

Μη Ντετερμινισμός και NP-Πληρότητα

Δημήτρης Φωτάκης

Σχολή Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών

Εθνικό Μετσόβιο Πολυτεχνείο

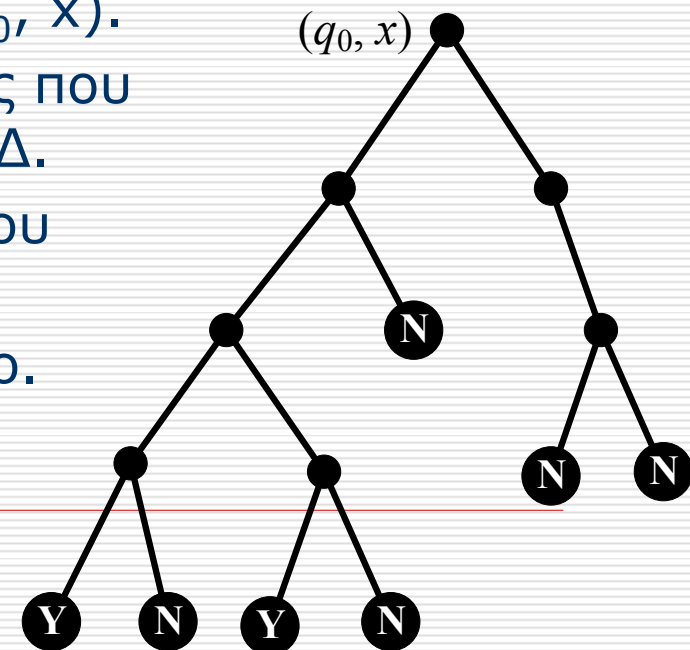


Μη Ντετερμινιστικές Μηχανές Turing

- Μη ντετερμινιστική Μηχ. Turing (NTM) $N \equiv (Q, \Sigma, \Delta, q_0, F)$
 - Q σύνολο καταστάσεων.
 - Σ αλφάβητο εισόδου και $\Gamma = \Sigma \cup \{\sqcup\}$ αλφάβητο ταινίας.
 - $q_0 \in Q$ αρχική κατάσταση.
 - $F \subseteq Q$ τελική κατάσταση (εστιάζουμε σε YES και NO).
 - $\Delta \subseteq ((Q \setminus F) \times \Gamma) \times (Q \times \Gamma \times \{L, R, S\})$ **σχέση** μετάβασης.
(κατάσταση q , διαβάζει a) \rightarrow **σύνολο** ενεργειών
(νέα κατάσταση q' , γράφει a' , κεφαλή μετακινείται L, R ή S).
- (Αρχική, τελική) **διαμόρφωση** όπως για DTM.
- Για κάθε τρέχουσα διαμόρφωση, υπάρχουν **καμία ή περισσότερες** επιτρεπτές επόμενες διαμορφώσεις όπου μπορεί DTM να μεταβεί!

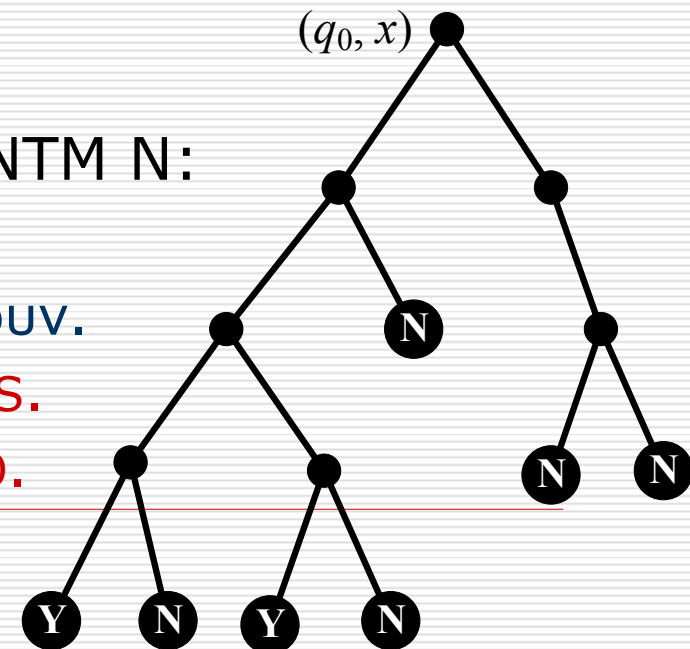
Μη Ντετερμινιστικές Μηχανές Turing

- Υπολογισμός NTM: **σχέση** \vdash και σχέση \vdash^* .
 - \vdash : διαμορφώσεις που προκύπτουν από τρέχουσα σε ένα βήμα.
 - \vdash^* : διαμορφώσεις που προκύπτουν σε κάποιο #βημάτων.
- Υπολογισμός NTM αναπαρίσταται με **δέντρο**:
 - Ρίζα: **αρχική** διαμόρφωση (q_0, x) .
 - **Κόμβοι**: όλες οι **διαμορφώσεις** που μπορεί να προκύψουν από **αρχική** διαμόρφωση (q_0, x) .
 - **Απόγονοι** κόμβου: όλες οι διαμορφώσεις που προκύπτουν με βάση σχέση μετάβασης Δ .
 - **Φύλλα**: όλες οι **τελικές** διαμορφώσεις που προκύπτουν από αρχική.
 - Βαθμός **σταθερός!** Χβτγ, **δυναμικό** δέντρο.
 - Υπολογισμός **DTM**: **μονοπάτι!**



Αποδοχή και Απόρριψη

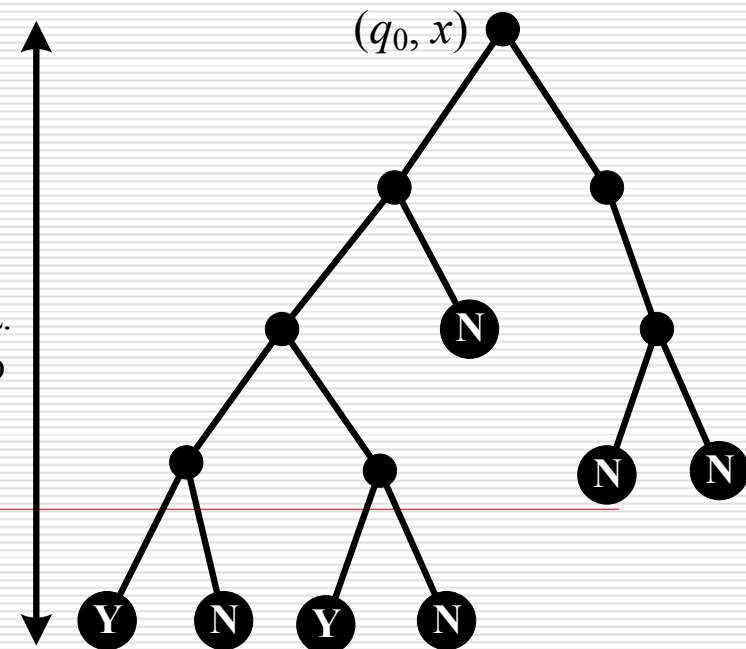
- NTM N έχει **πολλούς κλάδους** υπολογισμού («εκδοχές») που μπορεί να καταλήγουν σε **διαφορετικό αποτέλεσμα**.
 - Αποδέχεται αν **τουλάχιστον ένας** κλάδος αποδέχεται: «δικτατορία της αποδοχής»!
 - $N(x) = \text{YES}$ αν $(q_0, \underline{x_1 x_2 \dots x_n}) \vdash^* (\text{YES}, \dots)$
- Γλώσσα L **NTM-αποκρίσιμη** αν υπάρχει NTM N , $\forall x \in \Sigma^*$:
 - **όλοι** οι κλάδοι της $N(x)$ **τερματίζουν**, και $x \in L \Leftrightarrow N(x) = \text{YES}$
- Γλώσσα L **NTM-αποδεκτή** αν υπάρχει NTM N :
 - $\forall x \in \Sigma^*$, $x \in L \Leftrightarrow N(x) = \text{YES}$
 - Ενδέχεται κλάδοι $N(x)$ να μην τερματίζουν.
 - Όταν $x \in L$, τουλ. ένας τερματίζει σε **YES**.
 - Όταν $x \notin L$, όσοι τερματίζουν δίνουν **NO**.



Μη Ντετερμινιστική Χρονική Πολυπλοκότητα

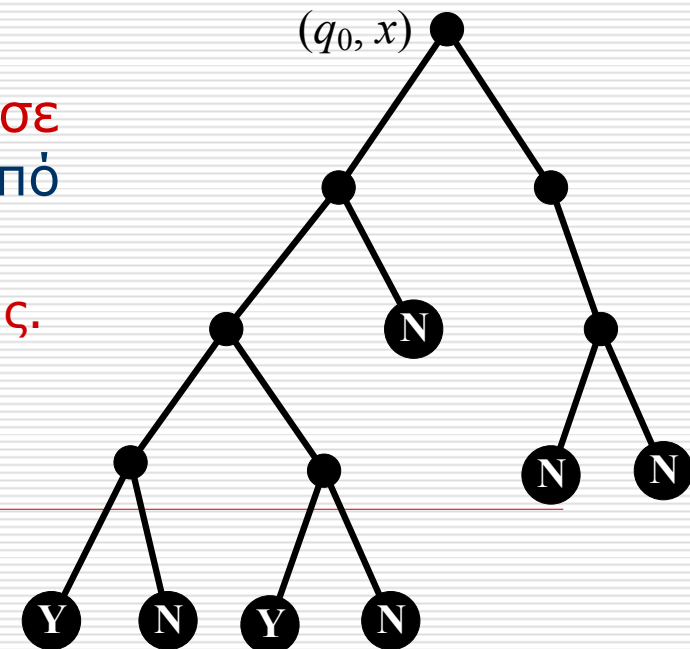
- Χρονική πολυπλοκότητα NTM N :
 - Αύξουσα συνάρτηση $t : \mathbb{N} \rightarrow \mathbb{N}$ ώστε για κάθε x , $|x| = n$, όλοι οι κλάδοι της $N(x)$ έχουν μήκος $\leq t(n)$.
 - Μέγιστο ύψος δέντρου υπολογισμού N με είσοδο μήκους n .
- Μη ντετερμινιστική χρονική πολυπλοκότητα προβλ. Π :
 - Χρονική πολυπλοκότητα «ταχύτερης» NTM που λύνει Π .
- Κλάση πολυπλοκότητας
 $\text{NTIME}[t(n)] \equiv \{\Pi : \Pi \text{ λύνεται σε μη ντετερμινιστικό χρόνο } O(t(n))\}$
- Όχι ρεαλιστικό μοντέλο, αλλά θεμελιώδες για Θεωρία Πολυπλοκότητας!

