Θεωρία Υπολογισμού

- Ασχολείται με την κατηγοριοποίηση των προβλημάτων σε ***κλάσεις πολυπλοκότητας*** (***complexity classes***) βάσει της δυσκολίας επιλύσεώς τους
- Χρήσιμο γιατί
  - Αποτρέπει ενασχόληση με άλυτα προβλήματα, π.χ., ατέρμων βρόχος
  - Εξηγεί γιατί ορισμένα προβλήματα, όσο μεγαλώνει η είσοδος, τόσο αργούν να τερματίσουν

Ιστορική Αναδρομή

- **Τέλη ’60 με αρχές ’70:** παρατηρήθηκε πως ορισμένα προβλήματα δεν επιδέχονταν πολυωνυμικής λύσεως
- **1971:** ο Cook απέδειξε πως αυτά τα προβλήματα σχετίζονται στενά μεταξύ τους -αρκεί ένα να λυθεί σε πολυωνυμικό χρόνο και όλα λύνονται! (κλάση **NPC**)

Η έννοια της εισόδου

- Το μέγεθος της εισόδου εξαρτάται από την υιοθετημένη κωδικοποίηση σε μπιτ
- Πρέπει να είναι ***εύλογα αποτελεσματική (reasonably efficient)*** –δηλαδή, να μην υπάρχει άλλη *σημαντικά* μικρότερη. Λ.χ., η αναπαράσταση των αριθμών με μοναδιαία κωδικοποίηση *δεν* είναι εύλογα αποτελεσματική, αφού υπάρχει, π.χ., η δυαδική με λογαριθμικό μέγεθος:

$$7=1111111\ ,\ 7=111\ (7=2^{\log 7})$$

Η έννοια της εισόδου (συν.)

- Υιοθετείται η σύμβαση πως η είσοδος x
  - περιγράφεται σε αλφάβητο Σ ($x \in \Sigma^*$), και
  - για την εσωτερική της αναπαράσταση χρησιμοποιείται μία εύλογα αποτελεσματική δυαδική αναπαράσταση

Προβλήματα Αποφάσεως

- Όλα όσα η λύση τους είναι μία καταφατική (‘ναι’) ή μία αποφατική (‘όχι’) απάντηση
- Μπορούν να μετατραπούν σε προβλήματα γενικά. Π.χ., η εύρεση του μήκους του μεγαλύτερου απλού μονοπατιού σε ένα γράφημα
- Είναι ισοδύναμα με προβλήματα αναγνωρίσεως γλώσσας

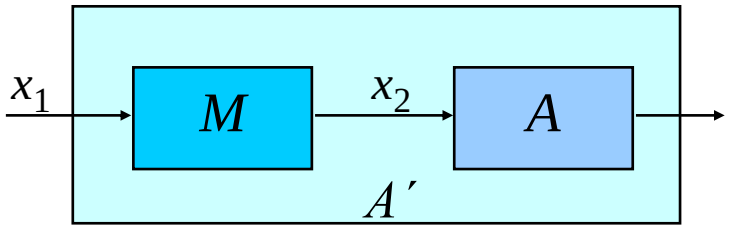
Προβλήματα Αναγνωρίσεως Γλώσσας

- Έστω $I \subseteq \Sigma^*$ όλες οι είσοδοι ενός προβλήματος **Π**. Τότε το σύνολο $L_{\mathbf{\Pi}} \subseteq \mathbf{\Pi}$ των εισόδων με καταφατική απάντηση ορίζεται ως ***γλώσσα του Π***.
- Έτσι
  - Το πρόβλημα αποφάσεως με είσοδο x ανάγεται στην διαπίστωση εάν $x \in L_{\mathbf{\Pi}}$
  - Λέμε τότε πως ο αλγόριθμος *Α αποφασίζει* μία γλώσσα L εάν μπορεί να αποφανθεί εάν μία είσοδος $x \in L$

Προβλήματα Αναγνωρίσεως Γλώσσας

- Πολυωνυμική Αναγωγή L_1 σε L_2 ($L_1 \propto L_2$)

  Υπάρχει αλγόριθμος που μετασχηματίζει μία είσοδο x_1 *της* L_1 *σε είσοδο* x_2 *της* L_2, *ώστε* $x_1 \in L_1$ *ανν* $x_2 \in L_2$



