Αλγόριθμοι και Πολυπλοκότητα

NP και Υπολογιστική Δυσεπιλυσιμότητα

Δημήτρης Μιχαήλ

Τμήμα Πληροφορικής και Τηλεματικής
Χαροκόπειο Πανεπιστήμιο

Κατηγοριοποίηση Προβλημάτων

Στόχος. Κατηγοριοποίηση προβλημάτων ανάλογα με το αν μπορούν να λυθούν σε πολυωνυμικό χρόνο ή όχι.

Κατηγοριοποίηση Προβλημάτων

Στόχος. Κατηγοριοποίηση προβλημάτων ανάλογα με το αν μπορούν να λυθούν σε πολυωνυμικό χρόνο ή όχι.

Άσχημα Νέα. Μια τεράστια συλλογή από βασικά προβλήματα δεν έχουν κατηγοριοποιηθεί με αυτό τον τρόπο, παρά τις μεγάλες μας προσπάθειες.

Κατηγοριοποίηση Προβλημάτων

Στόχος. Κατηγοριοποίηση προβλημάτων ανάλογα με το αν μπορούν να λυθούν σε πολυωνυμικό χρόνο ή όχι.

Άσχημα Νέα. Μια τεράστια συλλογή από βασικά προβλήματα δεν έχουν κατηγοριοποιηθεί με αυτό τον τρόπο, παρά τις μεγάλες μας προσπάθειες.

Εδώ. Θα δείξουμε πως αυτά τα προβλήματα είναι "υπολογιστικά ισοδύναμα" και φαίνεται να είναι διαφορετικός τρόπος περιγραφής ενός πραγματικά δύσκολου προβλήματος.

NP-Πλήρη Προβλήματα

Προβλήματα που δεν γνωρίζουμε αλγόριθμους πολυωνυμικού χρόνου και ταυτόχρονα δεν μπορούμε να αποδείξουμε ότι δεν υπάρχουν αλγόριθμοι πολυωνυμικού χρόνου.

Σημαντική Πρόοδος. Έχουμε καταφέρει να χαρακτηρίσουμε μια μεγάλη κλάση προβλημάτων σε αυτή την ”γκρίζα περιοχή”, και έχουμε αποδείξει ότι είναι ισοδύναμα με την ακόλουθη έννοια.

NP-πλήρη Προβλήματα (NP-complete Problems). Ένας αλγόριθμος πολυωνυμικού χρόνου για οποιοδήποτε από αυτά θα σήμαινε την ύπαρξη ενός αλγορίθμου πολυωνυμικού χρόνου για όλα.

Αναγωγές

Πως μπορούμε να διατυπώσουμε με τυπικό τρόπο προτάσεις όπως:

Το πρόβλημα X είναι τουλάχιστον εξίσου δύσκολο με το πρόβλημα Y.

Αναγωγή (reduction). Θα δείξουμε πως ένα συγκεκριμένο πρόβλημα X είναι τουλάχιστον τόσο δύσκολο όσο κάποιο άλλο πρόβλημα Y ισχυριζόμενοι ότι, αν είχαμε ένα ”μαύρο κουτί” ικανό να λύσει το X, τότε θα μπορούσαμε να λύσουμε και το Y.

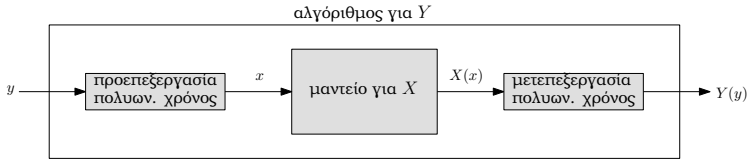
Αναγωγές Πολυωνυμικού Χρόνου

Ένα πρόβλημα Y **ανάγεται σε πολυωνυμικό χρόνο** (polynomial reduces to) σε ένα άλλο πρόβλημα X εαν οποιοδήποτε στιγμιότυπο του προβλήματος Y μπορεί να λυθεί με:

- ένα πολυωνυμικό αριθμό κλασικών υπολογιστικών βημάτων, συν
- ένα πολυωνυμικό αριθμό κλήσεων σε ένα μαντείο (oracle) που λύνει το πρόβλημα X.

Συμβολισμός. $Y \leq_p X$.

Μέγεθος Στιγμιοτύπων. Πληρώνουμε για τον χρόνο που χρειάζεται ώστε να γράψουμε τα στιγμιότυπα που θα δώσουμε στο μαύρο κουτί που επιλύει το πρόβλημα X, καθώς και για να διαβάσουμε την απάντηση που δίνει το μάυρο κουτί.



Τα στιγμιότυπα του X πρέπει να έχουν πολυωνυμικό μέγεθος.

Αναγωγές Πολυωνυμικού Χρόνου

Θεώρημα

Υποθέστε ότι $Y \leq_p X$. Αν το X μπορεί να λυθεί σε πολυωνυμικό χρόνο, τότε το Y μπορεί να λυθεί σε πολυωνυμικό χρόνο.

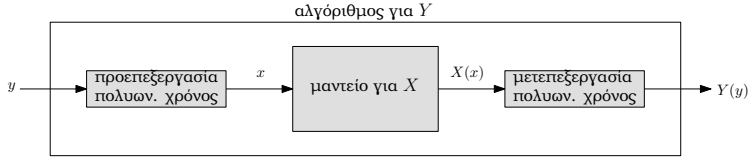
Αναγωγές Πολυωνυμικού Χρόνου

Θεώρημα

Υποθέστε ότι $Y \leq_p X$. Αν το X μπορεί να λυθεί σε πολυωνυμικό χρόνο, τότε το Y μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Απόδειξη

Αντικαθιστούμε το μαντείο με τον αλγόριθμο πολυωνυμικού χρόνου. Μετασχηματίζουμε το στιγμιότυπο του Y σε στιγμιότυπο του X μέσα σε πολυωνυμικό χρόνο, το επιλύουμε με τον αλγόριθμο πολυωνυμικού χρόνου για το X και μετά μετασχηματίζουμε την απάντηση πάλι σε πολυωνυμικό χρόνο ώστε να είναι η απάντηση για το αρχικό πρόβλημα. □



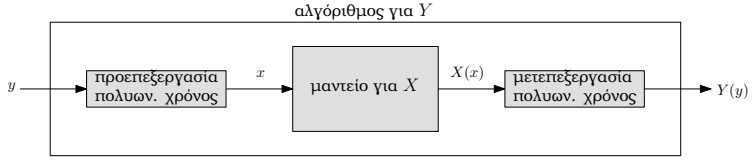
Αναγωγές Πολυωνυμικού Χρόνου

Θεώρημα

Υποθέστε ότι $Y \leq_p X$. Αν το X μπορεί να λυθεί σε πολυωνυμικό χρόνο, τότε το Y μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Απόδειξη

Αντικαθιστούμε το μαντείο με τον αλγόριθμο πολυωνυμικού χρόνου. Μετασχηματίζουμε το στιγμιότυπο του Y σε στιγμιότυπο του X μέσα σε πολυωνυμικό χρόνο, το επιλύουμε με τον αλγόριθμο πολυωνυμικού χρόνου για το X και μετά μετασχηματίζουμε την απάντηση πάλι σε πολυωνυμικό χρόνο ώστε να είναι η απάντηση για το αρχικό πρόβλημα. □



Έχουμε χρησιμοποιήσει αυτό το γεγονός έμμεσα π.χ στον αλγόριθμο εύρεσης μέγιστων ταιριασμάτων σε διμερή γραφήματα όπου χρησιμοποιήσαμε τον αλγόριθμο μέγιστης ροής.

Intractability

Σε αυτό το κεφάλαιο θα χρησιμοποιήσουμε τις αναγωγές πολυωνυμικού χρόνου για να εδραιώσουμε την υπολογιστική δυσεπιλυσιμότητα διαφόρων προβλημάτων.

Συσχέτιση Επιλυσιμότητας (tractability). Παρόλο που δεν γνωρίζουμε πως να λύσουμε διάφορα προβλήματα σε πολυωνυμικό χρόνο θα τα συσχετίσουμε όσο αναφορά την επιλυσιμότητα τους. Έτσι θα εδραιώσουμε σχετικά επίπεδα δυσκολίας μεταξύ των προβλημάτων.

Αντιστροφοαντίθετη Χρήση (contrapositive). Εκφράζουμε λοιπόν το προηγούμενο θεώρημα με την παρακάτω ισοδύναμη μορφή.

Θεώρημα

Υποθέστε ότι $Y \leq_p X$. Αν το Y δεν μπορεί να λυθεί σε πολυωνυμικό χρόνο, τότε το X δεν μπορεί να λυθεί σε πολυωνυμικό χρόνο.

Ανεξάρτητο Σύνολο

Independent Set

Ανεξάρτητο Σύνολο. Δεδομένου ενός γραφήματος $G = (V, E)$ λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ είναι *ανεξάρτητο* (independent) αν δεν υπάρχουν στο S κόμβοι που να ενώνονται ανά δύο με μια ακμή.

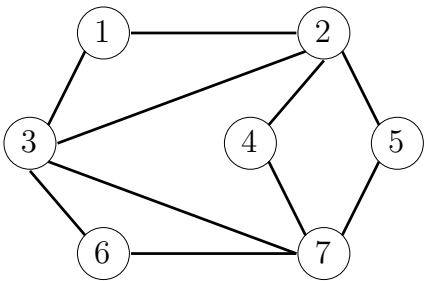
Πρόβλημα Μεγιστοποίησης. Το *πρόβλημα Ανεξάρτητου Συνόλου* είναι το εξής: Δεδομένου ενός γραφήματος G, βρείτε ένα ανεξάρτητο σύνολο που να είναι όσο το δυνατόν μεγαλύτερο.

Ανεξάρτητο Σύνολο

Independent Set

Ανεξάρτητο Σύνολο. Δεδομένου ενός γραφήματος $G = (V, E)$ λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ είναι *ανεξάρτητο* (independent) αν δεν υπάρχουν στο S κόμβοι που να ενώνονται ανά δύο με μια ακμή.