Χρονική Πολυπλ.
= Ύψος Δέντρου



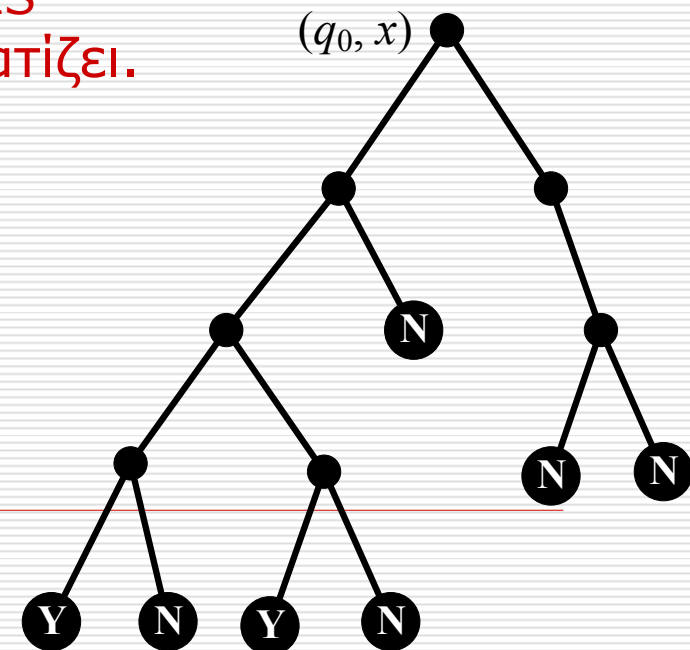
Μη Ντετερμινιστικός Υπολογισμός

- Ισοδύναμοι τρόποι για μη ντετερμινιστικό υπολογισμό:
 - $N(x)$ «**μαντεύει**» (πάντα σωστά) **κλάδο** που καταλήγει σε **YES** και **ακολουθεί μόνο αυτόν** (επιβεβαιώνει YES).
 - **Αναζήτηση** x σε πίνακα A με n στοιχεία:
«**Μάντεψε**» θέση k , και **επιβεβαίωσε** ότι $A[k] = x$.
 - **Hamilton Cycle**: «**Μάντεψε**» μετάθεση κορυφών και **επιβεβαίωσε** ότι δίνει HC.
 - **k -SAT**: «**Μάντεψε**» αποτίμηση και **επιβεβαίωσε** ότι ικανοποιεί φ .
 - Στο βήμα k , $N(x)$ «εκτελεί» / βρίσκεται σε **όλες** τις διαμορφώσεις σε **απόσταση k** από αρχική **ταυτόχρονα**.
 - «**Μηχανιστική**» **προσομοίωση νοημοσύνης**.
 - **Χρόνος** = ύψος δέντρου υπολογισμού.



Ντετερμινιστική Προσομοίωση

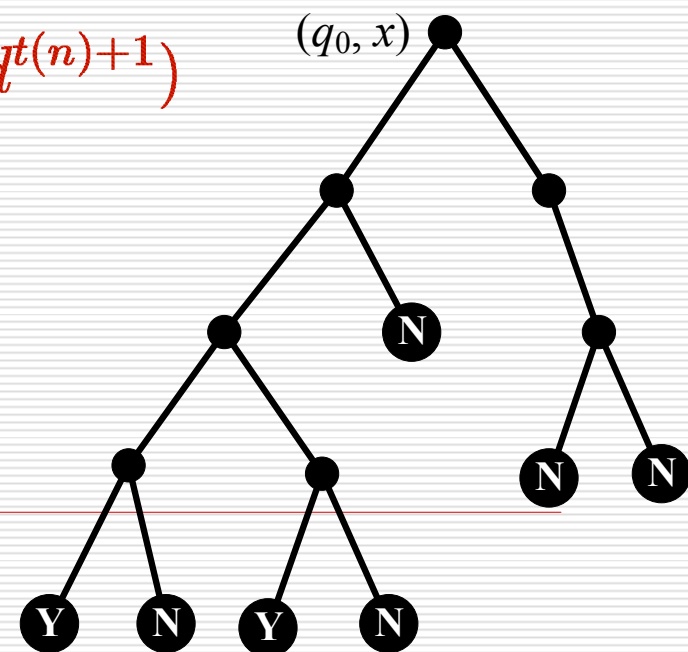
- Ντετερμινιστική **προσομοίωση NTM** με **εκθετική** επιβάρυνση.
 - Προσομοίωση δέντρου υπολογισμού με **BFS λογική**.
 - Για $t = 1, 2, \dots, t(|x|)$, **προσομοίωση όλων** των κλάδων υπολογισμού $N(x)$ **μήκους $\leq t$** .
 - Τερματισμός **YES**: **πρώτος** κλάδος που καταλήγει σε **YES**.
 - Τερματισμός **NO**: πρώτο t που **όλοι** οι κλάδοι **τερματίζουν σε NO**.
 - **Μη τερματισμός**: **κανένας** κλάδος σε **YES** και **κάποιος δεν τερματίζει**.
- NTM-αποκρίσιμο ανν DTM-αποκρίσιμο.
(Θέση Church-Turing)
- NTM-αποδεκτό ανν DTM-αποδεκτό.



NTIME και DTIME

- Ντετερμινιστική προσομοίωση NTM με εκθετική επιβάρυνση.
 - Για $t = 1, 2, \dots, t(|x|)$, προσομοίωση όλων των κλάδων υπολογισμού $N(x)$ μήκους $\leq t$.
 - Τερματισμός YES: πρώτος κλάδος που καταλήγει σε YES.
 - Τερματισμός NO: πρώτο t που όλοι οι κλάδοι τερματίζουν σε NO.
- Αν NTM χρόνου $t(n)$ και με βαθμό μη ντετερμινισμού d ,
χρόνος προσομοίωσης: $\sum_{t=1}^{t(n)} O(d^t) = O(d^{t(n)+1})$
- Κατά συνέπεια:

$$\text{NTIME}[t(n)] \subseteq \bigcup_{d>1} \text{DTIME}[d^{t(n)}]$$



Η Κλάση NP

- Προβλήματα που λύνονται σε πολυωνυμικό **μη ντετερμινιστικό** χρόνο: $NP \equiv \bigcup_{k \geq 0} NTIME[n^k]$
 - «YES-λύση» μπορεί να «μαντευθεί» σε πολυωνυμικό χρόνο (άρα πολυωνυμικού μήκους) και να επιβεβαιωθεί σε πολυωνυμικό **ντετερμινιστικό** χρόνο.
 - (k-)SAT, κύκλος Hamilton, TSP, Knapsack, MST, Shortest Paths, Max Flow, ... ανήκουν στην κλάση **NP**.
 - Χρειάζεται προσπάθεια για να σκεφθείτε πρόβλημα εκτός **NP**!
- Κλάση **NP** **κλειστή** ως προς ένωση, τομή, και πολυωνυμική αναγωγή.
 - Πιστεύουμε ότι κλάση **NP** **δεν** είναι **κλειστή** ως προς **συμπλήρωμα** (ασυμμετρία υπέρ αποδοχής).
 - **coNP**: αντίστοιχη κλάση με ασυμμετρία υπέρ **απόρριψης**.

NP και Συνοπτικά Πιστοποιητικά

- Σχέση $R \subseteq \Sigma^* \times \Sigma^*$ είναι:
 - πολυωνυμικά **ισορροπημένη** αν $\forall (x, y) \in R, |y| \leq \text{poly}(|x|)$
 - πολυωνυμικά **αποκρίσιμη** αν $(x, y) \in R$ ελέγχεται (ντετερμινιστικά) σε πολυωνυμικό χρόνο.
- $L \in \mathbf{NP}$ αν υπάρχει πολυωνυμικά **ισορροπημένη** και πολυωνυμικά **αποκρίσιμη** σχέση $R \subseteq \Sigma^* \times \Sigma^*$ ώστε
$$L = \{x \in \Sigma^* : \exists y \in \Sigma^*, (x, y) \in R\}$$
 - y αποτελεί «**σύντομο**» και «**εύκολο**» να ελεγχθεί **πιστοποιητικό** ότι $x \in L$.
- Αν υπάρχει τέτοια σχέση R , υπάρχει NTM N :
 - $\forall x \in L, N(x)$ «**μαντεύει**» πιστοποιητικό y και **επιβεβαιώνει** ότι $(x, y) \in R$ σε πολυωνυμικό χρόνο.

NP και Συνοπτικά Πιστοποιητικά

- $L \in \mathbf{NP}$ αν υπάρχει πολυωνυμικά **ισορροπημένη** και πολυωνυμικά **αποκρίσιμη** σχέση $R \subseteq \Sigma^* \times \Sigma^*$ ώστε

$$L = \{x \in \Sigma^* : \exists y \in \Sigma^*, (x, y) \in R\}$$

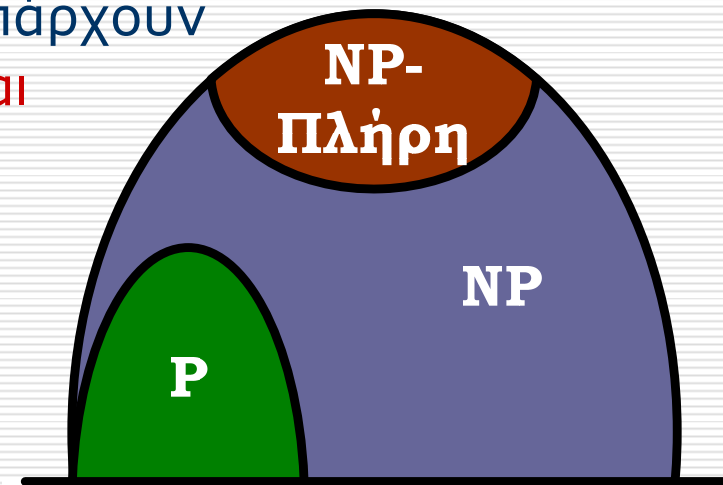
- Αν $L \in \mathbf{NP}$, θεωρούμε NTM N που αποφασίζει L .
 - Πιστοποιητικό y αποτελεί **κωδικοποίηση** μη ντετερμινιστικών επιλογών $N(x)$ που οδηγούν σε **YES**.
 $R = \{(x, y) : x \in L \text{ και } y \text{ κωδικοποιεί κλάδο } N(x) \text{ με YES}\}$
 - $|y| \leq \text{poly}(|x|)$ γιατί N πολυωνυμικού χρόνου.
 - $(x, y) \in R$ ελέγχεται πολυωνυμικά ακολουθώντας (**μόνο**) **κλάδο** υπολογισμού $N(x)$ που κωδικοποιείται από y .
 - $(x, y) \in R$ αν ο y -κλάδος $N(x)$ καταλήγει σε **YES**.