- Η $\propto$ είναι μεταβατική

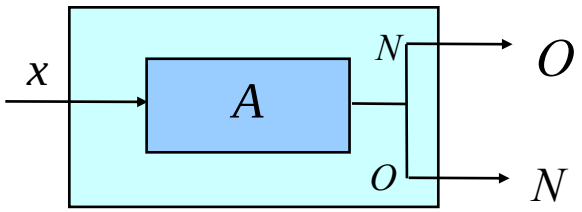
Η κλάση **P**

- Όλες οι γλώσσες που αποφασίζονται από κάποιον αλγόριθμο εντός πολυωνυμικού χρόνου
- Αυτά τα προβλήματα χαρακτηρίζονται ως ***πειθήνια (tractable)***

Η κλάση **co-P**

- **co-P**=$\{\Sigma^*-L, L\in$**P**$\}$
- **co-P=P (co-P**$\subseteq$**P** και **P**$\subseteq$**co-P)**

  Αρκεί να αντιστρέφεται η απάντηση!



Η κλάση **NP**

- Μη ντετερμινισμός

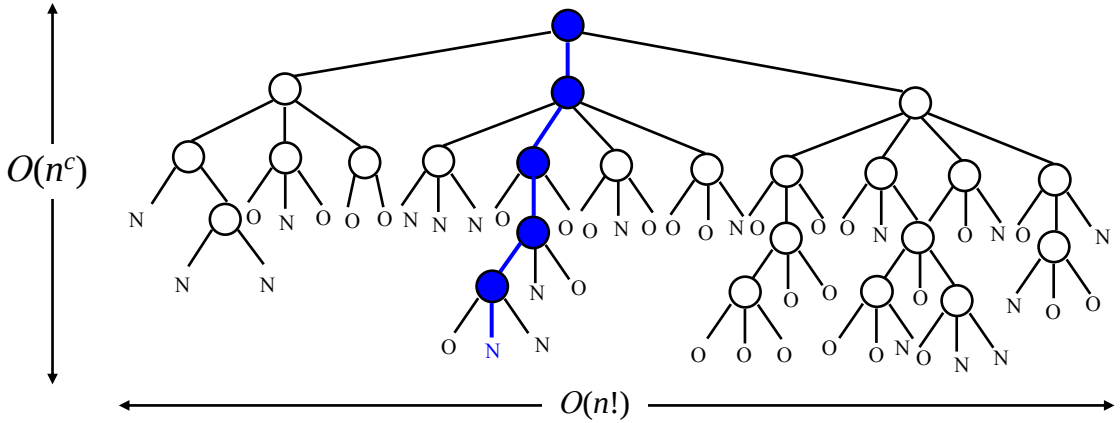
  Η δυνατότητα εκτελέσεως της εντολής «**μν-επιλογή**» (‘**nd-choice**’):

  Όταν υπάρχουν πολλαπλές επιλογές, με κάποιο …μαγικό τρόπο, η μν-επιλογή διαλέγει εκείνη που οδηγεί σε λύση (εάν, βεβαίως, υπάρχει)

Η κλάση **NP** (συν.)

- Τι πρακτικά σημαίνει;

  Δυνατότητα άπειρου παραλληλισμού!



Η κλάση **NP** (συν.)

- Ορισμός

  Σύνολο των προβλημάτων (γλωσσών) που λύνονται (γίνονται αποδεκτές) ***μη ντετερμινιστικά*** *εντός πολυωνυμικού χρόνου.*
- Παρατηρήστε πως ο ορισμός φράσσει ΜΟΝΟ τις καταφατικές λύσεις.
- Ως συνέπεια, δεν ξέρουμε πώς σχετίζεται η **co-NP** με την **NP**

Η κλάση **NP** (συν.)

