναγωγής σε όλες τις πλευρές είναι 1. Άρα, στο (C,D) υπάρχει μία πορεία του πωλητή συνολικής απόστασης $k=|V|$.

$$(C,D,k) \in \text{TSP}$$

$\Leftarrow$ Έστω ότι το (C,D) έχει μία πορεία συνολικής απόστασης $k=|V|$.

Η πορεία δεν μπορεί να περιέχει καμία ακμή απόστασης 2. Άρα έχουμε ένα Hamiltonian κύκλο στο G.

Απόδοση: Η αναγωγή γίνεται σε τετραγωνικό χρόνο (αποστάσεις στο πλήρες γράφημα)