Πρόβλημα Μεγιστοποίησης. Το *πρόβλημα Ανεξάρτητου Συνόλου* είναι το εξής: Δεδομένου ενός γραφήματος G, βρείτε ένα ανεξάρτητο σύνολο που να είναι όσο το δυνατόν μεγαλύτερο.

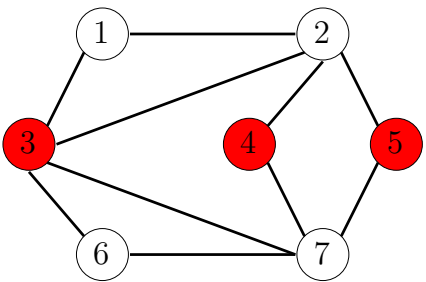


Ανεξάρτητο Σύνολο

Independent Set

Ανεξάρτητο Σύνολο. Δεδομένου ενός γραφήματος $G = (V, E)$ λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ είναι *ανεξάρτητο* (independent) αν δεν υπάρχουν στο S κόμβοι που να ενώνονται ανά δύο με μια ακμή.

Πρόβλημα Μεγιστοποίησης. Το *πρόβλημα Ανεξάρτητου Συνόλου* είναι το εξής: Δεδομένου ενός γραφήματος G, βρείτε ένα ανεξάρτητο σύνολο που να είναι όσο το δυνατόν μεγαλύτερο.

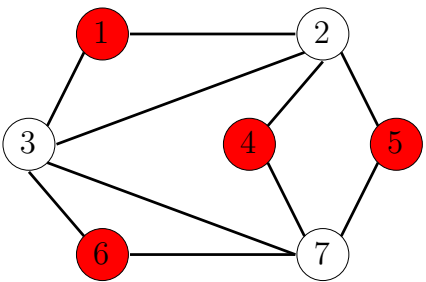


Ανεξάρτητο Σύνολο

Independent Set

Ανεξάρτητο Σύνολο. Δεδομένου ενός γραφήματος $G = (V, E)$ λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ είναι *ανεξάρτητο* (independent) αν δεν υπάρχουν στο S κόμβοι που να ενώνονται ανά δύο με μια ακμή.

Πρόβλημα Μεγιστοποίησης. Το *πρόβλημα Ανεξάρτητου Συνόλου* είναι το εξής: Δεδομένου ενός γραφήματος G, βρείτε ένα ανεξάρτητο σύνολο που να είναι όσο το δυνατόν μεγαλύτερο.



Εκδοχή Λήψης Απόφασης

Βελτιστοποίηση ή Απόφαση. Πολλές φορές είναι ευκολότερο, ως προς την δυνατότητα αναγωγής, να δουλεύουμε με προβλήματα που έχουν απαντήσεις μόνο του τύπου ΝΑΙ/ΟΧΙ.

Εκδοχή Βελτιστοποίησης. Δεδομένου ενός γραφήματος G, ποιο είναι το μεγαλύτερο μέγεθος ανεξαρτήτου συνόλου;

Εκδοχή Απόφασης. Δεδομένου ενός γραφήματος G και ενός αριθμού k, περιέχει το G ένα ανεξάρτητο σύνολο μεγέθους τουλάχιστον k;

Ανεξάρτητο Σύνολο και Ισοδυναμία Εκδοχών

Όσο αναφορά τις πολυωνυμικές αναγωγές

Ισοδυναμία. Όσο αναφορά την δυνατότητα επίλυσης σε πολυωνυμικό χρόνο δεν υπάρχουν σημαντικές διαφορές μεταξύ της *εκδοχής βελτιστοποίησης* και της εκδοχής *λήψης απόφασης* για το πρόβλημα ανεξαρτήτου συνόλου.

Ανεξάρτητο Σύνολο και Ισοδυναμία Εκδοχών

Όσο αναφορά τις πολυωνυμικές αναγωγές

Ισοδυναμία. Όσο αναφορά την δυνατότητα επίλυσης σε πολυωνυμικό χρόνο δεν υπάρχουν σημαντικές διαφορές μεταξύ της *εκδοχής βελτιστοποίησης* και της εκδοχής *λήψης απόφασης* για το πρόβλημα ανεξαρτήτου συνόλου.

Βελτιστοποίηση $\Rightarrow$ Απόφαση. Αν υπάρχει μέθοδος λύσης της εκδοχής βελτιστοποίησης, βρίσκουμε το μέγιστο ανεξάρτητο σύνολο και μετά μπορούμε να απαντήσουμε ερωτήματα απόφασης.

Ανεξάρτητο Σύνολο και Ισοδυναμία Εκδοχών

Όσο αναφορά τις πολυωνυμικές αναγωγές

Ισοδυναμία. Όσο αναφορά την δυνατότητα επίλυσης σε πολυωνυμικό χρόνο δεν υπάρχουν σημαντικές διαφορές μεταξύ της *εκδοχής βελτιστοποίησης* και της εκδοχής *λήψης απόφασης* για το πρόβλημα ανεξαρτήτου συνόλου.

Βελτιστοποίηση $\Rightarrow$ Απόφαση. Αν υπάρχει μέθοδος λύσης της εκδοχής βελτιστοποίησης, βρίσκουμε το μέγιστο ανεξάρτητο σύνολο και μετά μπορούμε να απαντήσουμε ερωτήματα απόφασης.

Απόφαση $\Rightarrow$ Βελτιστοποίηση. Αν υπάρχει μέθοδος λύσης της εκδοχής απόφασης, κάνουμε δυαδική αναζήτηση στις τιμές k επιλύοντας κάθε φορά την εκδοχή απόφασης. Επειδή σε ένα γράφημα G με n κόμβους, το μέγιστο ανεξάρτητο σύνολο δεν μπορεί να είναι μεγαλύτερο του n, στην χειρότερη περίπτωση κάνουμε $\mathcal{O}(\log n)$ βήματα.

Κάλυψη Κορυφών
Vertex Cover

Κάλυψη Κορυφών. Δεδομένου ενός γραφήματος $G(V, E)$, λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ αποτελεί **κάλυψη κορυφών** αν κάθε ακμή $e \in E$ έχει τουλάχιστον ένα άκρο στο S.

Ουσιαστικά οι κορυφές πραγματοποιούν την κάλυψη και οι ακμές ”καλύπτονται”.

Είναι εύκολο να βρούμε μεγάλες καλύψεις, το δύσκολο είναι να βρούμε μικρές.

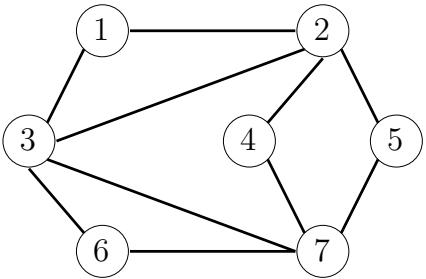
Πρόβλημα Κάλυψης Κορυφών (Vertex Cover). Δεδομένου ενός γραφήματος G και ενός αριθμού k, περιέχει το G μια κάλυψη κορυφών μεγέθους το πολύ k;

Κάλυψη Κορυφών

Vertex Cover

Κάλυψη Κορυφών. Δεδομένου ενός γραφήματος $G(V, E)$, λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ αποτελεί **κάλυψη κορυφών** αν κάθε ακμή $e \in E$ έχει τουλάχιστον ένα άκρο στο S.

Πρόβλημα Κάλυψης Κορυφών (Vertex Cover). Δεδομένου ενός γραφήματος G και ενός αριθμού k, περιέχει το G μια κάλυψη κορυφών μεγέθους το πολύ k;



Το σύνολο $\{1, 2, 6, 7\}$ είναι μια κάλυψη κορυφών μεγέθους 4 ενώ το $\{2, 3, 7\}$ είναι μια κάλυψη κορυφών μεγέθους 3.

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Δεν γνωρίζουμε τρόπο για να λύσουμε τα προβλήματα του Ανεξάρτητου Συνόλου και της Κάλυψης Κορυφών σε πολυωνυμικό χρόνο.

Σχετική Δυσκολία. Μπορούμε όμως να πούμε κάτι για την σχετική τους δυσκολία;

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Δεν γνωρίζουμε τρόπο για να λύσουμε τα προβλήματα του Ανεξάρτητου Συνόλου και της Κάλυψης Κορυφών σε πολυωνυμικό χρόνο.

Σχετική Δυσκολία. Μπορούμε όμως να πούμε κάτι για την σχετική τους δυσκολία;

Ισοδυναμία. Θα δείξουμε πως ως προς την δυσκολία είναι ισοδύναμα αποδεικνύοντας πως

$$\text{Ανεξάρτητο Σύνολο} \leq_p \text{Κάλυψη Κορυφών},$$

και

$$\text{Κάλυψη Κορυφών} \leq_p \text{Ανεξάρτητο Σύνολο}.$$

Θεώρημα

Έστω $G = (V, E)$ ένα γράφημα. Τότε το S είναι ένα ανεξάρτητο σύνολο αν και μόνο αν το συμπληρωματικό του $V \setminus S$ είναι μια κάλυψη κορυφών.

Θεώρημα

Έστω $G = (V, E)$ ένα γράφημα. Τότε το S είναι ένα ανεξάρτητο σύνολο αν και μόνο αν το συμπληρωματικό του $V \setminus S$ είναι μια κάλυψη κορυφών.

Απόδειξη

"$\Rightarrow$" Έστω πως S είναι ανεξάρτητο σύνολο. Θεωρήστε μια τυχαία ακμή $e = (u, v)$. Επειδή το S είναι ανεξάρτητο, δεν μπορεί και ο κόμβος u και ο v να ανήκουν στο S. Άρα ένας από τους δύο ανήκει στο $V \setminus S$. Κατά συνέπεια κάθε ακμή έχει ένα άκρο στο $V \setminus S$ και άρα το $V \setminus S$ είναι μια κάλυψη κορυφών.

□

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Θεώρημα

Έστω $G = (V, E)$ ένα γράφημα. Τότε το S είναι ένα ανεξάρτητο σύνολο αν και μόνο αν το συμπληρωματικό του $V \setminus S$ είναι μια κάλυψη κορυφών.