- Εναλλακτικός ορισμός

  Η κλάση των προβλημάτων που μπορεί κανείς να τα επαληθεύσει εντός πολυωνυμικού χρόνου, μέσω ενός αλγορίθμου επαληθεύσεως A

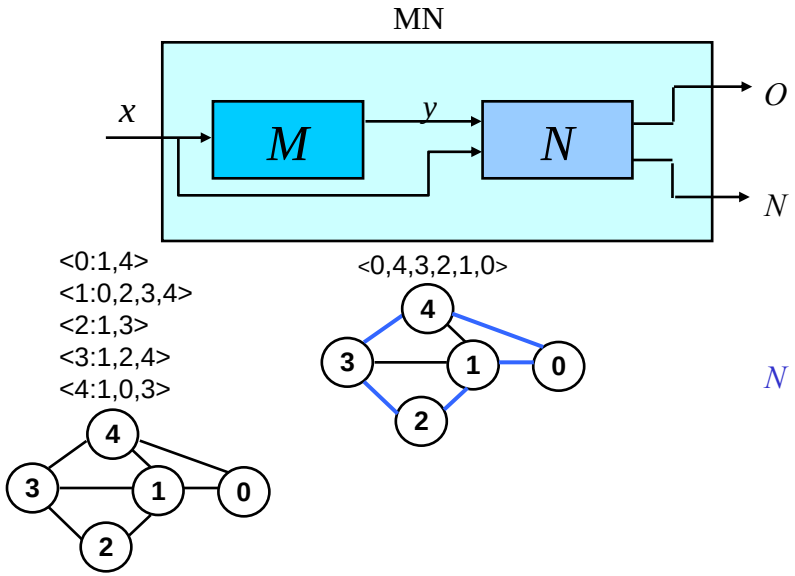
  Ο *A*, δεχόμενος μία είσοδο *x* και ένα πιστοποιητικό *y*, ελέγχει εάν $x \in L$. Εάν $x \notin L$ *δεν* πρέπει να υπάρχει αντίστοιχο πιστοποιητικό

Η κλάση **NP** (συν.)

- Παράδειγμα πιστοποιητικού για το πρόβλημα της ύπαρξης κύκλου Hamilton:
  - Μία ακολουθία κορυφών που συνιστούν έναν κύκλο Hamilton.
  - Εάν δεν υπάρχει, τότε δεν μπορεί κανείς να βρει πιστοποιητικό!

Η κλάση **NP** (συν.)

- Υπάρχει θεώρημα που αποδεικνύει την ισοδυναμία των δύο ορισμών. Οπότε, κάθε αλγόριθμος αποτελείται από δύο μέρη:
  - Μαντέματος, και
  - επαληθεύσεως.
- Π.χ., για κύκλο Hamilton



Το ερώτημα **P?NP**

- Προφανώς $\mathbf{P} \subseteq \mathbf{NP}$
- Το αντίστροφο $\mathbf{NP} \subseteq \mathbf{P}$ κανείς δεν το έχει απαντήσει!
- Έχει αποδειχθεί μόνον το θεώρημα πως:

  *Εάν μία γλώσσα ανήκει στο **NP**, τότε υπάρχει ντετερμινιστικός αλγόριθμος που την αποφασίζει σε εκθετικό χρόνο*

Η κλάση **NP**C

- Βοηθητική κλάση **NP-hard**

  Περιλαμβάνει όλες τις γλώσσες L με την ιδιότητα $L' \propto L$, $\forall L' \in$ **NP**
- $L \in$ **NPC** ανν:

  (i) $L \in$ **NP,** και

  (ii) $L \in$ **NP-hard**
- Το (ii) είναι δύσκολο. Γι' αυτό στην πράξη χρησιμοποιείται το ακόλουθο Λήμμα:

  $L \in$ **NPC** ανν (i) $L \in$ **NP**, και (ii) $\exists L' \in$ **NPC:** $L' \propto L$

  Απόδ. $L' \in$ **NPC** $\Rightarrow L'' \propto L'$, $\forall L'' \in$ **NP** $\Rightarrow L'' \propto L$, $\forall L'' \in$ **NP** (μεταβατικότητα της $\propto$) $\Rightarrow L \in$ **NP-hard**

Η κλάση **NPC** (συν.)