NP και Συνοπτικά Πιστοποιητικά

- Η κλάση **NP** περιλαμβάνει προβλήματα απόφασης:
 - Για κάθε **YES-στιγμιότυπο**, υπάρχει «**συνοπτικό**» πιστοποιητικό που ελέγχεται «**εύκολα**» (πολυωνυμικά).
 - Ένα τέτοιο πιστοποιητικό μπορεί να είναι **δύσκολο να υπολογισθεί**.
 - Δεν απαιτείται κάτι αντίστοιχο για **NO-στιγμιότυπα**.
 - Κλάση **coNP** περιλαμβάνει προβλήματα απόφασης που έχουν αντίστοιχο **πιστοποιητικό για NO-στιγμιότυπα**.
 - Αν πρόβλημα $\Pi \in \mathbf{NP}$, πρόβλημα $\text{co}\Pi = \{x : x \notin \Pi\} \in \mathbf{coNP}$.
 - Προβλήματα στο **P** ανήκουν **NP**
 - Προβλήματα στο **P** ανήκουν **coNP**
- } $\Rightarrow \mathbf{P} \subseteq \mathbf{NP} \cap \mathbf{coNP}$

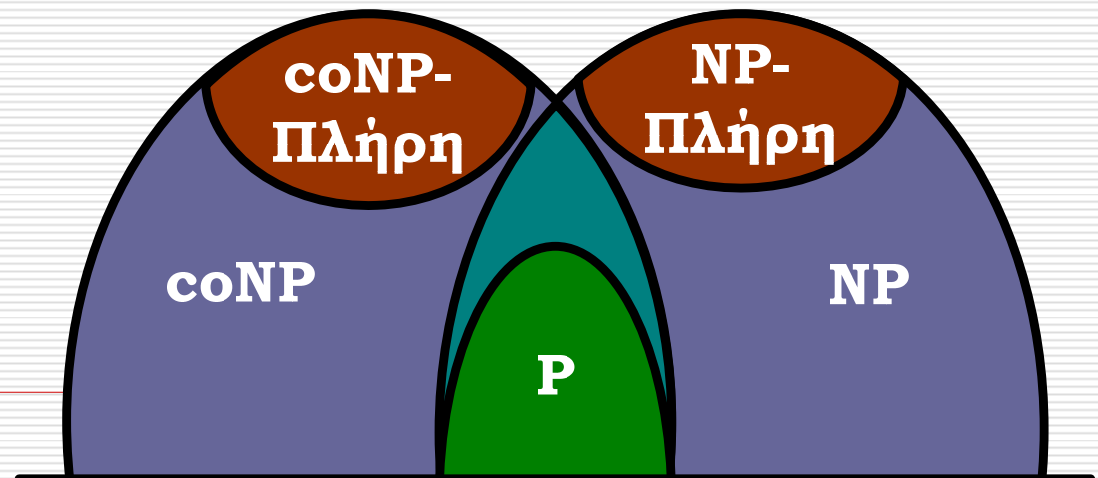
NP-Πληρότητα

- Πρόβλημα Π είναι **NP-πλήρες** αν $\Pi \in \mathbf{NP}$ και κάθε πρόβλημα $\Pi' \in \mathbf{NP}$ ανάγεται πολυωνυμικά στο Π ($\Pi' \leq_p \Pi$).
 - Π είναι από τα δυσκολότερα προβλήματα στο **NP** (όσον αφορά στον υπολογισμό πολυωνυμικού χρόνου).
- Π κάποιο **NP-πλήρες** πρόβλημα: $\Pi \in \mathbf{P}$ αν $\mathbf{P} = \mathbf{NP}$.
 - Αν $\mathbf{P} = \mathbf{NP}$, πολλά σημαντικά προβλήματα **ευεπίλυτα!**
 - Αν $\mathbf{P} \neq \mathbf{NP}$ (όπως όλοι πιστεύουν), υπάρχουν προβλήματα στο **NP** που **δεν** λύνονται σε **πολυωνυμικό** χρόνο!
 - Εξ' ορισμού, τα **NP-πλήρη** ανήκουν σε αυτή την κατηγορία.



NP-Πληρότητα

- Αντίστοιχα με **coNP** και **coNP-πλήρη** προβλήματα.
- Έστω προβλήματα $\Pi_1, \Pi_2 \in \mathbf{NP}$ ώστε $\Pi_1 \leq_P \Pi_2$. Ποιες από τις παρακάτω δηλώσεις αληθεύουν;
 1. $\Pi_1 \in \mathbf{P} \Rightarrow \Pi_2 \in \mathbf{P}$
 2. $\Pi_2 \in \mathbf{P} \Rightarrow \Pi_1 \in \mathbf{P}$
 3. Π_2 όχι NP-πλήρες $\Rightarrow \Pi_1$ όχι NP-πλήρες
 4. Π_1 NP-πλήρες $\Rightarrow \Pi_2 \leq_P \Pi_1$



SAT είναι NP-Πλήρες

- **Ικανοποιησιμότητα (SAT):**
 - Δίνεται λογική πρόταση φ σε CNF. Είναι φ ικανοποιήσιμη;
- **SAT \in NP.**
 - «Μαντεύουμε» ανάθεση τιμών αλήθειας a σε μεταβλητές φ .
 - Ελέγχουμε ότι ανάθεση a ικανοποιεί φ .
- **Θεώρημα Cook (1971):**
 - SAT είναι **NP**-πλήρες.
 - Υπολογισμός οποιασδήποτε NTM πολυωνυμικού χρόνου N με είσοδο x κωδικοποιείται σε CNF πρόταση $\varphi_{N,x}$:
 - $\varphi_{N,x}$ έχει μήκος πολυωνυμικό σε $|x|$ και $|N|$.
 - $\varphi_{N,x}$ υπολογίζεται σε χρόνο πολυωνυμικό σε $|x|$ και $|N|$.
 - $\varphi_{N,x}$ είναι ικανοποιήσιμη ανν $N(x) = \text{YES}$.

SAT είναι NP-Πλήρες

- Έστω NTM N $p(n)$ -χρόνου και είσοδος x , $|x| = n$.
- Για κωδικοποίηση $N(x)$, εισάγουμε 3 είδη μεταβλητών:
 - $Q[k, t]$: $N(x)$ βρίσκεται στην κατάσταση q_k την στιγμή t .
 - $H[j, t]$: κεφαλή βρίσκεται στη θέση j την στιγμή t .
 - $S[j, i, t]$: θέση j περιέχει σύμβολο s_i την στιγμή t .
$$0 \leq t \leq p(n), 0 \leq k \leq r, -p(n) \leq j \leq p(n), 0 \leq i \leq |\Gamma|$$
- Για κωδικοποίηση $N(x)$, εισάγουμε 7 ομάδες όρων:
 - G_1 : $N(x)$ βρίσκεται σε μία μόνο κατάσταση κάθε στιγμή.
 - G_2 : κεφαλή σε μία μόνο θέση κάθε στιγμή.
 - G_3 : κάθε θέση ταινίας περιέχει ένα μόνο σύμβολο κάθε στιγμή.
 - G_4 : $N(x)$ ξεκινά από αρχική διαμόρφωση (q_0, x) .
 - G_5 : $N(x)$ βρίσκεται σε κατάσταση YES την στιγμή $p(n)$.