Απόδειξη

"$\Rightarrow$" Έστω πως S είναι ανεξάρτητο σύνολο. Θεωρήστε μια τυχαία ακμή $e = (u, v)$. Επειδή το S είναι ανεξάρτητο, δεν μπορεί και ο κόμβος u και ο v να ανήκουν στο S. Άρα ένας από τους δύο ανήκει στο $V \setminus S$. Κατά συνέπεια κάθε ακμή έχει ένα άκρο στο $V \setminus S$ και άρα το $V \setminus S$ είναι μια κάλυψη κορυφών.

"$\Leftarrow$" Αντιστρόφως υποθέστε πως το $V \setminus S$ είναι μια κάλυψη κορυφών. Θεωρήστε δύο τυχαίους κόμβους u και v του S. Αν οι κόμβοι αυτοί συνδέονται με μια ακμή e, τότε κανένα άκρο της e δεν θα είναι στο $V \setminus S$ και άρα η ακμή e δεν θα καλυπτόταν από το $V \setminus S$, που είναι αντίφαση. Άρα δεν υπάρχει ακμή που να συνδέει δύο κόμβους του S και άρα το S είναι ανεξάρτητο σύνολο. □

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Θεώρημα

Ανεξάρτητο Σύνολο $\leq_p$ Κάλυψη Κορυφών .

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Θεώρημα

Ανεξάρτητο Σύνολο $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το G έχει ανεξάρτητο σύνολο μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το G έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Θεώρημα

Ανεξάρτητο Σύνολο $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το G έχει ανεξάρτητο σύνολο μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το G έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Θεώρημα

Κάλυψη Κορυφών $\leq_p$ Ανεξάρτητο Σύνολο .

Ανεξάρτητο Σύνολο και Κάλυψη Κορυφών

Θεώρημα

Ανεξάρτητο Σύνολο $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το G έχει ανεξάρτητο σύνολο μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το G έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Θεώρημα

Κάλυψη Κορυφών $\leq_p$ Ανεξάρτητο Σύνολο .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Ανεξάρτητου Συνόλου, τότε μπορούμε να αποφασίσουμε αν το G έχει Κάλυψη Κορυφών το πολύ k ρωτώντας το μαύρο κουτί αν το G έχει ανεξάρτητο σύνολο μεγέθους τουλάχιστον $n - k$. □

Κλίκα
Clique

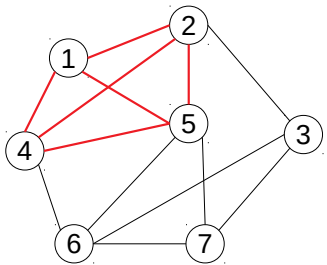
Κλίκα. Δεδομένου ενός μη-κατευθυνόμενου γραφήματος $G(V, E)$, λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ αποτελεί **κλίκα** αν υπάρχει ακμή μεταξύ κάθε ζεύγους κόμβων στο S.

Πρόβλημα Εύρεσης Κλίκας (Clique). Δεδομένου ενός γραφήματος G και ενός αριθμού k, περιέχει το G μια κλίκα μεγέθους τουλάχιστον k;

Κλίκα
Clique

Κλίκα. Δεδομένου ενός μη-κατευθυνόμενου γραφήματος $G(V, E)$, λέμε ότι ένα σύνολο κόμβων $S \subseteq V$ αποτελεί **κλίκα** αν υπάρχει ακμή μεταξύ κάθε ζεύγους κόμβων στο S.

Πρόβλημα Εύρεσης Κλίκας (Clique). Δεδομένου ενός γραφήματος G και ενός αριθμού k, περιέχει το G μια κλίκα μεγέθους τουλάχιστον k;

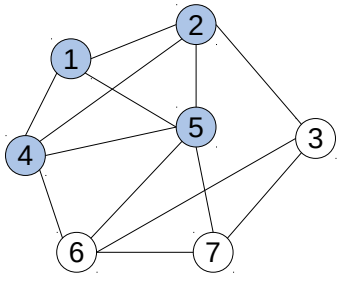


Το σύνολο $\{1, 2, 4, 5\}$ είναι μια κλίκα μεγέθους 4.

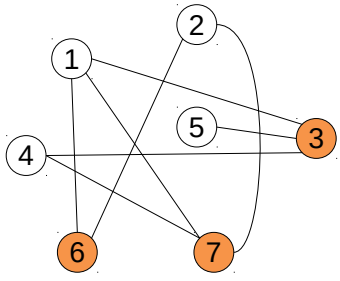
Κλίκα και Κάλυψη Κορυφών

Θεώρημα

Έστω $G = (V, E)$ ένα μη-κατευθυνόμενο γράφημα και το συμπληρωματικό του γράφημα $G' = (V, E')$ όπου $E' = \{(v, w) : (v, w) \notin E\}$. Τότε το G έχει κλίκα μεγέθους k αν και μόνο αν το G' έχει κάλυψη κορυφών μεγέθους $|V| - k$.



G



G'

Θεώρημα

Έστω $G = (V, E)$ ένα μη-κατευθυνόμενο γράφημα και το συμπληρωματικό του γράφημα $G' = (V, E')$ όπου $E' = \{(v, w) : (v, w) \notin E\}$. Τότε το G έχει κλίκα μεγέθους k αν και μόνο αν το G' έχει κάλυψη κορυφών μεγέθους $|V| - k$.

Θεώρημα

Έστω $G = (V, E)$ ένα μη-κατευθυνόμενο γράφημα και το συμπληρωματικό του γράφημα $G' = (V, E')$ όπου $E' = \{(v, w) : (v, w) \notin E\}$. Τότε το G έχει κλίκα μεγέθους k αν και μόνο αν το G' έχει κάλυψη κορυφών μεγέθους $|V| - k$.

Απόδειξη

"$\Rightarrow$"

- Έστω πως ο G έχει μία κλίκα S με μέγεθος $|S| = k$.
- Θεωρήστε το σύνολο $S' = V \setminus S$ που έχει μέγεθος $|V| - k$.
- Για να δείξουμε πως το S' είναι κάλυψη κορυφών στον G' διαλέγουμε οποιαδήποτε ακμή $(v, w) \in E'$:
  - η ακμή $(v, w) \notin E$ (αφού ανήκει στον G')
  - τουλάχιστον ένας από τους v ή w δεν ανήκουν στο S (αλλιώς το S δεν θα ήταν κλίκα)
  - άρα τουλάχιστον ένας από τους v ή w ανήκει στο S'
  - συνεπώς η (v, w) καλύπτεται από το S'

□

Θεώρημα

Έστω $G = (V, E)$ ένα μη-κατευθυνόμενο γράφημα και το συμπληρωματικό του γράφημα $G' = (V, E')$ όπου $E' = \{(v, w) : (v, w) \notin E\}$. Τότε το G έχει κλίκα μεγέθους k αν και μόνο αν το G' έχει κάλυψη κορυφών μεγέθους $|V| - k$.

Απόδειξη

"$\Leftarrow$"

- Υποθέστε πως ο G' έχει μία κάλυψη κορυφών S' με $|S'| = |V| - k$.
- Θεωρήστε το σύνολο $S = V \setminus S'$ που έχει μέγεθος k.
- Για να δείξουμε πως το S είναι κλίκα στον G διαλέγουμε δύο κόμβους $v \in S$ και $w \in S$:
  - υποθέστε πως δεν υπάρχει ακμή $(v, w) \in E$
  - τότε υπάρχει ακμή $(v, w) \in E'$
  - η ακμή αυτή δεν καλύπτεται από το S', που είναι άτοπο
  - άρα υπάρχει ακμή $(v, w) \in E$
  - συνεπώς το S είναι κλίκα

□

Κλίκα και Κάλυψη Κορυφών

Θεώρημα

$\text{Κλίκα} \leq_p \text{Κάλυψη Κορυφών}$.

Κλίκα και Κάλυψη Κορυφών

Θεώρημα

Κλίκα $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το $G(V, E)$ έχει κλίκα μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το $G'(V, E')$ έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Κλίκα και Κάλυψη Κορυφών

Θεώρημα

Κλίκα $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το $G(V, E)$ έχει κλίκα μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το $G'(V, E')$ έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Θεώρημα

Κάλυψη Κορυφών $\leq_p$ Κλίκα .

Κλίκα και Κάλυψη Κορυφών

Θεώρημα

Κλίκα $\leq_p$ Κάλυψη Κορυφών .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κάλυψης Κορυφών, τότε μπορούμε να αποφασίσουμε αν το $G(V, E)$ έχει κλίκα μεγέθους τουλάχιστον k ρωτώντας το μαύρο κουτί αν το $G'(V, E')$ έχει κάλυψη κορυφών μεγέθους το πολύ $n - k$. □

Θεώρημα

Κάλυψη Κορυφών $\leq_p$ Κλίκα .

Απόδειξη

Διαθέτοντας ένα μαύρο κουτί για την επίλυση του προβλήματος Κλίκας, τότε μπορούμε να αποφασίσουμε αν το G έχει Κάλυψη Κορυφών το πολύ k ρωτώντας το μαύρο κουτί αν το $G'(V, E')$ έχει κλίκα μεγέθους τουλάχιστον $n - k$. □

Κάλυψη Συνόλου

Το πρόβλημα κάλυψης κορυφών είναι ένα πρόβλημα κάλυψης διατυπωμένο ειδικά στη γλώσσα των γραφημάτων. Υπάρχει ένα πιο γενικό πρόβλημα.

Κάλυψη Συνόλου (Set Cover). Με δεδομένα ένα σύνολο U με n στοιχεία, μια συλλογή $S_1, \ldots, S_m$ υποσυνόλων του U, και έναν αριθμό k, υπάρχει συλλογή με k το πολύ από αυτά τα σύνολα των οποίων η ένωση να είναι ίση με όλο το U;

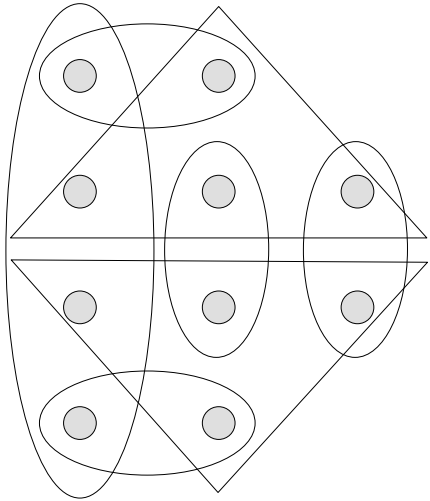
Κάλυψη Συνόλου

Το πρόβλημα κάλυψης κορυφών είναι ένα πρόβλημα κάλυψης διατυπωμένο ειδικά στη γλώσσα των γραφημάτων. Υπάρχει ένα πιο γενικό πρόβλημα.