- Το προηγούμενο λήμμα είναι χρήσιμο *εφ' όσον υπάρχει κάποιο πρόβλημα που είναι* **NPC**
- Αυτό το έλυσε ο Cook το 1970, αποδεικνύοντας πως το πρόβλημα SAT:

  «Δοθείσης μίας λογικής εκφράσεως $p(x_1,x_2,\ldots,x_n)$ *αιτείται η διακρίβωση, εάν υπάρχει ανάθεση τιμών στις λογικές μεταβλητές που την ικανοποιούν»*

  είναι **NPC (Θεώρημα Cook)**

Αναγωγές

- Το θεώρημα τού Cook αξιοποιήθηκε από τον Karp το 1972, ο οποίος παρουσίασε έναν κατάλογο από 24 προβλήματα **NPC,** εισάγοντας την τεχνική των ***πολυωνυμικών αναγωγών***

Κατηγορίες Αναγωγών

- **Περιορισμός (Restriction)**

  Αποδεικνύεται πως ένα γνωστό πρόβλημα **NPC** *αποτελεί ειδική περίπτωση του υπό εξέταση. Απλή, θέλει, όμως, προσοχή!*
- **Τοπική Αντικατάσταση (Local Replacement)**

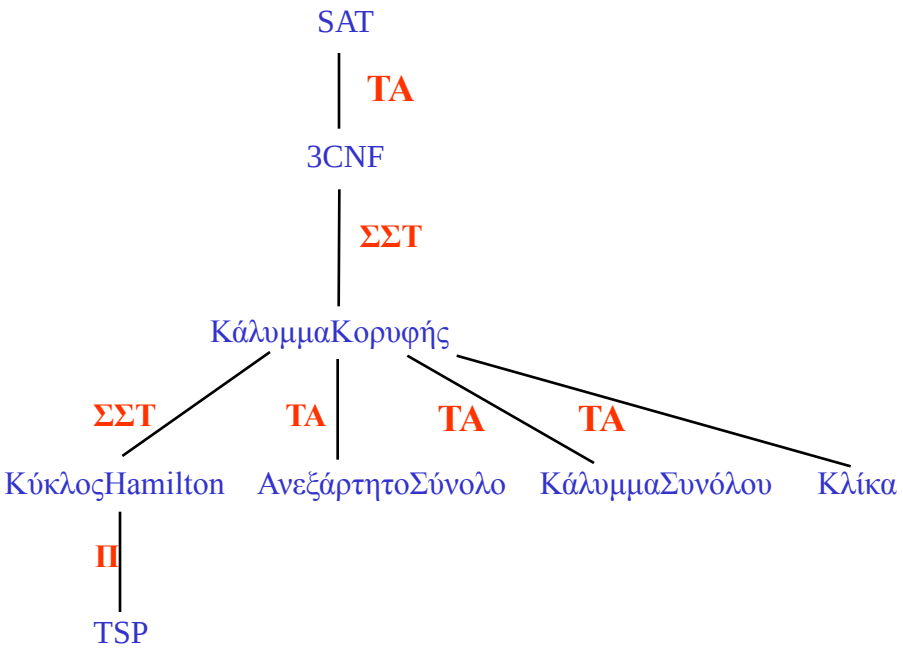
  Τμήματα (αντικείμενα) του ενός αντικαθίστανται από τμήματα (αντικείμενα) του άλλου. Δυσκολία επιλογής των αντικειμένων που θα αντικατασταθούν

Κατηγορίες Αναγωγών (συν.)

- **Σχεδιασμός Συνθετικών Τμημάτων (Component Design)**

  Σχεδιάζονται «συνθετικά» αντικείμενα, τα οποία χρησιμοποιούνται για την αναγωγή. Η δυσκολότερη περίπτωση

Παραδείγματα Αναγωγών



3CNF (ή 3SAT)

- Μία πρόταση είναι σε μορφή 3CNF (3-κανονική συζευκτική μορφή), όταν
  - αποτελεί σύζευξη λογικών υποπροτάσεων, και
  - κάθε λογική υποπρόταση είναι διάζευξη τριών δυαδικών μεταβλητών ή των αρνήσεών τους. Π.χ.,

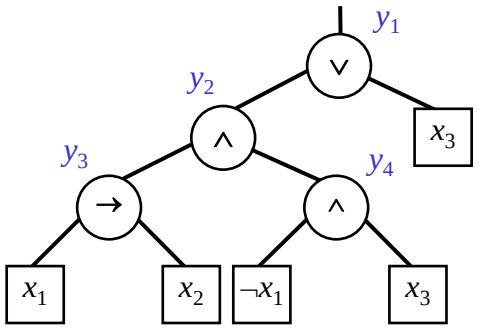
$$(x+y+\neg z)(\neg w+z+y)$$

- Το 3CNF είναι **NP**, καθώς μία ανάθεση τιμών αληθείας στις λογικές μεταβλητές αποτελεί και πιστοποιητικό
- Το SAT είναι **NPC** και θα το χρησιμοποιήσουμε για την αναγωγή με τοπική αντικατάσταση