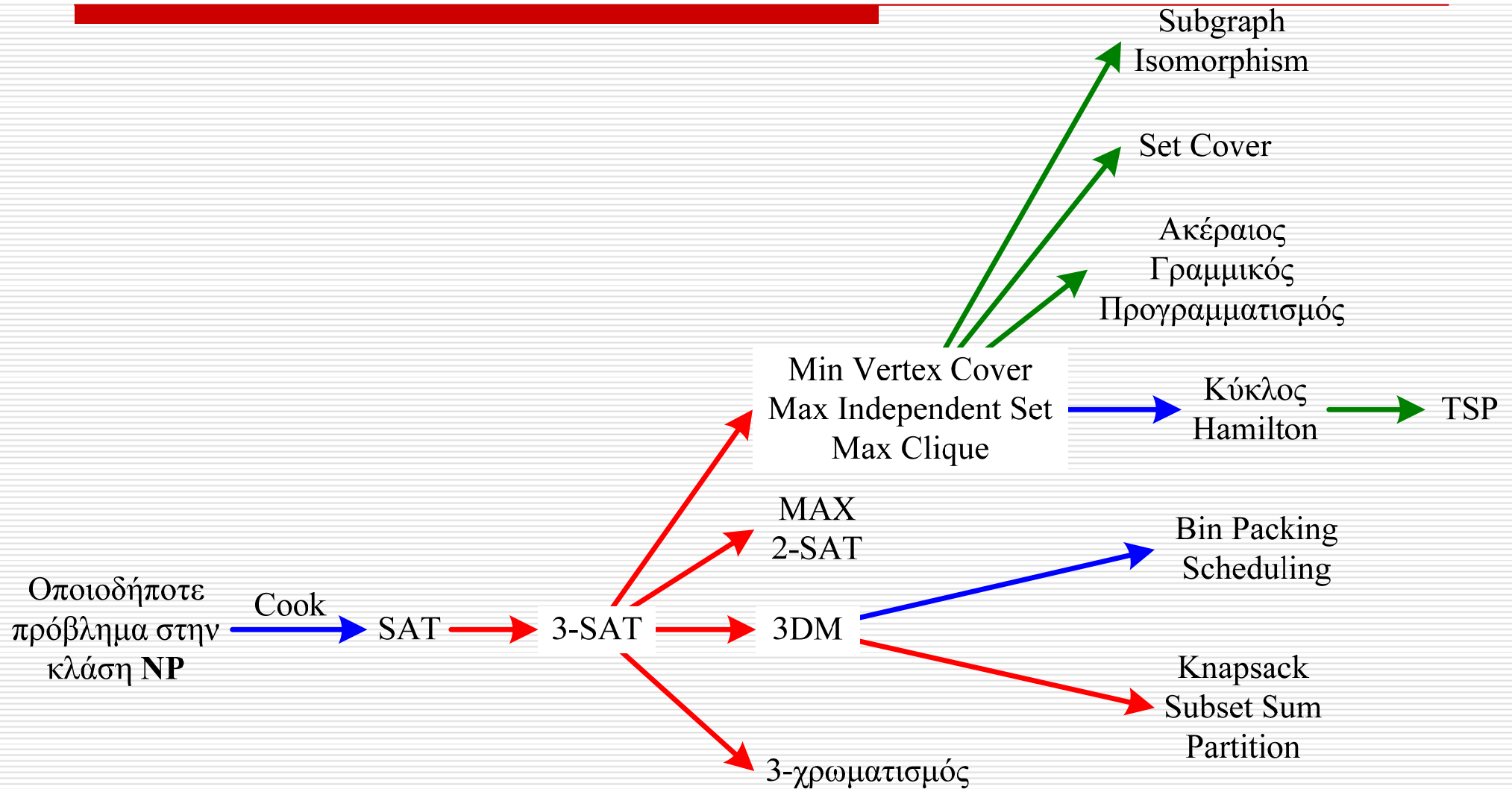
SAT είναι NP-Πλήρες

- Για κωδικοποίηση $N(x)$, εισάγουμε 7 ομάδες όρων:
 - G_6 : για κάθε t , μόνο το σύμβολο στη θέση όπου βρίσκεται η κεφαλή μπορεί να αλλάξει στην επόμενη στιγμή $t+1$.
 - G_7 : για κάθε t , η διαμόρφωση στην επόμενη στιγμή $t+1$ προκύπτει από την τρέχουσα διαμόρφωση με εφαρμογή της σχέσης μετάβασης Δ .
- Τελικά: $\varphi_{N,x} = G_1 \wedge G_2 \wedge G_3 \wedge G_4 \wedge G_5 \wedge G_6 \wedge G_7$
 - $\varphi_{N,x}$ έχει μήκος και κατασκευάζεται σε χρόνο $O(p^3(n))$ από περιγραφή N και είσοδο x .
 - $\varphi_{N,x}$ είναι ικανοποιήσιμη ανν $N(x) = \text{YES}$.

Αποδείξεις NP-Πληρότητας

- Απόδειξη ότι πρόβλημα (απόφασης) Π είναι **NP**-πλήρες:
 - Αποδεικνύουμε ότι $\Pi \in \mathbf{NP}$ (εύκολο, αλλά απαραίτητο!).
 - Επιλέγουμε (κατάλληλο) γνωστό **NP**-πλήρες πρόβλημα Π' .
 - **Ανάγουμε** πολυωνυμικά το Π' στο Π ($\Pi' \leq_p \Pi$):
 - Περιγράφουμε κατασκευή στιγμιότυπου $R(x)$ του Π από στιγμιότυπο x του Π' .
 - Εξηγούμε ότι $R(x)$ υπολογίζεται σε πολυωνυμικό χρόνο.
 - Αποδεικνύουμε ότι $x \in \Pi' \Leftrightarrow R(x) \in \Pi$.
- Αναγωγή με γενίκευση.
 - Π αποτελεί γενίκευση του Π' , και προφανώς Π είναι τουλάχιστον τόσο δύσκολο όσο το Π' .

Ακολουθία Αναγωγών



3-SAT είναι NP-Πλήρες

- **3-SAT**: λογική πρόταση φ σε **3-CNF**. Είναι φ ικανοποιήσιμη;
- **3-SAT** \in **NP** (όπως και SAT). Θδο **SAT** \leq_p **3-SAT**.
 - Έστω πρόταση $\psi = c_1 \wedge \dots \wedge c_m$ σε CNF.
 - Κατασκευάζουμε φ_ψ σε **3-CNF** αντικαθιστώντας κάθε όρο $c_j = \ell_{j_1} \vee \dots \vee \ell_{j_k}$, $k \geq 4$, με όρο
$$c'_j = (\ell_{j_1} \vee \ell_{j_2} \vee z_{j_1}) \wedge (\neg z_{j_1} \vee \ell_{j_3} \vee z_{j_2}) \wedge (\neg z_{j_2} \vee \ell_{j_4} \vee z_{j_3}) \wedge \dots \wedge (\neg z_{j_{k-4}} \vee \ell_{j_{k-2}} \vee z_{j_{k-3}}) \wedge (\neg z_{j_{k-3}} \vee \ell_{j_{k-1}} \vee \ell_{j_k})$$
 - c_j ικανοποιήσιμος αν c'_j ικανοποιήσιμος.
Αν ℓ_p πρώτο αληθές literal c_j , θέτουμε $z_{j_i} = \begin{cases} 1 & \text{αν } i < p - 1 \\ 0 & \text{αν } i \geq p - 1 \end{cases}$
 - Άρα φ_ψ ικανοποιήσιμη αν ψ ικανοποιήσιμη.
 - Και βέβαια, κατασκευή φ_ψ σε πολυωνυμικό χρόνο.

3-SAT(3) είναι NP-Πλήρες

- 3-SAT(3): στην φ κάθε μεταβλητή εμφανίζεται ≤ 3 φορές:
 - Είτε ≤ 1 χωρίς άρνηση και ≤ 2 με άρνηση, είτε ≤ 2 χωρίς άρνηση και ≤ 1 με άρνηση.
- Θδο $3\text{-SAT} \leq_p 3\text{-SAT}(3)$.
 - Έστω πρόταση $\psi = c_1 \wedge \dots \wedge c_m$ σε 3-CNF.
 - \forall μεταβλητή x που εμφανίζεται $k > 3$ φορές, αντικαθιστούμε κάθε εμφάνιση x με διαφορετική μεταβλητή x_1, x_2, \dots, x_k .
 - Προσθέτουμε όρους που ικανοποιούνται ανν οι x_1, x_2, \dots, x_k έχουν ίδια τιμή αλήθειας (εμφανίσεις ίδιας μετ/τής x):
$$(\neg x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge \dots \wedge (\neg x_{k-1} \vee x_k) \wedge (\neg x_k \vee x_1)$$
 - Έτσι κατασκευάζουμε 3-SAT(3) στιγμιότυπο ψ' :
 - ψ' ικανοποιήσιμη ανν ψ ικανοποιήσιμη.

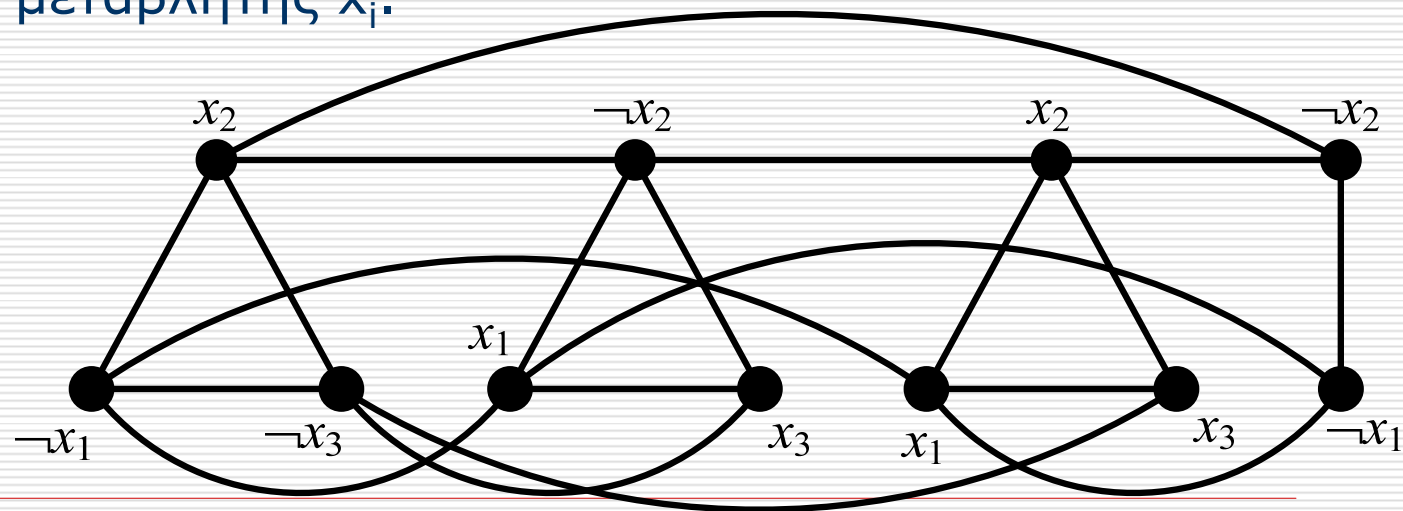
MAX 2-SAT είναι NP-Πλήρες

- **MAX 2-SAT:** (μη ικανοποιήσιμη) φ σε 2-CNF και $K < \# \text{όρων}$. Υπάρχει **ανάθεση** τιμών αλήθειας που **ικανοποιεί** $\geq K$ όρους;
- MAX 2-SAT \in **NP**. Θδο **3-SAT** \leq_p MAX 2-SAT.
 - Έστω $c_i = x \vee y \vee z, w_i$ μετ/τή, $(x), (y), (z), (w_i)$
και ομάδα C'_i 10 2-CNF όρων: $(\neg x \vee \neg y), (\neg y \vee \neg z), (\neg z \vee \neg x)$
 $(x \vee \neg w_i), (y \vee \neg w_i), (z \vee \neg w_i)$
 - Ανάθεση **ικανοποιεί** c_i : επιλέγουμε w_i , ικανοποιούνται 7 όροι C'_i .
 - Ανάθεση **δεν ικανοποιεί** c_i : ικανοποιούνται μόνο 6 όροι C'_i .
 - Έτσι από $\psi = c_1 \wedge \dots \wedge c_m$ σε 3-CNF, κατασκευάζουμε $\varphi_\psi = C'_1 \wedge \dots \wedge C'_m$ σε 2-CNF σε **πολυωνυμικό** χρόνο.
 - ψ **ικανοποιήσιμη** ανν υπάρχει ανάθεση τιμών αλήθειας που **ικανοποιεί** $\geq 7m$ όρους της φ_ψ .