Κάλυψη Συνόλου (Set Cover). Με δεδομένα ένα σύνολο U με n στοιχεία, μια συλλογή $S_1, \ldots, S_m$ υποσυνόλων του U, και έναν αριθμό k, υπάρχει συλλογή με k το πολύ από αυτά τα σύνολα των οποίων η ένωση να είναι ίση με όλο το U;

Παράδειγμα. Έχουμε m διαθέσιμα τμήματα λογισμικού και ένα σύνολο U από n δυνατότητες που θα θέλαμε να έχει το σύστημα μας. Το τμήμα λογισμικού i περιλαμβάνει το σύνολο $S_i \subseteq U$ των δυνατοτήτων. Στο πρόβλημα της κάλυψης συνόλου ζητούμε να συμπεριλάβουμε στο σύστημα μας ένα μικρό αριθμό από αυτά τα κομμάτια λογισμικού, με την ιδιότητα ότι το σύστημα μας θα έχει και τις n δυνατότητες.

Κάλυψη Συνόλου



Κάλυψη Συνόλου και Κάλυψη Κορυφών

Θεώρημα

$\textsc{Κάλυψη Κορυφών} \leq_p \textsc{Κάλυψη Συνόλου}$

Ας υποθέσουμε πως έχουμε ένα μαύρο κουτί που μπορεί να λύσει την Κάλυψη Συνόλου, και θεωρήστε ένα στιγμιότυπο του προβλήματος Κάλυψης Κορυφής, που καθορίζεται από ένα γράφημα $G = (V, E)$ και ένα αριθμό k.

Θεώρημα

$\textsc{Κάλυψη Κορυφών} \leq_p \textsc{Κάλυψη Συνόλου}$

Ας υποθέσουμε πως έχουμε ένα μαύρο κουτί που μπορεί να λύσει την Κάλυψη Συνόλου, και θεωρήστε ένα στιγμιότυπο του προβλήματος Κάλυψης Κορυφής, που καθορίζεται από ένα γράφημα $G = (V, E)$ και ένα αριθμό k.

Θα κατασκευάσουμε σε πολυωνυμικό χρόνο ένα στιγμιότυπο του προβλήματος κάλυψης συνόλου.

- Θέτουμε $U = E$.
- Επίσης για κάθε κορυφή $i \in V$ φτιάχνουμε ένα υποσύνολο $S_i = \{e \in E : e \text{ προσκείμενη στην κορυφή } i\} \subseteq U$.

Μεταβιβάζουμε το στιγμιότυπο αυτό στο μαύρο κουτί και απαντάμε ναι αν και μόνο αν το μαύρο κουτί απαντήσει ναι.

Θεώρημα

Κάλυψη Κορυφών $\leq_p$ Κάλυψη Συνόλου

Ισχυριζόμαστε πως το U μπορεί να καλυφθεί με το πολύ k από αυτά τα σύνολα $S_1, \ldots, S_n$ αν και μόνο αν το G έχει μια κάλυψη κορυφών μεγέθους το πολύ k.

"$\Rightarrow$" Αν $S_{i_1}, \ldots, S_{i_l}$ είναι $l \leq k$ σύνολα που καλύπτουν το U, τότε κάθε ακμή του G προσπίπτει σε μία από τις κορυφές $i_1, \ldots, i_l$, και άρα το σύνολο $\{i_1, \ldots, i_l\}$ είναι μια κάλυψη κορυφών του G με μέγεθος $l \leq k$.

"$\Leftarrow$" Αν $\{i_1, \ldots, i_l\}$ είναι μια κάλυψη κορυφών του G με μέγεθος $l \leq k$, τότε τα σύνολα $S_{i_1}, \ldots, S_{i_l}$ καλύπτουν το U.

Το πρόβλημα SAT είναι ένα πρόβλημα μεγάλης πρακτικής σημασίας, με εφαρμογές που εκτείνονται από τον έλεγχο των τσιπ και τη σχεδίαση υπολογιστών μέχρι την ανάλυση εικόνων και την τεχνολογία λογισμικού.

Μοντελοποιεί ένα ευρύ σύνολο προβλημάτων όπου πρέπει να ορίσουμε μεταβλητές απόφασης έτσι ώστε να ικανοποιήσουμε ένα δεδομένο σύνολο περιορισμών.

Μορφή. Ένα στιγμιότυπο SAT έχει την εξής μορφή:

$$(x \vee y \vee z) \wedge (x \vee \bar{y}) \wedge (y \vee \bar{z}) \wedge (z \vee \bar{x}) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}).$$

Πρόκειται για ένα *λογικό τύπο* (Boolean formula) σε *συζευκτική κανονική μορφή* (conjunctive normal form - CNF):

- είναι η σύζευξη (λογικό and, που συμβολίζεται με $\wedge$) μιας συλλογής *όρων* (clauses) – οι παρενθέσεις –
- κάθε όρος αποτελείται από την διάζευξη (λογικό or, που συμβολίζεται με $\vee$) διαφόρων *στοιχείων* (literals)
- κάθε στοιχείο είναι μια λογική μεταβλητή όπως η x ή η άρνηση της $\bar{x}$.

Ικανοποιούσα ανάθεση τιμών αληθείας. Είναι μια ανάθεση τιμών ”ψευδές” ή ”αληθές” (false ή true) σε κάθε μεταβλητή έτσι ώστε ο λογικός τύπος να είναι αληθής (satisfying truth assignment).

SAT

Πρόβλημα SAT. Δεδομένου ενός λογικού τύπου σε συζευκτική κανονική μορφή, είτε βρείτε μια ικανοποιούσα ανάθεση τιμών αληθείας, ή αλλιώς αναφέρετε ότι δεν υπάρχει καμία.

SAT

Πρόβλημα SAT. Δεδομένου ενός λογικού τύπου σε συζευκτική κανονική μορφή, είτε βρείτε μια ικανοποιούσα ανάθεση τιμών αληθείας, ή αλλιώς αναφέρετε ότι δεν υπάρχει καμία.

Στον τύπο

$$(x \vee y \vee z) \wedge (x \vee \bar{y}) \wedge (y \vee \bar{z}) \wedge (z \vee \bar{x}) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}),$$

δεν υπάρχει ικανοποιούσα ανάθεση τιμών αληθείας. Το πρόβλημα είναι πως οι τρεις ενδιάμεσοι όροι αναγκάζουν και τις τρεις μεταβλητές να έχουν την ίδια τιμή.

SAT

Πρόβλημα SAT. Δεδομένου ενός λογικού τύπου σε συζευκτική κανονική μορφή, είτε βρείτε μια ικανοποιούσα ανάθεση τιμών αληθείας, ή αλλιώς αναφέρετε ότι δεν υπάρχει καμία.

Στον τύπο

$$(x \vee y \vee z) \wedge (x \vee \bar{y}) \wedge (y \vee \bar{z}) \wedge (z \vee \bar{x}) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}),$$

δεν υπάρχει ικανοποιούσα ανάθεση τιμών αληθείας. Το πρόβλημα είναι πως οι τρεις ενδιάμεσοι όροι αναγκάζουν και τις τρεις μεταβλητές να έχουν την ίδια τιμή.

Η λύση ωμής βίας δεν παρέχει καμία λύση εδώ αφού σε τύπους με n μεταβλητές το πλήθος των δυνατών αναθέσεων τιμών είναι εκθετικό, 2^n.

SAT και 3-SAT

Ειδική Περίπτωση. Η περίπτωση όπου κάθε όρος (clause) έχει ακριβώς τρία στοιχεία (literals), έχει την ίδια δυσκολία με την γενική περίπτωση, αλλά είναι πιο εύκολο να εξεταστεί.

Πρόβλημα 3-SAT. Δεδομένου ενός λογικού τύπου σε συζευκτική κανονική μορφή, όπου κάθε όρος έχει ακριβώς τρία στοιχεία, βρείτε μια ικανοποιούσα ανάθεση τιμών αληθείας, ή αλλιώς αναφέρετε ότι δεν υπάρχει καμία.

SAT και 3-SAT

Τα προβλήματα αυτά είναι θεμελιώδη συνδυαστικά προβλήματα αναζήτησης.

Περιέχουν με τρόπο ”απογυμνωμένο” τα βασικά συστατικά ενός δύσκολου υπολογιστικού προβλήματος.

Πρέπει

- να πάρουμε n ανεξάρτητες αποφάσεις (τις αποδόσεις τιμών στις μεταβλητές $x_1, \ldots, x_n$) έτσι ώστε να ικανοποιείται ένα συνολο περιορισμών,
- μεμονωμένα υπάρχουν αρκετοί τρόποι ικανοποίησης κάθε περιορισμού, αλλά θα πρέπει να ρυθμίσουμε τις αποφάσεις μας έτσι ώστε να ικανοποιούνται ταυτόχρονα όλοι οι περιορισμοί.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Παρόλο που τα προβλήματα

- 3-SAT και
- Ανεξάρτητο Σύνολο

φαίνονται διαφορετικά, η δυσκολία τους είναι ίδιου τύπου.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Παρόλο που τα προβλήματα

- 3-SAT και
- Ανεξάρτητο Σύνολο

φαίνονται διαφορετικά, η δυσκολία τους είναι ίδιου τύπου.

Ενώ το πρόβλημα 3-SAT αφορά την απόδοση τιμών σε λογικές μεταβλητές υπό την παρουσία περιορισμών, το πρόβλημα Ανεξάρτητου Συνόλου αφορά την επιλογή κορυφών σε ένα γράφημα.

Και όμως θα δείξουμε πως

$$\text{3-SAT} \leq_p \text{Ανεξάρτητο Σύνολο}\,.$$

Μέσα από την απόδειξη πως

$$\text{3-SAT} \leq_p \text{Ανεξάρτητο Σύνολο}$$

θα δείξουμε μια γενική αρχή για το σχεδιασμό πολύπλοκων αναγωγών.