Αναγωγή SAT σε 3CNF

- **1ο Βήμα**

  Ανάλυση σε συστατικά μέρη μέσω δυαδικού δένδρου αναλύσεως (parse tree), και εισαγωγή βοηθητικών μεταβλητών (για κάθε τελεστή, το πολύ μία νέα μεταβλητή και νέα υποπρόταση)



Από $(x_1 \rightarrow x_2) \wedge (\neg x_1 \wedge x_3) \vee x_3$ μετασχηματίζεται σε $y_1 \wedge (y_2 \leftrightarrow (y_3 \wedge y_4)) \wedge (y_3 \leftrightarrow (x_1 \rightarrow x_2)) \wedge (y_4 \leftrightarrow (\neg x_1 \wedge x_3)) \wedge (y_1 \leftrightarrow (y_2 \vee x_3))$

Αναγωγή SAT σε 3CNF (συν.)

- **2ο Βήμα**

  Κάθε υποπρόταση γίνεται διάζευξη, μέσω κανόνων De-Morgan και πινάκων αληθείας (διάζευξη της αρνήσεως των γραμμών που δίδουν 0). Π.χ.,

y_1	y_2	x_3	$(y_2 \vee x_3) \leftrightarrow y_1$	Γραμμές που κρατάμε	Άρνησή τους…
0	0	0	0 1		
0	**0**	**1**	**1** **0**	$(\neg y_1 \wedge \neg y_2 \wedge x_3)$	$(y_1 \vee y_2 \vee \neg x_3)$
0	**1**	**0**	**1** **0**	$(\neg y_1 \wedge y_2 \wedge \neg x_3)$	$(y_1 \vee \neg y_2 \vee x_3)$
0	**1**	**1**	**1** **0**	$(\neg y_1 \wedge y_2 \wedge x_3)$	$(y_1 \vee \neg y_2 \vee \neg x_3)$
1	**0**	**0**	**1** **0**	$(y_1 \wedge \neg y_2 \wedge \neg x_3)$	$(\neg y_1 \vee y_2 \vee x_3)$
1	0	1	1 1		
1	1	0	1 1		
1	1	1	1 1		

Οπότε παίρνουμε $y_1 \wedge (y_2 \vee y_1 \vee \neg x_3) \wedge (y_1 \vee \neg y_2 \vee x_3) \wedge \ldots \wedge (\neg y_4 \vee \neg x_1 \vee \neg x_3)$ (Για κάθε υποπρόταση, εισάγονται το πολύ 8 νέες)

Αναγωγή SAT σε 3CNF (συν.)

- **3ο Βήμα**

  Οι υποπροτάσεις των δύο ή της μίας μεταβλητής μετατρέπονται σε διαζεύξεις τριών μεταβλητών, με την χρήση νέων μεταβλητών (εισάγονται το πολύ 4 νέες):

  - $(y_k \vee y_l) \leftrightarrow (y_k \vee y_l \vee w) \wedge (y_k \vee y_l \vee \neg w)$
  - $y_k \leftrightarrow (y_k \vee w \vee z) \wedge (y_k \vee w \vee \neg z) \wedge (y_k \vee \neg w \vee z) \wedge (y_k \vee \neg w \vee \neg z)$