MIS είναι NP-πλήρες

- **Max Independent Set (MIS)**: Γράφημα $G(V, E)$ και $k < |V|$. Έχει G ανεξάρτητο σύνολο με $\geq k$ κορυφές;
- $MIS \in \mathbf{NP}$. Θδο $3\text{-SAT} \leq_p MIS$.
 - Έστω $\psi = c_1 \wedge \dots \wedge c_m$ σε 3-CNF. Κατασκευάζουμε G_ψ .
 - Ένα «τρίγωνο» t_j για κάθε όρο $c_j = l_{j_1} \vee l_{j_2} \vee l_{j_3}$
 - Μια ακμή $(x_i, \neg x_i)$ για κάθε ζευγάρι συμπληρωματικών εμφανίσεων μεταβλητής x_i .

$$\begin{aligned}\psi &= (\neg x_1 \vee x_2 \vee \neg x_3) \\ &\wedge (x_1 \vee \neg x_2 \vee x_3) \\ &\wedge (x_1 \vee x_2 \vee x_3) \\ &\wedge (\neg x_1 \vee \neg x_2)\end{aligned}$$



MIS είναι NP-πλήρες

- 3-SAT \leq_p MIS (συνέχεια).
 - Έστω $\psi = c_1 \wedge \dots \wedge c_m$ σε 3-CNF. Κατασκευάζουμε G_ψ .
 - Ένα «τρίγωνο» t_j για κάθε όρο $c_j = l_{j_1} \vee l_{j_2} \vee l_{j_3}$
 - Μια ακμή $(x_i, \neg x_i)$ για κάθε ζευγάρι συμπληρωματικών εμφανίσεων μεταβλητής x_i .
 - Αν ψ ικανοποιήσιμη, από κάθε «τρίγωνο» t_j επιλέγουμε μια κορυφή που αντιστοιχεί σε (κάποιο) αληθές literal όρου c_j .
 - Όχι συμπληρωματικά literals \Rightarrow ανεξάρτητο σύν. m κορυφών.
 - Αν G_ψ έχει ανεξάρτητο σύν. m κορυφών, αυτό έχει μια κορυφή από κάθε «τρίγωνο» t_j και όχι «συμπληρωματικές» κορυφές.
 - Θέτουμε αντίστοιχα literals αληθή: ψ ικανοποιήσιμη.
 - ψ ικανοποιήσιμη αν G_ψ έχει ανεξάρτητο συν. $\geq m$ κορυφών.

MIS(4) είναι NP-πλήρες

- Πρόταση ψ στιγμιότυπο **3-SAT(3)**:
 - Κάθε μετ/τή εμφανίζεται ≤ 3 φορές.
 - Είτε ≤ 1 χωρίς άρνηση και ≤ 2 με άρνηση, είτε ≤ 2 χωρίς άρνηση και ≤ 1 με άρνηση.
- Στο γράφημα G_ψ , μέγιστος βαθμός κορυφής = 4.
- MIS παραμένει **NP-πλήρες** για γραφήματα με μέγιστο βαθμό 4!

Vertex Cover, Independent Set, και Clique

- Min Vertex Cover \equiv_p Max Independent Set \equiv_p Max Clique.
 - Vertex cover C σε γράφημα $G(V, E)$ ανν
independent set $V \setminus C$ σε γράφημα G ανν
clique $V \setminus C$ σε συμπληρωματικό γράφημα \bar{G} .
- Έστω μη κατευθυνόμενο γράφημα $G(V, E)$, $|V| = n$.
Τα παρακάτω είναι ισοδύναμα:
 - Το G έχει vertex cover $\leq k$.
 - Το G έχει independent set $\geq n - k$.
 - Το συμπληρωματικό \bar{G} έχει clique $\geq n - k$.
- Min Vertex Cover αποτελεί (απλή) ειδική περίπτωση **Ακέραιου Γραμμικού Προγρ. (ILP)**:
$$\begin{array}{ll} \min & \sum_{v \in V} x_v \\ \text{s.t.} & x_v + x_u \geq 1 \quad \forall e = \{v, u\} \in E \\ & x_v \in \{0, 1\} \quad \forall v \in V \end{array}$$

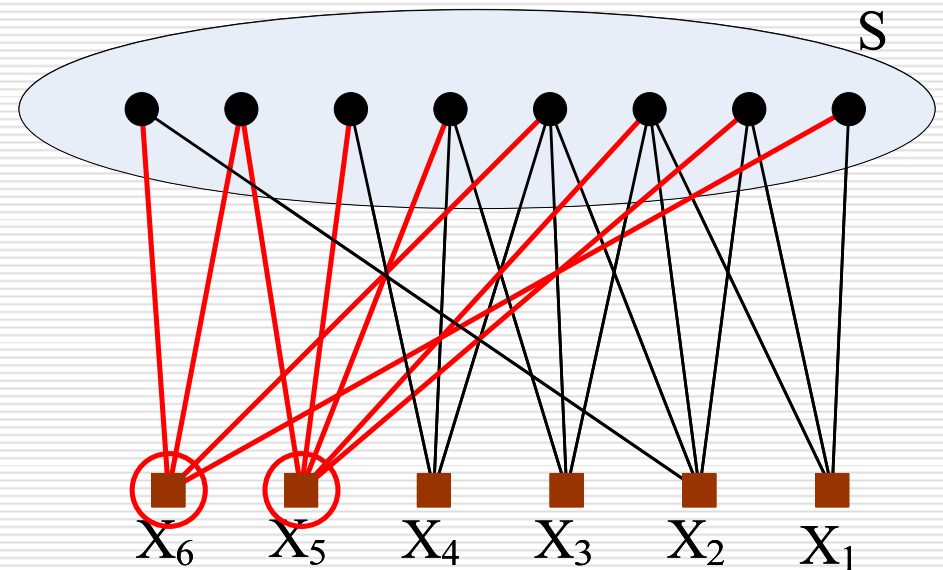
Set Cover

□ Κάλυμμα Συνόλου (Set Cover):

- Σύνολο S , υποσύνολα X_1, \dots, X_m του S , φυσικός k , $1 < k < m$.
- Υπάρχουν $\leq k$ υποσύνολα που η ένωσή τους είναι το S .
 - «Κάλυψη» του S με $\leq k$ υποσύνολα (από συγκεκριμένα).

□ Παράδειγμα:

- $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$
- $X_1 = \{1, 2, 3\}$
 $X_2 = \{2, 3, 4, 8\}$
 $X_3 = \{3, 4, 5\}$
 $X_4 = \{4, 5, 6\}$
 $X_5 = \{2, 3, 5, 6, 7\}$
 $X_6 = \{1, 4, 7, 8\}$
- Βέλτιστη λύση: X_5, X_6



Set Cover

- **Κάλυμμα Συνόλου (Set Cover):**
 - Σύνολο S , υποσύνολα X_1, \dots, X_m του S , φυσικός k , $1 < k < m$.
 - Υπάρχουν $\leq k$ υποσύνολα που η ένωσή τους είναι το S .
 - «Κάλυψη» του S με $\leq k$ υποσύνολα (από συγκεκριμένα).
- Set Cover αποτελεί **γενίκευση** του **Vertex Cover**:
 - Vertex Cover προκύπτει όταν κάθε στοιχείο $e \in S$ ανήκει σε (ακριβώς) δύο υποσύνολα X_i και X_j .
 - S : ακμές γραφήματος με m κορυφές / υποσύνολα.
 - Ακμή $e \in S$ συνδέει κορυφές / υποσύνολα X_i και X_j .

Subgraph Isomorphism

□ Subgraph Isomorphism:

- Γραφήματα $G_1(V_1, E_1)$ και $G_2(V_2, E_2)$, $|V_1| > |V_2|$.
- Υπάρχει υπογράφημα του G_1 ισομορφικό με το G_2 ;
 - Δηλ. είναι το G_2 υπογράφημα του G_1 ;

□ Subgraph Isomorphism αποτελεί γενίκευση MIS (Clique):

- MIS προκύπτει για G_2 ανεξάρτητο σύνολο k κορυφών.
- Clique προκύπτει για G_2 πλήρες γράφημα k κορυφών.

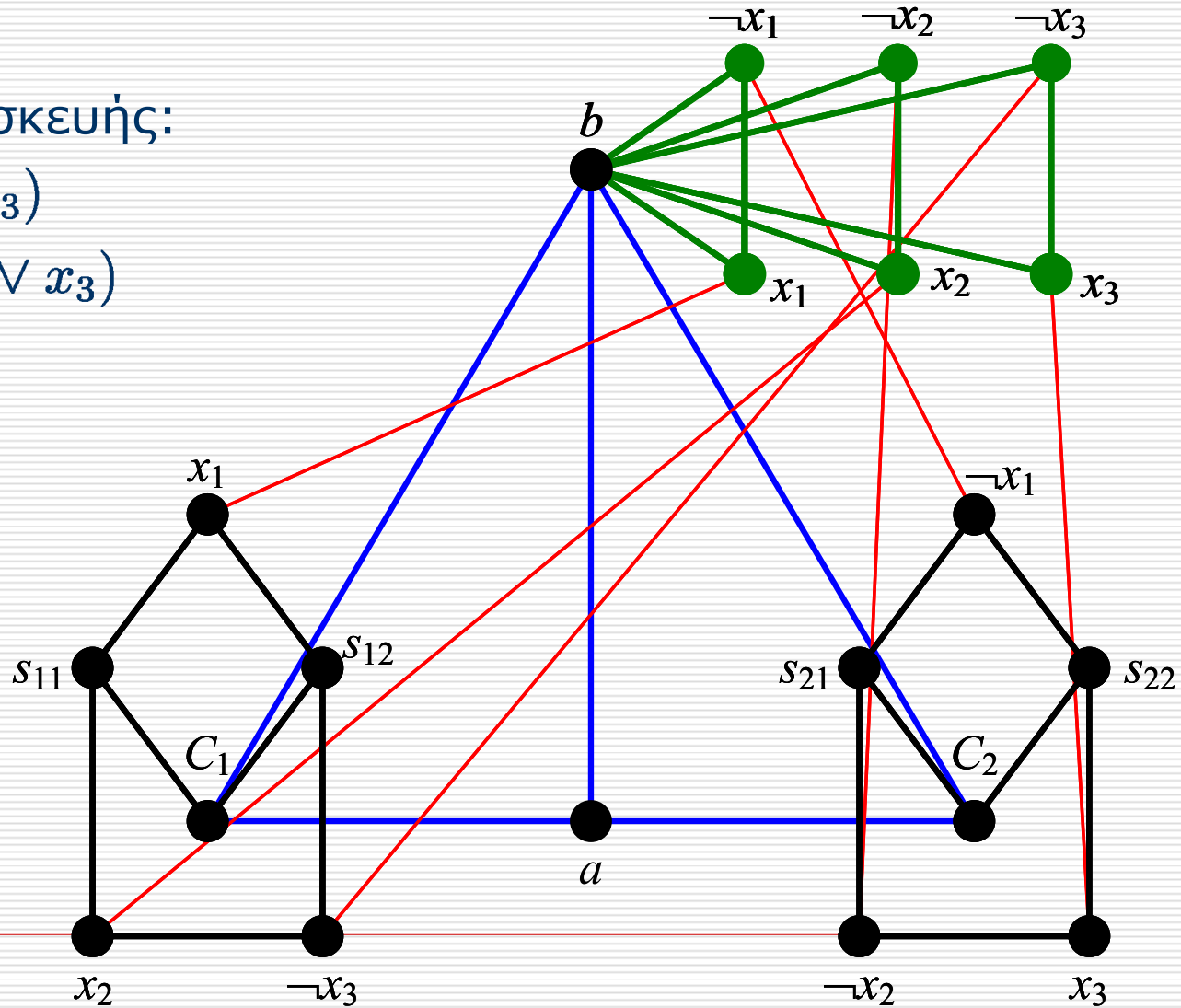
3-COL είναι NP-πλήρες

□ 3-SAT \leq_p 3-COL.