Μικροεργαλεία (gadgets). Πολλές φορές μια πολύπλοκη αναγωγή $Y \leq_p X$ γίνεται ευκολότερη δημιουργώντας "μικροεργαλεία" από συστατικά του προβλήματος X για να αναπαραστήσουμε αυτό που συμβαίνει στο πρόβλημα Y.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Ιδέα της Αναγωγής

Θέλουμε να λύσουμε το πρόβλημα 3-SAT έχοντας πρόσβαση σε ένα μαύρο κουτί που λύνει το πρόβλημα Ανεξαρτήτου Συνόλου.

Ιδέα της Αναγωγής. Το κλειδί είναι να κοιτάξουμε το πρόβλημα 3-SAT λίγο διαφορετικά:

- Πρέπει να επιλέξουμε μια μεταβλητή (literal) από κάθε όρο (clause),
- και να βρούμε μια απόδοση τιμών αληθείας που θα κάνει όλες αυτές τις μεταβλητές να πάρουν την τιμή ”αλήθεια”, ικανοποιώντας έτσι όλους τους όρους.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Ιδέα της Αναγωγής

Θέλουμε να λύσουμε το πρόβλημα 3-SAT έχοντας πρόσβαση σε ένα μαύρο κουτί που λύνει το πρόβλημα Ανεξαρτήτου Συνόλου.

Ιδέα της Αναγωγής. Το κλειδί είναι να κοιτάξουμε το πρόβλημα 3-SAT λίγο διαφορετικά:

- Πρέπει να επιλέξουμε μια μεταβλητή (literal) από κάθε όρο (clause),
- και να βρούμε μια απόδοση τιμών αληθείας που θα κάνει όλες αυτές τις μεταβλητές να πάρουν την τιμή ”αλήθεια”, ικανοποιώντας έτσι όλους τους όρους.

Διενέξεις. Αυτό επιτυγχάνεται αν μπορούμε να επιλέξουμε μια μεταβλητή από κάθε όρο με τέτοιο τρόπο ώστε να μην υπάρχει ”διένεξη” (conflict) μεταξύ δύο επιλεγμένων όρων.
Δύο μεταβλητές βρίσκονται σε διένεξη όταν η μία είναι ίση με την άρνηση της άλλης.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Είσοδος. Έστω λοιπόν το στιγμιότυπο του προβλήματος 3-SAT που αποτελείται από τις μεταβλητές $X = \{x_1, \ldots, x_n\}$ και είναι

$$(y_{11} \vee y_{12} \vee y_{13}) \wedge (y_{21} \vee y_{22} \vee y_{23}) \wedge \ldots \wedge (y_{k1} \vee y_{k2} \vee y_{k3})$$

όπου η μεταβλητή y_{ij} είναι κάποια μεταβλητή από το X ή η άρνηση κάποιας μεταβλητής από το X.

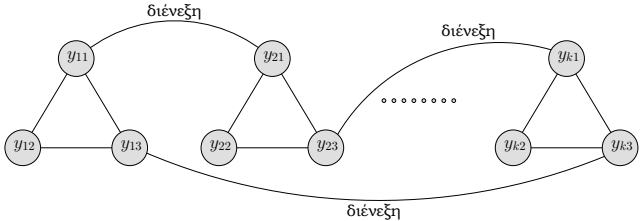
Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Είσοδος. Έστω λοιπόν το στιγμιότυπο του προβλήματος 3-SAT που αποτελείται από τις μεταβλητές $X = \{x_1, \ldots, x_n\}$ και είναι

$$(y_{11} \vee y_{12} \vee y_{13}) \wedge (y_{21} \vee y_{22} \vee y_{23}) \wedge \ldots \wedge (y_{k1} \vee y_{k2} \vee y_{k3})$$

όπου η μεταβλητή y_{ij} είναι κάποια μεταβλητή από το X ή η άρνηση κάποιας μεταβλητής από το X.

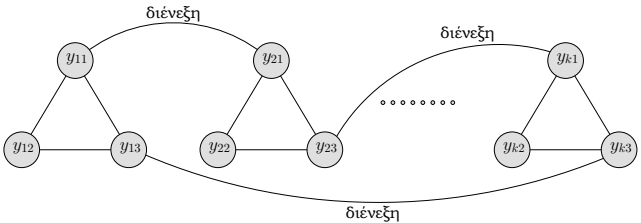
Γράφημα.
Κατασκευάζουμε ένα γράφημα με $3k$ κόμβους ομαδοποιημένους σε k τρίγωνα.



Όταν δύο στοιχεία (literals) είναι μια μεταβλητή και η άρνηση της (διένεξη), ενώνουμε τους κόμβους που αντιστοιχούν στα δύο αυτά στοιχεία με μια ακμή.

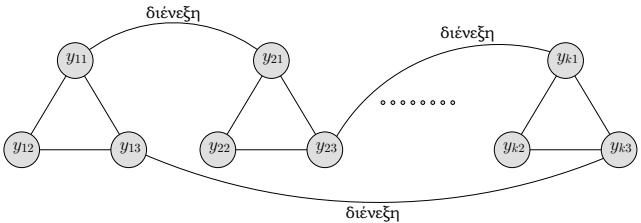
Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Ισχυρισμός. Ισχυριζόμαστε πως το αρχικό στιγμιότυπο 3-SAT είναι ικανοποιήσιμο αν και μόνο αν το γράφημα G που έχουμε κατασκευάσει διαθέτει ένα ανεξάρτητο σύνολο μεγέθους τουλάχιστον k.



Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

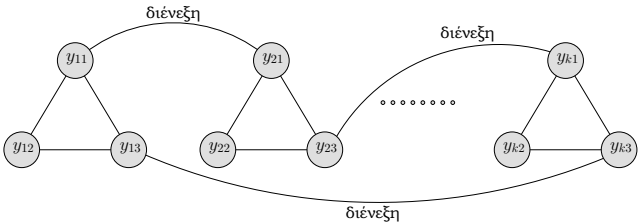
Ισχυρισμός. Ισχυριζόμαστε πως το αρχικό στιγμιότυπο 3-SAT είναι ικανοποιήσιμο αν και μόνο αν το γράφημα G που έχουμε κατασκευάσει διαθέτει ένα ανεξάρτητο σύνολο μεγέθους τουλάχιστον k.



"$\Rightarrow$". Αν το στιγμιότυπο 3-SAT είναι ικανοποιήσιμο, τότε κάθε τρίγωνο του G περιέχει τουλάχιστον ένα κόμβο ο οποίος πέρνει την τιμή "αλήθεια".

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Ισχυρισμός. Ισχυριζόμαστε πως το αρχικό στιγμιότυπο 3-SAT είναι ικανοποιήσιμο αν και μόνο αν το γράφημα G που έχουμε κατασκευάσει διαθέτει ένα ανεξάρτητο σύνολο μεγέθους τουλάχιστον k.

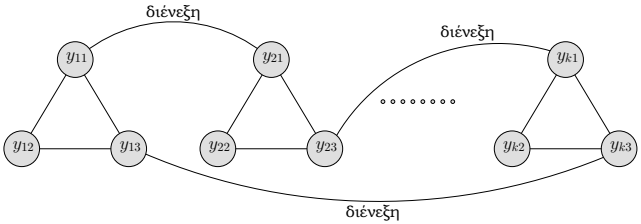


"$\Rightarrow$". Αν το στιγμιότυπο 3-SAT είναι ικανοποιήσιμο, τότε κάθε τρίγωνο του G περιέχει τουλάχιστον ένα κόμβο ο οποίος πέρνει την τιμή "αλήθεια".

Έστω S ένα σύνολο που αποτελείται από έναν τέτοιο κόμβο από κάθε τρίγωνο. Τότε $|S| \geq k$ και ισχυριζόμαστε πως το S είναι ανεξάρτητο.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

Ισχυρισμός. Ισχυριζόμαστε πως το αρχικό στιγμιότυπο 3-SAT είναι ικανοποιήσιμο αν και μόνο αν το γράφημα G που έχουμε κατασκευάσει διαθέτει ένα ανεξάρτητο σύνολο μεγέθους τουλάχιστον k.

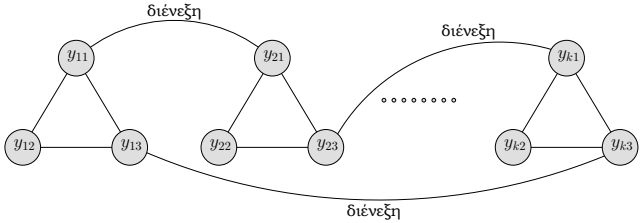


"$\Rightarrow$". Αν το στιγμιότυπο 3-SAT είναι ικανοποιήσιμο, τότε κάθε τρίγωνο του G περιέχει τουλάχιστον ένα κόμβο ο οποίος πέρνει την τιμή "αλήθεια".

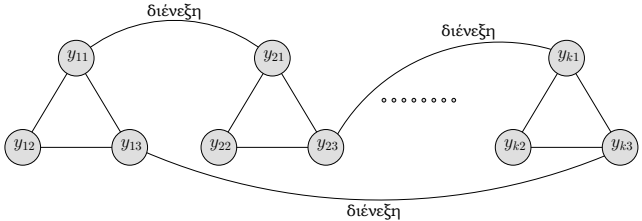
Έστω S ένα σύνολο που αποτελείται από έναν τέτοιο κόμβο από κάθε τρίγωνο. Τότε $|S| \geq k$ και ισχυριζόμαστε πως το S είναι ανεξάρτητο.

Αλλιώς, υπάρχει ακμή μεταξύ δύο κόμβων $u, v \in S$, και άρα τα στοιχεία (literals) στο στιγμιότυπο του 3-SAT βρίσκονται σε διένεξη. Αδύνατο, γιατί και τα δύο έχουν τιμή αλήθεια.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο

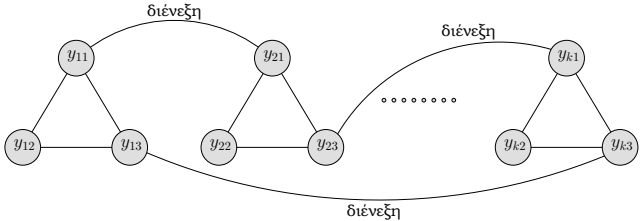


Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο



"$\Leftarrow$". Έστω πως το G έχει ένα ανεξάρτητο σύνολο S με $|S| \geq k$. Τότε λόγω των τριγώνων, κάθε τρίγωνο έχει ένα ακριβώς στοιχείο του S και άρα $|S| = k$.