- Και τα τρία βήματα απαιτούν πολυωνυμικό χρόνο και πολυωνυμικό χώρο

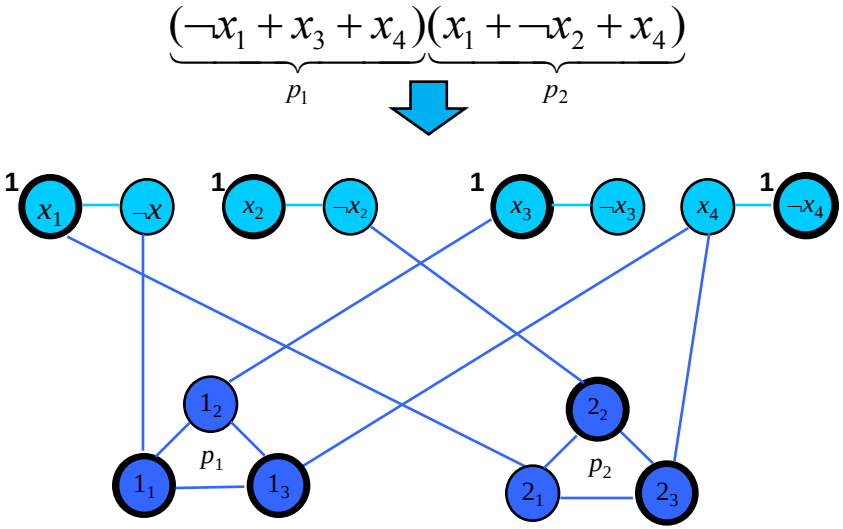
Κάλυμμα Κορυφής

- Είναι **NP**, καθώς
  - ένα σύνολο *k* κορυφών συνιστά ένα πιστοποιητικό
  - η επαλήθευση γίνεται σε πολυωνυμικό χρόνο:

    μία προς μία οι ακμές ελέγχονται εάν έχουν άκρα κάποιες από αυτές
- Για το **NP-Hard** τμήμα της αποδείξεως, θα χρησιμοποιήσουμε το 3CNF και την τεχνική του σχεδιασμού συνθετικών τμημάτων

3CNF∝VC

- 2 είδη συνθετικών τμημάτων:
  - το πρώτο αντιστοιχεί σε μία μεταβλητή και το συμπλήρωμά της
  - το δεύτερο στην υποπρόταση
- k = #μεταβλητών + 2#υποπροτάσεων



Απόδειξη Ισοδυναμίας

- ($\Rightarrow$) Η πρόταση ικανοποιείται.
  - Για κάθε μεταβλητή ή συμπλήρωμα μεταβλητής με 1, η αντίστοιχη κορυφή μπαίνει στο κάλυμμα
    - Έτσι καλύπτουμε τις ειδικές ακμές και τις ακμές που συνδέονται με τρίγωνο
  - Σε κάθε τρίγωνο, μία τουλάχιστον μεταβλητή/κορυφή θα είναι 1, οπότε συμπεριλαμβάνουμε στο κάλυμμα τις άλλες δύο
  - Άρα καλύπτονται όλες οι ακμές, και έχουμε ***ακριβώς*** k κορυφές στο κάλυμμα

Απόδειξη Ισοδυναμίας (συν.)

- ($\Leftarrow$) Έστω κάλυμμα μεγέθους k
  - Τότε, αναγκαστικά

    $$k = \#\text{μεταβλητών} + 2\#\text{υποπροτάσεων}$$

    ώστε να καλύπτονται οι ακμές εκτός τριγώνων και οι ακμές των τριγώνων
  - Εάν δώσουμε 1 σε κάθε κορυφή που συνδέεται με την εκτός καλύμματος κορυφή του αντίστοιχου τριγώνου, τότε έχουμε ικανοποιήσει την πρόταση

Ισοδυναμίες

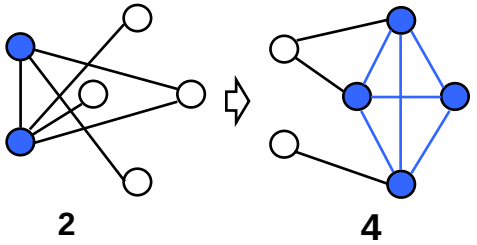
- Έστω γράφημα $G = (V, E)$ και $V' \subseteq V$. Τότε
  - V' κάλυμμα κορυφής $\Rightarrow$ V-V' ανεξάρτητο σύνολο
    Διαφορετικά, δεν θα καλυπτόταν η υποτιθέμενη ακμή
  - V-V' ανεξάρτητο σύνολο $\Rightarrow$ V-V' κλίκα του συμπληρώματος του G

    Ανά δύο δεν συνδέονται άρα στο συμπλήρωμα όλες θα διασυνδέονται
  - V-V' κλίκα του συμπληρώματος του $G \Rightarrow V'$ κάλυμμα κορυφής

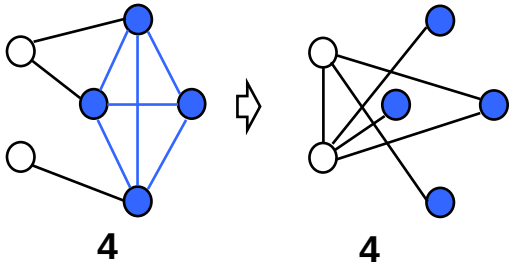
    Ανά δύο οι κορυφές του V-V' στο G δεν θα συνδέονται, άρα όλες οι ακμές του G έχουν τα άκρα τους στο V'