■ Παράδειγμα κατασκευής:

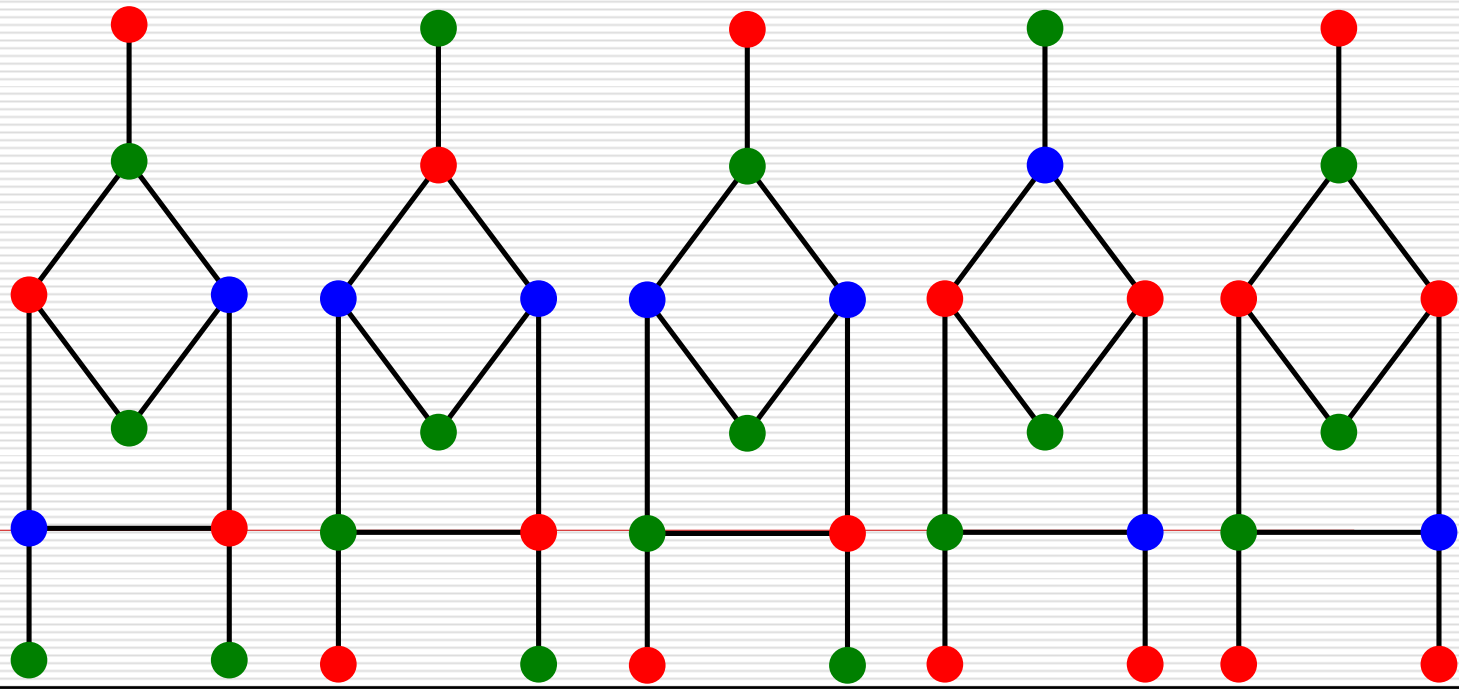
$$\psi = (x_1 \vee x_2 \vee \neg x_3)$$

$$\wedge (\neg x_1 \vee \neg x_2 \vee x_3)$$



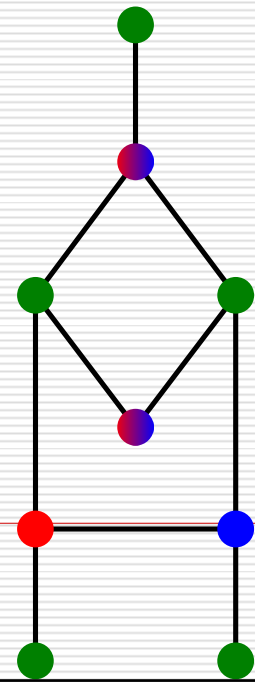
3-COL είναι NP-πλήρες

- Θδο ψ ικανοποιήσιμη ανν $\chi(G_\psi) = 3$.
 - Χβτγ, υποθέτουμε ότι $\chi_r(b) = 2$, $\chi_r(a) = 1$.
Έτσι $\chi(G_\psi) = 3$ ανν $\chi_r(C_j) = 0$ για κάθε gadget g_j (όρο c_j).
 - Αν ψ ικανοποιήσιμη, $\chi_r(x_i) = 1$ και $\chi_r(\neg x_i) = 0$ αν x_i αληθής, και $\chi_r(x_i) = 0$ και $\chi_r(\neg x_i) = 1$ αν x_i ψευδής (βλ. b-τρίγωνα).
 - Αν όρος c_j ικανοποιείται: χρωματίζουμε g_j ώστε $\chi_r(C_j) = 0$.



3-COL είναι NP-πλήρες

- Θδο ψ ικανοποιήσιμη ανν $\chi(G_\psi) = 3$.
 - Χβτγ, υποθέτουμε ότι $\chi_r(b) = \mathbf{2}$, $\chi_r(a) = \mathbf{1}$.
Έτσι $\chi(G_\psi) = 3$ ανν $\chi_r(C_j) = \mathbf{0}$ για κάθε gadget g_j (όρο c_j).
 - Αν $\chi_r(C_j) = \mathbf{0}$ για κάθε gadget g_j πρέπει τουλ. μία από 3 «εισόδους» g_j έχει χρώμα $\mathbf{1}$ (αντιστοιχεί σε αληθές literal).
 - Θέτουμε x_i αληθές αν $\chi_r(x_i) = \mathbf{1}$ και $\chi_r(\neg x_i) = \mathbf{0}$ και x_i ψευδές αν $\chi_r(x_i) = \mathbf{0}$ και $\chi_r(\neg x_i) = \mathbf{1}$.
 - Έτσι ψ ικανοποιείται, αφού υπάρχει τουλ. ένα αληθές literal σε κάθε όρο c_j .



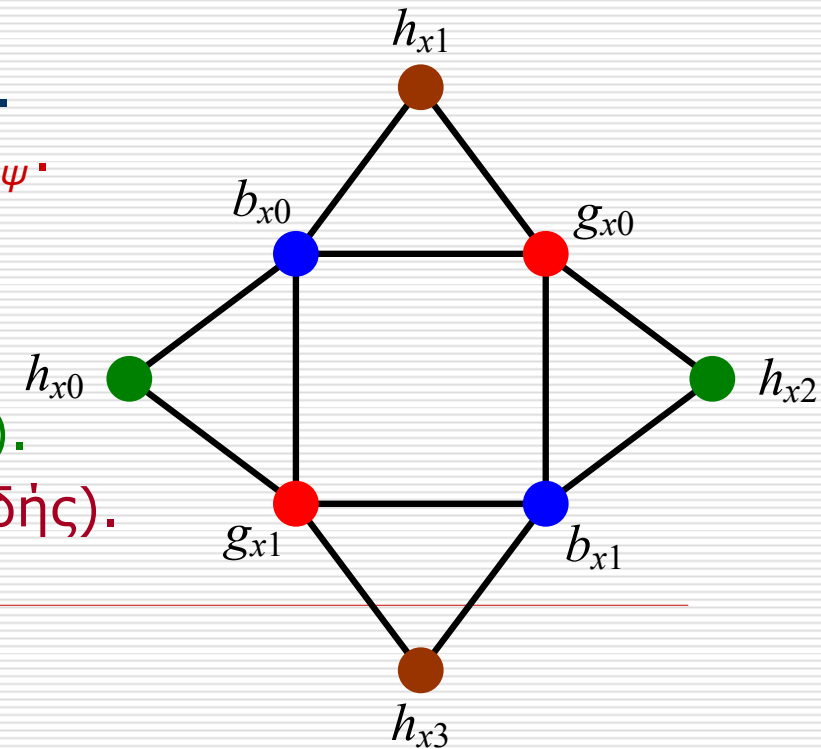
3DM είναι NP-πλήρες

□ Τρισδιάστατο Ταίριασμα (3-Dimensional Matching, **3DM**).

- Ξένα μεταξύ τους σύνολα B, G, H , $|B| = |G| = |H| = n$, και σύνολο τριάδων $M \subseteq B \times G \times H$.
- Υπάρχει $M' \subseteq M$, $|M'| = n$, όπου κάθε στοιχείο των B, G, H εμφανίζεται **μία φορά** (δηλ. M' καλύπτει όλα τα στοιχεία).