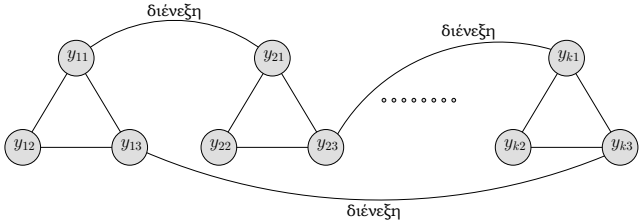
Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο



"$\Leftarrow$". Έστω πως το G έχει ένα ανεξάρτητο σύνολο S με $|S| \geq k$. Τότε λόγω των τριγώνων, κάθε τρίγωνο έχει ένα ακριβώς στοιχείο του S και άρα $|S| = k$.

Θα δώσουμε τιμές στα στοιχεία (literals) που αντιστοιχούν στους κόμβους του S ώστε να κάνουμε το στιγμιότυπο 3-SAT αλήθεια.

Αναγωγή του 3-SAT στο Ανεξάρτητο Σύνολο



"$\Leftarrow$". Έστω πως το G έχει ένα ανεξάρτητο σύνολο S με $|S| \geq k$. Τότε λόγω των τριγώνων, κάθε τρίγωνο έχει ένα ακριβώς στοιχείο του S και άρα $|S| = k$.

Θα δώσουμε τιμές στα στοιχεία (literals) που αντιστοιχούν στους κόμβους του S ώστε να κάνουμε το στιγμιότυπο 3-SAT αλήθεια.

Για κάθε μεταβλητή x_i, αν δεν ανήκει καθόλου στο S την θέτουμε "αλήθεια".

Επειδή το S είναι ανεξάρτητο σύνολο, δεν γίνεται και η x_i αλλά και η $\bar{x}_i$ να ανήκουν στο S (λόγω ύπαρξης διένεξης και άρα ακμής).

Αν $x_i \in S$ την θέτουμε "αλήθεια" και αν $\bar{x}_i \in S$ την θέτουμε "ψέματα".

Μεταβατική Ιδιότητα των Αναγωγών

Θεώρημα

Αν $Z \leq_p Y$ και $Y \leq_p X$, τότε $Z \leq_p X$.

Μεταβατική Ιδιότητα των Αναγωγών

Θεώρημα

Αν $Z \leq_p Y$ και $Y \leq_p X$, τότε $Z \leq_p X$.

Απόδειξη

Με δεδομένο ένα μαύρο κουτί για το X, θα δείξουμε με ποιον τρόπο επιλύεται ένα στιγμιότυπο του Z.

Εκτελούμε τον αλγόριθμο για το Z χρησιμοποιώντας ένα μαύρο κουτί για το Y. Όμως κάθε φορά που καλείται το μαύρο κουτί για το Y, το προσομοιώνουμε με έναν πολυωνυμικό αριθμό βημάτων χρησιμοποιώντας τον αλγόριθμο που επιλύει στιγμιότυπα του Y μέσω του μαύρου κουτιού για το X. □

Μεταβατική Ιδιότητα των Αναγωγών

Θεώρημα

Αν $Z \leq_p Y$ και $Y \leq_p X$, τότε $Z \leq_p X$.

Απόδειξη

Με δεδομένο ένα μαύρο κουτί για το X, θα δείξουμε με ποιον τρόπο επιλύεται ένα στιγμιότυπο του Z.

Εκτελούμε τον αλγόριθμο για το Z χρησιμοποιώντας ένα μαύρο κουτί για το Y. Όμως κάθε φορά που καλείται το μαύρο κουτί για το Y, το προσομοιώνουμε με έναν πολυωνυμικό αριθμό βημάτων χρησιμοποιώντας τον αλγόριθμο που επιλύει στιγμιότυπα του Y μέσω του μαύρου κουτιού για το X. □

Και άρα μπορούμε π.χ να πούμε πως αφού

$$\text{3-SAT} \leq_p \text{Ανεξάρτητο Σύνολο} \leq_p \text{Κάλυψη Κορυφών}$$

ισχύει πως

$$\text{3-SAT} \leq_p \text{Κάλυψη Κορυφών}\ .$$

Αποδοτική Πιστοποίηση

Ένα βασικό ερώτημα που θα μας απασχολήσει είναι η αντίθεση μεταξύ

1. της εύρεσης μιας λύσης, και
2. του ελέγχου μιας προτεινόμενης λύσης.

Αποδοτική Πιστοποίηση

Ένα βασικό ερώτημα που θα μας απασχολήσει είναι η αντίθεση μεταξύ

1. της εύρεσης μιας λύσης, και
2. του ελέγχου μιας προτεινόμενης λύσης.

Παράδειγμα 3-SAT.

- Δεν γνωρίζουμε κάποιον αλγόριθμο πολυωνυμικού χρόνου για την εύρεση λύσεων.
- Ο έλεγχος όμως μιας προτεινόμενης λύσης μπορεί να πραγματοποιηθεί σε πολυωνυμικό χρόνο.

Αποδοτική Πιστοποίηση

Ένα βασικό ερώτημα που θα μας απασχολήσει είναι η αντίθεση μεταξύ

1. της εύρεσης μιας λύσης, και
2. του ελέγχου μιας προτεινόμενης λύσης.

Παράδειγμα 3-SAT.

- Δεν γνωρίζουμε κάποιον αλγόριθμο πολυωνυμικού χρόνου για την εύρεση λύσεων.
- Ο έλεγχος όμως μιας προτεινόμενης λύσης μπορεί να πραγματοποιηθεί σε πολυωνυμικό χρόνο.

Δυσκολία; Το ζήτημα αυτό δεν είναι απλό. Σκεφτείτε το πρόβλημα που θα αντιμετωπίζατε αν έπρεπε να αποδείξετε ότι ένα στιγμιότυπο 3-SAT δεν είναι ικανοποιήσιμο.

- Ποια ”στοιχεία” θα παρουσιάζατε που θα έπειθαν, σε πολυωνυμικό χρόνο, ότι το στιγμιότυπο δεν μπορεί να ικανοποιηθεί;

Είσοδος. Θα κωδικοποιήσουμε την είσοδο σε ένα υπολογιστικό πρόβλημα ως ένα πεπερασμένο δυαδικό αλφαριθμητικό s. Συμβολίζουμε με $|s|$ το μήκος της εισόδου.

Προβλήματα Απόφασης

Λίγο πιο τυπικά

Είσοδος. Θα κωδικοποιήσουμε την είσοδο σε ένα υπολογιστικό πρόβλημα ως ένα πεπερασμένο δυαδικό αλφαριθμητικό s. Συμβολίζουμε με $|s|$ το μήκος της εισόδου.

Υπολογιστικό Πρόβλημα. Προσδιορίζουμε ένα υπολογιστικό πρόβλημα X με το σύνολο των αλφαριθμητικών για τα οποία η απάντηση είναι "ναι".

Είσοδος. Θα κωδικοποιήσουμε την είσοδο σε ένα υπολογιστικό πρόβλημα ως ένα πεπερασμένο δυαδικό αλφαριθμητικό s. Συμβολίζουμε με $|s|$ το μήκος της εισόδου.

Υπολογιστικό Πρόβλημα. Προσδιορίζουμε ένα υπολογιστικό πρόβλημα X με το σύνολο των αλφαριθμητικών για τα οποία η απάντηση είναι ”ναι”.

Αλγόριθμος. Ένας αλγόριθμος A *επιλύει* το πρόβλημα X αν, για όλα τα αλφαριθμητικά s, έχουμε

$$A(s) = \text{ναι} \quad \text{αν και μόνο αν } s \in X.$$

Είσοδος. Θα κωδικοποιήσουμε την είσοδο σε ένα υπολογιστικό πρόβλημα ως ένα πεπερασμένο δυαδικό αλφαριθμητικό s. Συμβολίζουμε με $|s|$ το μήκος της εισόδου.

Υπολογιστικό Πρόβλημα. Προσδιορίζουμε ένα υπολογιστικό πρόβλημα X με το σύνολο των αλφαριθμητικών για τα οποία η απάντηση είναι "ναι".

Αλγόριθμος. Ένας αλγόριθμος A *επιλύει* το πρόβλημα X αν, για όλα τα αλφαριθμητικά s, έχουμε

$$A(s) = \text{ναι} \quad \text{αν και μόνο αν } s \in X.$$

Πολυωνυμικός Χρόνος. Ο αλγόριθμος τρέχει σε πολυωνυμικό χρόνο αν για κάθε αλφαριθμητικό s, $A(s)$ τερματίζει μετά από το πολύ $p(|s|)$ βήματα όπου $p(\cdot)$ είναι μια πολυωνυμική συνάρτηση.

Κλάση Προβλημάτων $\mathcal{P}$

$\mathcal{P}$. Σύνολο προβλημάτων απόφασης για τα οποία υπάρχει πολυωνυμικός αλγόριθμος.

Είδαμε πολλά προβλήματα στα προηγούμενα κεφάλαια τα οποία ανήκουν στην κλάση $\mathcal{P}$.

Πιστοποιητής

Ένας ”ελεγκτικός αλγόριθμος” για ένα πρόβλημα X έχει διαφορετική δομή από έναν αλγόριθμο που προσπαθεί να λύσει το πρόβλημα.

Χρειαζόμαστε

1. το αλφαριθμητικό εισόδου s,
2. ένα αλφαριθμητικό ”πιστοποίησης” t που περιέχει την μαρτυρία ότι το s είναι ένα στιγμιότυπο ”ναι” του X.

Αποδοτικός Πιστοποιητής.

Το $C(s, t)$ είναι ένας πιστοποιητής για το πρόβλημα X αν ισχύουν οι ακόλουθες ιδιότητες.