Αναγωγές

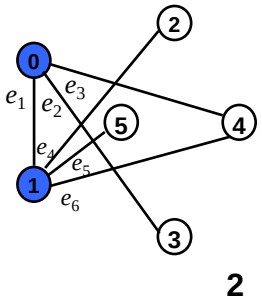
- VC $\propto$ Κλίκα
  συμπλήρωμα και ερώτημα με V-k



- Κλίκα $\propto$ IS
  συμπλήρωμα και ερώτημα με V



- VC $\propto$ CS
  V σύνολα ένα για κάθε κορυφή με τις προσπίπτουσες



$S_0=\{e_1, e_2, e_3\}$
$S_1=\{e_1, e_4, e_5, e_6\}$
$S_2=\{e_4\}$
$S_3=\{e_2\}$
$S_4=\{e_3, e_6\}$
$S_5=\{e_5\}$

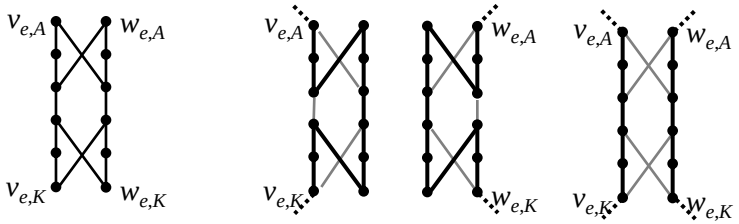
$S=\cup S_i=\{e_1, e_2, e_3, e_4, e_5, e_6\}$
$S_0 \cup S_1=S$

Κύκλος Hamilton

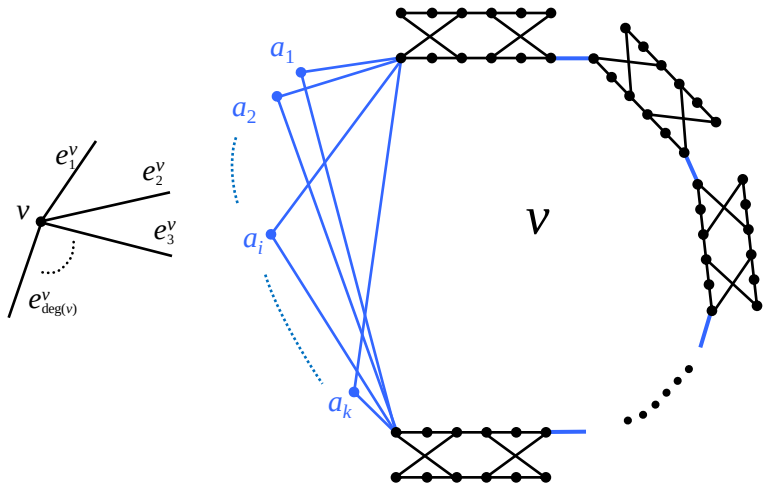
- Είναι **NP** καθώς
  - πιστοποιητικό αποτελεί μία ακολουθία κορυφών
  - εύκολα επαληθεύσιμο
- Για την απόδειξη του **NP-hard** θα χρησιμοποιήσουμε την τεχνική των συνθετικών τμημάτων στο κάλυμμα κορυφής