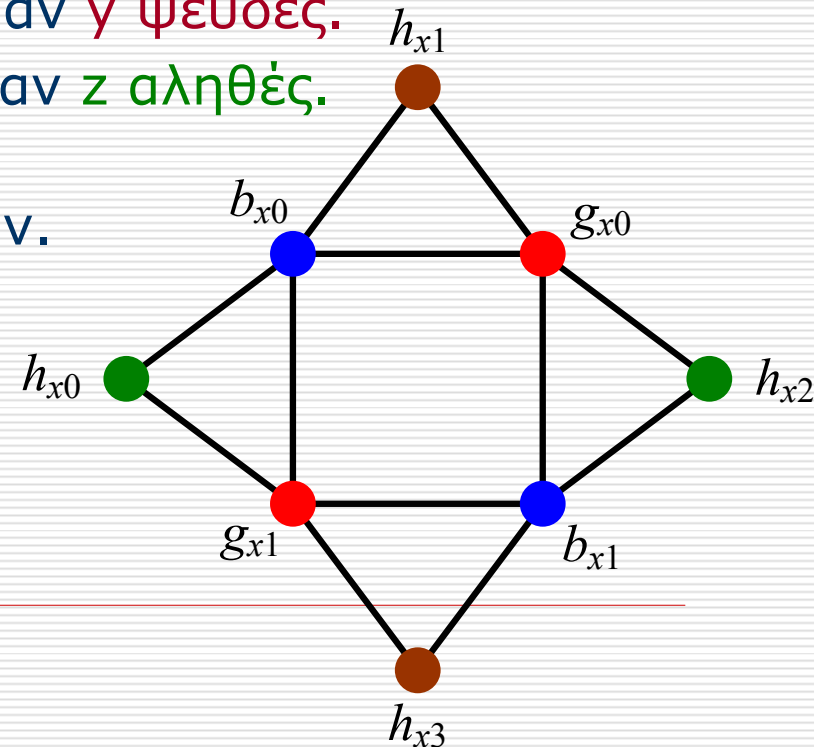
□ $3DM \in \mathbf{NP}$. Θδο $3\text{-SAT}(3) \leq_p 3DM$.

- Έστω $\psi = c_1 \wedge \dots \wedge c_m$ σε $3\text{-CNF}(3)$. Κατασκευάζουμε B_ψ, G_ψ, H_ψ , και M_ψ .
- Για κάθε μετ/τή x , 2 «αγόρια», 2 «κορίτσια», 4 «σπίτια», και 4 τριάδες.
- Τριάδες με h_{x0}, h_{x2} για x (x αληθής).
- Τριάδες με (h_{x1}, h_{x3}) για $\neg x$ (x ψευδής).



3DM είναι NP-πλήρες

- 3-SAT(3) \leq_p 3DM.
- $\psi = c_1 \wedge \dots \wedge c_m$ σε 3-CNF(3). Κατασκ. B_ψ , G_ψ , H_ψ , και M_ψ .
- Για κάθε όρο, π.χ. $c = x \vee \neg y \vee z$, «ζευγάρι» όρου c («αγόρι» b_c και «κορίτσι» g_c), και 3 τριάδες:
 - (b_c, g_c, h_{x1}) (ή με h_{x3}): επιλογή αν x αληθές.
 - (b_c, g_c, h_{y0}) (ή με h_{y2}): επιλογή αν y ψευδές.
 - (b_c, g_c, h_{z1}) (ή με h_{z3}): επιλογή αν z αληθές.
- Περιορισμός στον #εμφανίσεων:
«σπίτια» επαρκούν για τριάδες όρων.
- $4n$ «σπίτια» και $2n+m$ «ζευγάρια».
 - $2n - m$ «αζήτητα σπίτια»!
- $2n - m$ «εύκολα ζευγάρια» που συνδέονται με όλα τα «σπίτια».



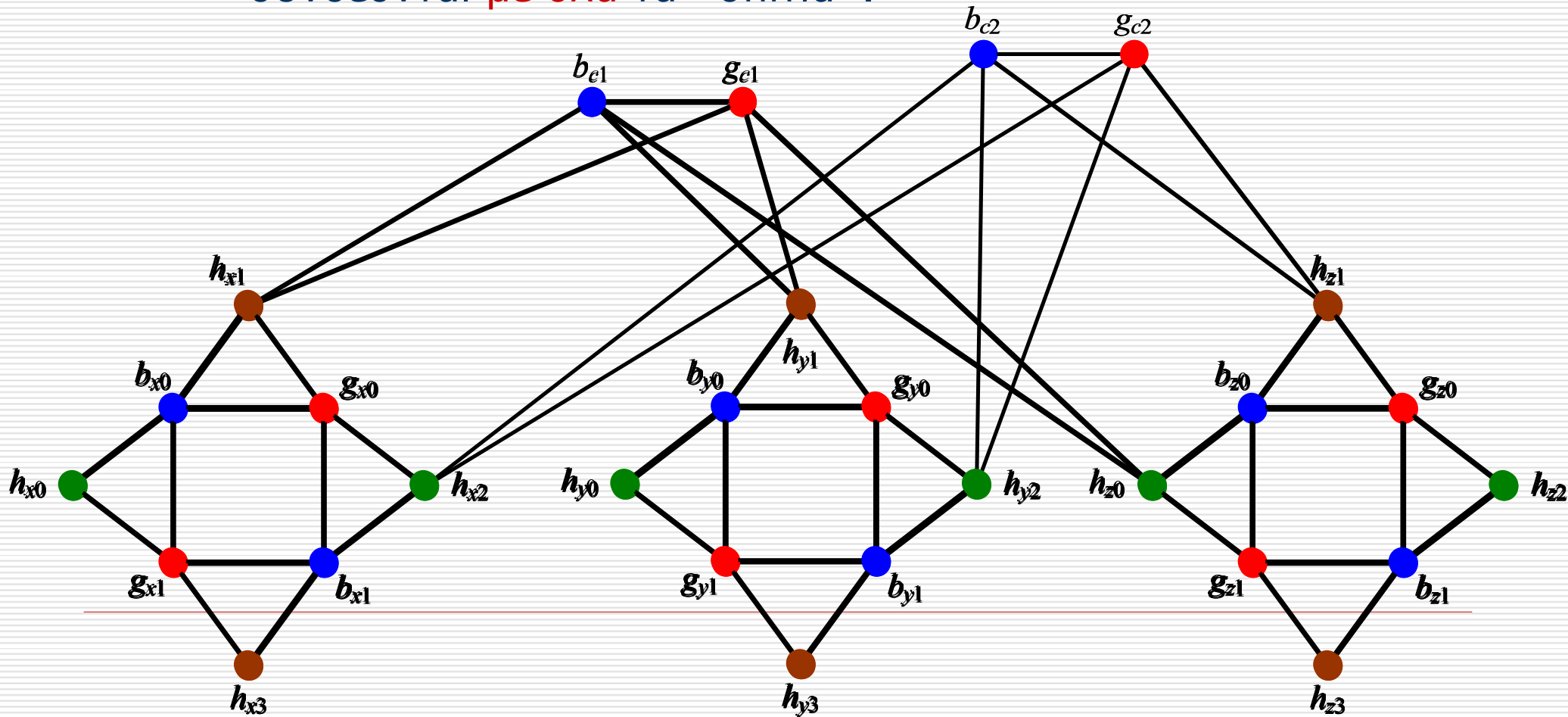
3DM είναι NP-πλήρες

□ 3-SAT(3) \leq_p 3DM.

■ Ακόμη 4 «εύκολα ζευγάρια» που συνδέονται με όλα τα «σπίτια».

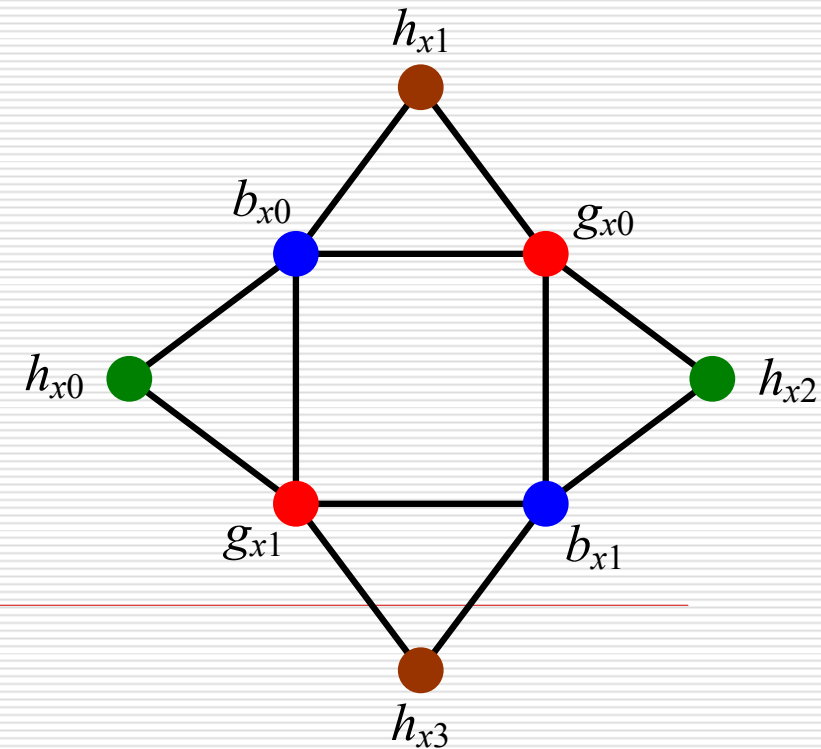
$$\psi = (x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z)$$

$x = F$
 $y = T$
 $z = T$



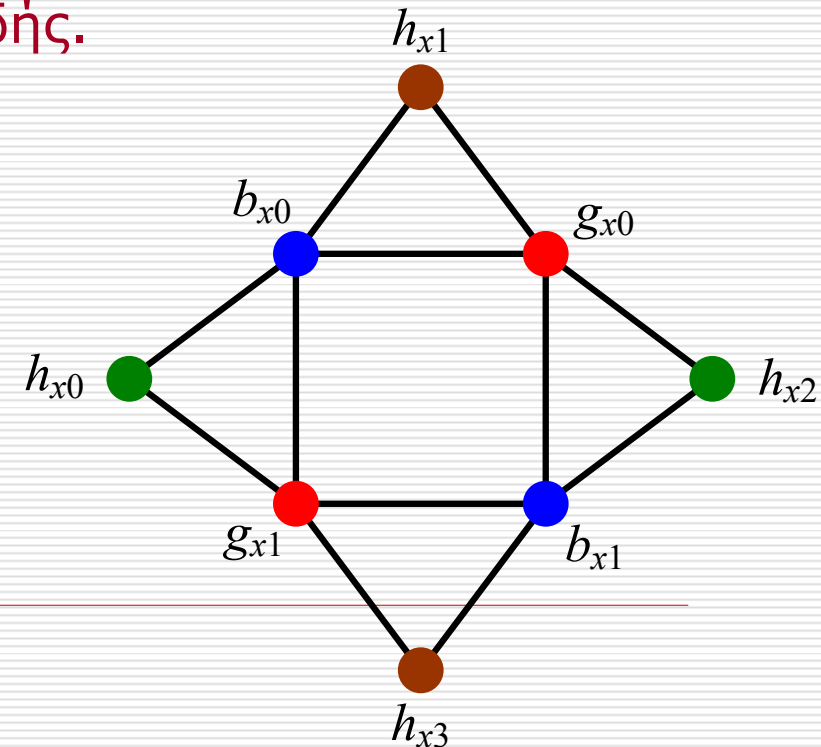
3DM είναι NP-πλήρες

- Θδο ψ ικανοποιήσιμη ανν υπάρχει 3DM $M' \subseteq M_\psi$, $|M'| = 4n$.
- Αν ψ ικανοποιήσιμη:
 - \forall αληθή μετ/τή x , επιλέγουμε 2 x -τριάδες.
 - \forall ψευδή μετ/τή x , επιλέγουμε 2 $\neg x$ -τριάδες ($2n$).
 - Τουλ. ένα αληθές literal σε κάθε όρο της ψ : τουλ. ένα «ελεύθερο σπίτι» για «ζευγάρι» κάθε όρου (m).
 - «Αζήτητα σπίτια» καλύπτονται από $2n - m$ «εύκολα ζευγάρι».