1. Το C είναι ένας αλγόριθμος πολυωνυμικού χρόνου που δέχεται δύο ορίσματα εισόδου s και t.
2. Υπάρχει μια πολυωνυμική συνάρτηση $p(\cdot)$ τέτοια ώστε,

για κάθε αλφαριθμητικό s, **αν και μόνο αν** ισχύει $s \in X$ υπάρχει αλφαριθμητικό t με $|t| \leq p(|s|)$ όπου $C(s, t) =$ ναι

Κλάση Προβλημάτων $\mathcal{NP}$

$\mathcal{NP}$. Σύνολο προβλημάτων απόφασης για τα οποία υπάρχει αποδοτικός πιστοποιητής.

3-SAT

3-SAT. Δεδομένου ενός CNF τύπου Φ όπου κάθε όρος έχει ακριβώς τρία στοιχεία, υπάρχει ικανοποιούσα ανάθεση τιμών αληθείας;

π.χ

$$(\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (\bar{x}_1 \vee \bar{x}_3 \vee \bar{x}_4)$$

Πιστοποιητής 3-SAT

Είσοδος.

- CNF τύπος Φ με n μεταβλητές όπου κάθε όρος έχει ακριβώς τρία στοιχεία
- Μία ανάθεση τιμών στις n μεταβλητές

Αλγόριθμος Πιστοποιητή.

Ελέγχει πως κάθε όρος έχει τουλάχιστον ένα στοιχείο που είναι ”αληθής”.

3-SAT και Πιστοποιητής

π.χ

Στιγμιότυπο s

$$(\bar{x_1} \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x_2} \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (\bar{x_1} \vee \bar{x_3} \vee \bar{x_4})$$

Πιστοποιητικά t

$x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1 \Rightarrow$ ΝΑΙ

$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1 \Rightarrow$ ΟΧΙ

3-SAT και Πιστοποιητής

π.χ

Στιγμιότυπο s

$$(\bar{x_1} \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x_2} \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (\bar{x_1} \vee \bar{x_3} \vee \bar{x_4})$$

Πιστοποιητικά t

$x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 0, x_3 = 0, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 1, x_3 = 0, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 1 \Rightarrow$ ΝΑΙ

$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 0, x_3 = 1, x_4 = 1 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 0 \Rightarrow$ ΟΧΙ
$x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 0 \Rightarrow$ ΝΑΙ
$x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1 \Rightarrow$ ΟΧΙ

Ο πιστοποιητής επιστρέφει ΝΑΙ σε τουλάχιστον ένα πιστοποιητικό.

3-SAT και Πιστοποιητής

π.χ

Στιγμιότυπο s

$$(x \vee y \vee z) \wedge (x \vee \bar{y}) \wedge (y \vee \bar{z}) \wedge (z \vee \bar{x}) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}),$$

πιστοποιητικά t

$$x = 0, y = 0, z = 0 \Rightarrow \text{ OXI}$$
$$x = 0, y = 0, z = 1 \Rightarrow \text{ OXI}$$
$$x = 0, y = 1, z = 0 \Rightarrow \text{ OXI}$$
$$x = 0, y = 1, z = 1 \Rightarrow \text{ OXI}$$
$$x = 1, y = 0, z = 0 \Rightarrow \text{ OXI}$$
$$x = 1, y = 0, z = 1 \Rightarrow \text{ OXI}$$
$$x = 1, y = 1, z = 0 \Rightarrow \text{ OXI}$$
$$x = 1, y = 1, z = 1 \Rightarrow \text{ OXI}$$

3-SAT και Πιστοποιητής

π.χ

Στιγμιότυπο s

$$(x \vee y \vee z) \wedge (x \vee \bar{y}) \wedge (y \vee \bar{z}) \wedge (z \vee \bar{x}) \wedge (\bar{x} \vee \bar{y} \vee \bar{z}),$$

πιστοποιητικά t

$$x = 0, y = 0, z = 0 \Rightarrow \text{ ΟΧΙ}$$
$$x = 0, y = 0, z = 1 \Rightarrow \text{ ΟΧΙ}$$
$$x = 0, y = 1, z = 0 \Rightarrow \text{ ΟΧΙ}$$
$$x = 0, y = 1, z = 1 \Rightarrow \text{ ΟΧΙ}$$
$$x = 1, y = 0, z = 0 \Rightarrow \text{ ΟΧΙ}$$
$$x = 1, y = 0, z = 1 \Rightarrow \text{ ΟΧΙ}$$
$$x = 1, y = 1, z = 0 \Rightarrow \text{ ΟΧΙ}$$
$$x = 1, y = 1, z = 1 \Rightarrow \text{ ΟΧΙ}$$

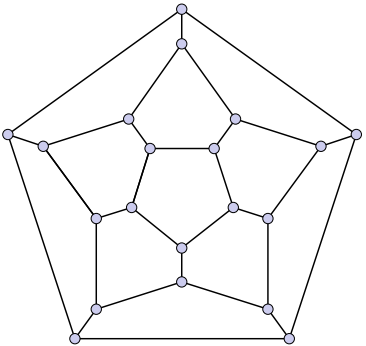
Ο πιστοποιητής επιστρέφει ΟΧΙ με όλα τα παραπάνω πιστοποιητικά.

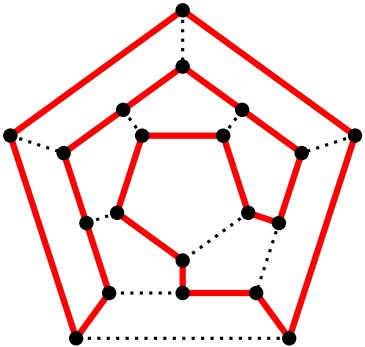
3-SAT

Συμπέρασμα. SAT $\in \mathcal{NP}$

Κύκλος Hamilton

Κύκλος Hamilton (HAM-CYCLE). Δεδομένου ενός γραφήματος $G = (V, E)$, υπάρχει ένα απλός κύκλος C που να επισκέπτεται όλους τους κόμβους;





Πιστοποιητής Κύκλου Hamilton

Είσοδος.

- Ένα γράφημα $G(V, E)$ με n κόμβους και m ακμές
- Μία μετάθεση των n κόμβων

Αλγόριθμος Πιστοποιητή.

Ελέγχει πως:

1. η μετάθεση περιέχει κάθε κόμβο του V ακριβώς μια φορά, και
2. οτι υπάρχει ακμή μεταξύ κάθε ζεύγους γειτονικών κόμβων στη μετάθεση.

Κύκλος Hamilton

Συμπέρασμα. HAM-CYCLE $\in \mathcal{NP}$.

Κλάση Προβλημάτων $\mathcal{NP}$

Θεώρημα

$\mathcal{P} \subseteq \mathcal{NP}$

Θεώρημα

$\mathcal{P} \subseteq \mathcal{NP}$

Απόδειξη

Έστω πως $X \in \mathcal{P}$. Άρα υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου A που λύνει το X. Θα δείξουμε πως υπάρχει ένας αποδοτικός πιστοποιητής B για το X, και άρα $X \in \mathcal{NP}$.

□

Θεώρημα

$\mathcal{P} \subseteq \mathcal{NP}$

Απόδειξη

Έστω πως $X \in \mathcal{P}$. Άρα υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου A που λύνει το X. Θα δείξουμε πως υπάρχει ένας αποδοτικός πιστοποιητής B για το X, και άρα $X \in \mathcal{NP}$.

Σχεδιάζουμε τον πιστοποιητή B με τον εξής τρόπο. Μόλις μας παρουσιαστεί το ζεύγος εισόδου (s, t), ο πιστοποιητής επιστρέφει απλώς την τιμή $A(s)$. Ουσιαστικά ο B απλά αδιαφορεί για την προτεινόμενη απόδειξη t και λύνει το πρόβλημα μόνος του.

□

Θεώρημα

$\mathcal{P} \subseteq \mathcal{NP}$

Απόδειξη

Έστω πως $X \in \mathcal{P}$. Άρα υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου A που λύνει το X. Θα δείξουμε πως υπάρχει ένας αποδοτικός πιστοποιητής B για το X, και άρα $X \in \mathcal{NP}$.

Σχεδιάζουμε τον πιστοποιητή B με τον εξής τρόπο. Μόλις μας παρουσιαστεί το ζεύγος εισόδου (s, t), ο πιστοποιητής επιστρέφει απλώς την τιμή $A(s)$. Ουσιαστικά ο B απλά αδιαφορεί για την προτεινόμενη απόδειξη t και λύνει το πρόβλημα μόνος του.

Είναι αποδοτικός επειδή

- είναι πολυωνυμικός αφού ο A είναι πολυωνυμικός
- αν ένα αλφαριθμητικό $s \in X$, τότε για κάθε t μήκους το πολύ $p(|s|)$ έχουμε $B(s, t) =$ ναι,
- αν $s \notin X$, τότε για κάθε t μήκους το πολύ $p(|s|)$ έχουμε $B(s, t) =$ όχι.

□

Κλάση Προβλημάτων $\mathcal{EXP}$

$\mathcal{EXP}$. Σύνολο προβλημάτων απόφασης που μπορούν να λυθούν από αλγορίθμους εκθετικού χρόνου.

Κλάση Προβλημάτων $\mathcal{EXP}$

$\mathcal{EXP}$. Σύνολο προβλημάτων απόφασης που μπορούν να λυθούν από αλγορίθμους εκθετικού χρόνου.

Θεώρημα

$\mathcal{NP} \subseteq \mathcal{EXP}$

Κλάση Προβλημάτων $\mathcal{EXP}$

$\mathcal{EXP}$. Σύνολο προβλημάτων απόφασης που μπορούν να λυθούν από αλγορίθμους εκθετικού χρόνου.