VC $\propto$ КύκλοςHamilton

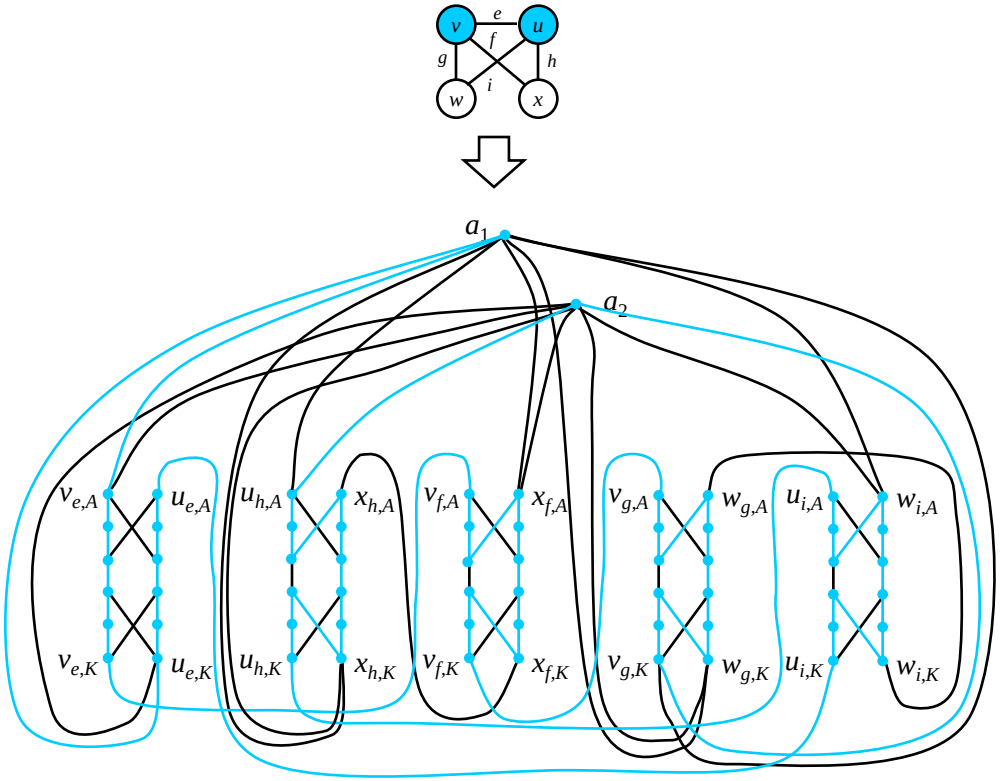
- 1ο συνθετικό:
  k κορυφές a_i,
  $\forall i \in [1,k]$



- 2ο συνθετικό:
  ένα για κάθε ακμή (v,w) του γραφήματος



Παράδειγμα



$\Rightarrow$ Διαπέραση περί των *v, u*

Οι *e, f, g* καλύπτονται από την *v*. Οπότε, ξεκινώντας από την a_1, πηγαίνουμε στην $v_{e,A}$ και συνεχίζουμε μόνο από την πλευρά της *v* μέχρι να βγούμε στην $v_{e,K}$, κατόπιν διαπερνούμε τα συνθετικά που αντιστοιχούν στις *f, g εξ ολοκλήρου από την πλευρά της v,* μεταβαίνουμε στην a_2, εισερχόμαστε και διαπερνούμε εξ ολοκλήρου τα συνθετικά των *h, i* και κατόπιν στο συνθετικό της *e* μόνο από την πλευρά της *u* και τέλος, κλείνουμε τον κύκλο μέσω της a_1

$\Leftarrow$ Εύρεση καλύμματος μέσω κύκλου Hamilton

Παρατηρήστε ότι τα τμήματα του κύκλου μεταξύ των κορυφών a_1, a_2 καλύπτουν τις αντίστοιχες ακμές του αρχικού γραφήματος περί των *v, u*

Απόδειξη

- ($\Rightarrow$) Έστω πως υπάρχει κύκλος Hamilton.
  - Οι ειδικές κορυφές τον τέμνουν σε «κομμάτια» με εκκίνηση και τερματισμό αυτές, τα οποία πρέπει να αντιστοιχούν σε προσπίπτουσες ακμές κορυφών.
- ($\Leftarrow$) Εάν υπάρχει κάλυμμα μεγέθους k, τότε
  - κατασκευάζουμε κύκλο Hamilton που τα τμήματά του περνούν από τις κορυφές a_i, ενδιάμεσα, εξαντλώντας τις συνιστώσες που αντιστοιχούν στην εκάστοτε κορυφή v_j.

TSP

- Είναι **NP** αφού
  - μία ακολουθία κορυφών αποτελούν ένα πιστοποιητικό επαληθεύσιμο σε πολυωνυμικό χρόνο.
- Είναι **NP-Hard** καθώς κύκλοςHamilton $\propto$ TSP
  - βάζοντας μοναδιαία βάρη στις ακμές, οπότε εύκολα προκύπτει πως

    κύκλος Hamilton $\Leftrightarrow$ TSP κόστους V

Ποια Εικασία Ισχύει