Θεώρημα

$\mathcal{NP} \subseteq \mathcal{EXP}$

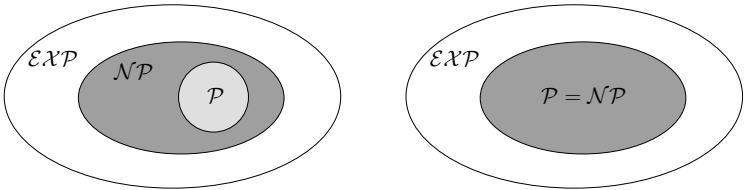
Απόδειξη

Έστω ένα πρόβλημα $X \in \mathcal{NP}$. Υπάρχει από την υπόθεση ένας πολυωνυμικός πιστοποιητής $C(s, t)$ για το X.
Δεδομένου μιας εισόδου s για το πρόβλημα, τρέχουμε τον πιστοποιητή $C(s, t)$ για κάθε αλφαριθμητικό t με $|t| \leq p(|s|)$.
Επιστρέφουμε ναι, αν ο $C(s, t)$ επιστρέψει ναι για κάποιο από αυτά τα αλφαριθμητικά.
Ο αλγόριθμος είναι ωμής βίας και επειδή υπάρχει εκθετικός αριθμός πιστοποιητικών, ανήκει στην $\mathcal{EXP}$. □

Το Ερώτημα $\mathcal{P} = \mathcal{NP}$;

Ισχύει $\mathcal{P} = \mathcal{NP}$;

- Είναι το πρόβλημα απόφασης όσο εύκολο είναι το πρόβλημα της πιστοποίησης;
- Clay $1 million prize
  http://www.claymath.org/millennium



Αν ναι: Αποδοτικοί αλγόριθμοι για SAT, VERTEX COVER, ...
Αν οχι: Δεν υπάρχουν αποδοτικοί αλγόριθμοι για SAT, VERTEX COVER, ...

Άποψη Κοινότητας. Μάλλον $\mathcal{P} \neq \mathcal{NP}$.

NP-Πλήρη Προβλήματα

Αφού δεν έχουμε πρόοδο όσο αναφορά το ερώτημα $\mathcal{P} = \mathcal{NP}$, στραφήκαμε σε πιο βατά ερωτήματα.

Ερώτημα. Ποια είναι τα δυσκολότερα προβλήματα στην κλάση $\mathcal{NP}$;

NP-Πλήρη Προβλήματα

Αφού δεν έχουμε πρόοδο όσο αναφορά το ερώτημα $\mathcal{P} = \mathcal{NP}$, στραφήκαμε σε πιο βατά ερωτήματα.

Ερώτημα. Ποια είναι τα δυσκολότερα προβλήματα στην κλάση $\mathcal{NP}$;

Δυσκολότερα προβλήματα της $\mathcal{NP}$.
Αν για ένα πρόβλημα X ισχύουν οι παρακάτω δύο ιδιότητες:

1. $X \in \mathcal{NP}$,
2. για όλα τα $Y \in \mathcal{NP}$, έχουμε $Y \leq_p X$.

ονομάζουμε το πρόβλημα X ένα **NP-πλήρες** (NP-Complete) πρόβλημα.

NP-Πλήρη Προβλήματα

Αφού δεν έχουμε πρόοδο όσο αναφορά το ερώτημα $\mathcal{P} = \mathcal{NP}$, στραφήκαμε σε πιο βατά ερωτήματα.

Ερώτημα. Ποια είναι τα δυσκολότερα προβλήματα στην κλάση $\mathcal{NP}$;

Δυσκολότερα προβλήματα της $\mathcal{NP}$.
Αν για ένα πρόβλημα X ισχύουν οι παρακάτω δύο ιδιότητες:

1. $X \in \mathcal{NP}$,
2. για όλα τα $Y \in \mathcal{NP}$, έχουμε $Y \leq_p X$.

ονομάζουμε το πρόβλημα X ένα **NP-πλήρες** (NP-Complete) πρόβλημα.

NP-Δύσκολο. Ονομάζουμε ένα πρόβλημα **NP-Δύσκολο** (NP-Hard) εαν ισχύει η ιδιότητα (2) που φαίνεται παραπάνω, αλλά όχι υποχρεωτικά και η (1).

Λήμμα

Υποθέστε ότι το X είναι ένα NP-πλήρες πρόβλημα. Τότε το X λύνεται σε πολυωνυμικό χρόνο αν και μόνο αν $\mathcal{P} = \mathcal{NP}$.

Λήμμα

Υποθέστε ότι το X είναι ένα NP-πλήρες πρόβλημα. Τότε το X λύνεται σε πολυωνυμικό χρόνο αν και μόνο αν $\mathcal{P} = \mathcal{NP}$.

Απόδειξη

Αν $\mathcal{P} = \mathcal{NP}$, τότε το $X \in P$ και άρα λύνεται σε πολυωνυμικό χρόνο.

Αντιστρόφως, υποθέστε πως το X λύνεται σε πολυωνυμικό χρόνο. Αν το $Y \in \mathcal{NP}$, τότε λόγω της NP-πληρότητας του X έχουμε πως $Y \leq_p X$ και άρα το Y μπορεί να λυθεί σε πολυωνυμικό χρόνο (χρησιμοποιώντας ένα πολυωνυμικό αλγόριθμο για το X στο μαύρο κουτί). Καταλήγουμε πως $\mathcal{NP} \subseteq \mathcal{P}$ και αφού ξέρουμε πως $\mathcal{P} \subseteq \mathcal{NP}$ ισχύει πως $\mathcal{P} = \mathcal{NP}$. □

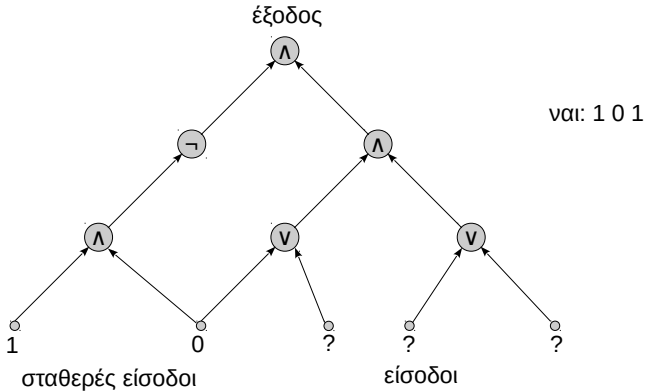
Πρώτο NP-Πλήρες Πρόβλημα

Έχουμε ορίσει την έννοια ενός NP-πλήρες προβλήματος, αλλά δεν έχουμε αποδείξει πως υπάρχει ένα NP-πλήρες πρόβλημα.

Ικανοποιησιμότητα Κυκλώματος

CIRCUIT-SAT

Δεδομένου ενός συνδυαστικού κυκλώματος που αποτελείται από AND, OR, και NOT πύλες, υπάρχει τρόπος να βάλουμε εισόδους ώστε το τελικό αποτέλεσμα να είναι 1 (αλήθεια);



ναι: 1 0 1

Πρώτο NP-Πλήρες Πρόβλημα

Ικανοποιησιμότητα Κυκλώματος. Θα αρκεστούμε να πούμε πως το 1971 οι Cook και Levin έδειξαν πως μπορούμε να κωδικοποιήσουμε κάθε πρόβλημα του $\mathcal{NP}$, χρησιμοποιώντας το πρόβλημα *Ικανοποιησιμότητας Κυκλώματος* (Circuit Satisfiability Problem).

Θεώρημα

Το πρόβλημα Ικανοποιησιμότητας Κυκλώματος είναι NP-πλήρες.

Γενική Στρατηγική Απόδειξης Νέων Προβλημάτων

Γνωρίζοντας το πρώτο NP-πλήρες πρόβλημα τα άλλα ακολουθούν.

Στρατηγική.
Έχοντας ένα νέο πρόβλημα X, για να αποδείξουμε πως είναι NP-πλήρες:

1. Αποδεικνύουμε ότι $X \in \mathcal{NP}$.
2. Επιλέγουμε ένα πρόβλημα Y που είναι γνωστό πως είναι NP-πλήρες.
3. Αποδεικνύουμε πως $Y \leq_p X$.

Γενική Στρατηγική Απόδειξης Νέων Προβλημάτων

Γνωρίζοντας το πρώτο NP-πλήρες πρόβλημα τα άλλα ακολουθούν.

Στρατηγική.
Έχοντας ένα νέο πρόβλημα X, για να αποδείξουμε πως είναι NP-πλήρες:

1. Αποδεικνύουμε ότι $X \in \mathcal{NP}$.
2. Επιλέγουμε ένα πρόβλημα Y που είναι γνωστό πως είναι NP-πλήρες.
3. Αποδεικνύουμε πως $Y \leq_p X$.

Γιατί;
Έστω W ένα οποιοδήποτε πρόβλημα που ανήκει στην $\mathcal{NP}$. Τότε $W \leq_p Y$ αφού το Y είναι NP-πλήρες.
Αφού αποδείξουμε πως $Y \leq_p X$, το αποτέλεσμα ακολουθεί λόγω μεταβατικής ιδιότητας των αναγωγών.

Άλλα NP-Πλήρες Προβλήματα

3-SAT. Είναι δυνατό να δείξουμε πως

$$\text{Ικανοποιησιμότητα Κυκλώματος} \leq_p \text{3-SAT}$$

και τελικά να βγάλουμε το συμπέρασμα πως το 3-SAT είναι NP-πλήρες.

Άλλα NP-Πλήρες Προβλήματα

3-SAT. Είναι δυνατό να δείξουμε πως

$$\text{Ικανοποιησιμότητα Κυκλώματος} \leq_p \text{3-SAT}$$

και τελικά να βγάλουμε το συμπέρασμα πως το 3-SAT είναι NP-πλήρες.

Περισσότερα. Επειδή

$$\text{3-SAT} \leq_p \text{Ανεξάρτητο Σύνολο} \leq_p \text{Κάλυψη Κορυφών}$$

έχουμε πως τα προβλήματα Ανεξάρτητου Συνόλου και Κάλυψης Κορυφών είναι NP-πλήρη.

Περισσότερες Πληροφορίες

Για περισσότερες πληροφορίες

- Κεφάλαιο 8, του βιβλίου.
- Garey, Michael R.; Johnson, David S. (1979), Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman, ISBN 0-7167-1045-5
- Wikipedia.
  http://en.wikipedia.org/wiki/List_of_NP-complete_problems
- A compendium of NP optimization problems.
  http://www.csc.kth.se/~viggo/wwwcompendium/