3DM είναι NP-πλήρες

- Θδο ψ ικανοποιήσιμη ανν υπάρχει 3DM $M' \subseteq M_\psi$, $|M'| = 4n$.
- Αν υπάρχει 3DM $M' \subseteq M_\psi$, $|M'| = 4n$:
 - Εστιάζουμε σε $2n+m$ «δύσκολα ζευγάρια».
 - Επιλέγονται $2n$ «ζευγάρια» μεταβλητών:
 - \forall μετ/τη x , είτε 2 x -τριάδες, οπότε x αληθής, είτε 2 $\neg x$ -τριάδες, οπότε x ψευδής.
 - Επιλέγονται m «ζευγάρια» όρων:
 - «Ελεύθερο σπίτι» για κάθε όρο.
 - Ανάθεση τιμών αλήθειας δημιουργεί τουλάχιστον ένα αληθές literal σε κάθε όρο.
- Bipartite Matching (2DM) $\in \mathbf{P}$.



Subset Sum και Knapsack

□ Subset Sum:

- Σύνολο φυσικών $A = \{w_1, \dots, w_n\}$ και $W, 0 < W < w(A)$.
- Υπάρχει $A' \subseteq A$ με $w(A') = \sum_{i \in A'} w_i = W$;

□ Knapsack αποτελεί γενίκευση Subset Sum.

- Subset sum προκύπτει όταν για κάθε αντικείμενο i , μέγεθος(i) = αξία(i) (θεωρούμε μέγεθος σακιδίου = W).

Subset Sum και Partition

□ Partition:

- Σύνολο φυσικών $A = \{w_1, \dots, w_n\}$ με άρτιο $w(A) = \sum_{i \in A} w_i$;
- Υπάρχει $A' \subseteq A$ με $w(A') = w(A \setminus A')$;

□ Subset Sum \leq_p Partition.

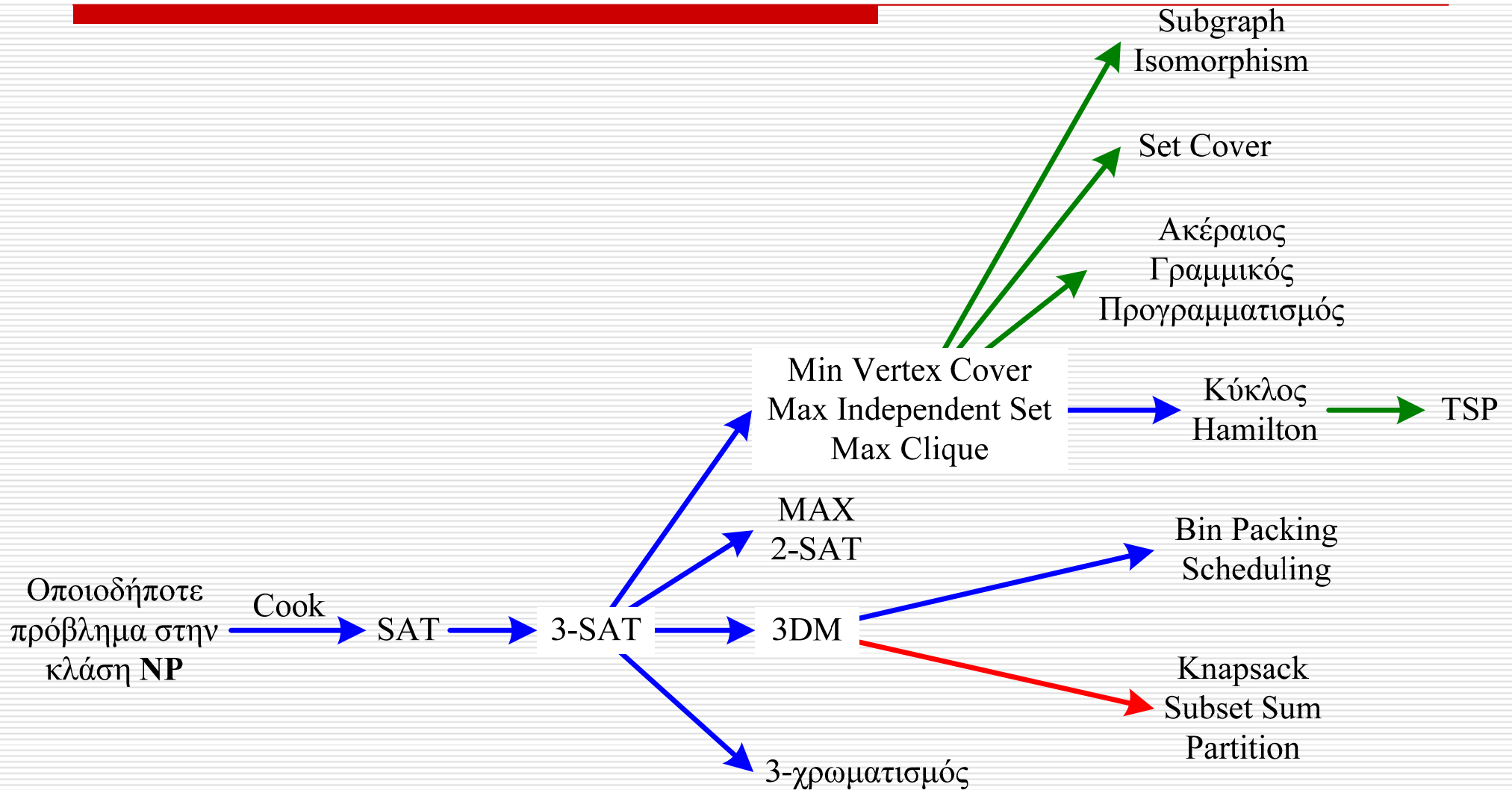
- Έστω σύνολο $A = \{w_1, \dots, w_n\}$ και $W, 0 < W < w(A)$.
- Χβτγ, θεωρούμε ότι $W \geq w(A)/2$.
- Σύνολο $B = \{w_1, \dots, w_n, 2W - w(A)\}$ με $w(B) = 2W$.
- Υπάρχει $A' \subseteq A$ με $w(A') = W$ ανν
υπάρχει $B' \subseteq B$ με $w(B') = w(B \setminus B') = W$.

□ Ένα από τα $B', B \setminus B'$ είναι υποσύνολο του A .

□ Όμως το Subset Sum αποτελεί γενίκευση Partition.

- Τελικά $\text{Subset Sum} \equiv_p \text{Partition}$.

Ακολουθία Αναγωγών



Subset Sum είναι NP-Πλήρες

- Subset Sum \in **NP**. Θδο $3DM \leq_p$ Subset Sum.
 - Έστω $B = \{b_1, \dots, b_n\}$, $G = \{g_1, \dots, g_n\}$, $H = \{h_1, \dots, h_n\}$, και $M \subseteq B \times G \times H$, $|M| = m$.
 - Τριάδα $t_i \in M \rightarrow$ δυαδική συμβ/ρά b_i μήκους $3n$ με 3 «άσσους».
 - 1^{ος} «άσσος» σε θέση 1 ως n δηλώνει το «αγόρι».
 - 2^{ος} «άσσος» σε θέση $n+1$ ως $2n$ δηλώνει το «κορίτσι».
 - 3^{ος} «άσσος» σε θέση $2n+1$ ως $3n$ δηλώνει το «σπίτι».
 - Π.χ. $n = 4$. (b_2, g_3, h_1) : 0001 0100 0010
 - Υπάρχει $3DM$ $M' \subseteq M$, $|M'| = n$, αν υπάρχει $B' = \{b_{i_1}, \dots, b_{i_n}\}$ που οι «άσσοι» των $b_{i_\ell} \in B'$ καλύπτουν όλες τις $3n$ θέσεις.

Subset Sum είναι NP-Πλήρες

□ $3DM \leq_p$ Subset Sum.

■ Υπάρχει $3DM$ $M' \subseteq M$, $|M'| = n$, αν υπάρχει $B' = \{b_{i_1}, \dots, b_{i_n}\}$ που οι «άσσοι» των $b_{i_\ell} \in B'$ καλύπτουν όλες τις $3n$ θέσεις.

■ ... ανν σύνολο $A = \{w_1, \dots, w_m\}$ με $w_i = \sum_{j=1}^{3n} b_i(j)2^{j-1}$ έχει υποσύνολο $A' \subseteq A$ με $w(A) = 2^{3n} - 1$ (;).

□ **Μπορεί και όχι(!)**: π.χ. $A = \{0011, 0101, 0111\}$

□ «Επιπλοκή» λόγω κρατούμενου δυαδικής πρόσθεσης.

□ **Λύση**: ερμηνεύουμε αριθμούς σε βάση $m+1$ ώστε πρόσθεση m «άσσων» να μην εμφανίζει κρατούμενο.

■ ... ανν σύνολο $A = \{w_1, \dots, w_m\}$ με $w_i = \sum_{j=1}^{3n} b_i(j)(m+1)^{j-1}$ έχει υποσύνολο $A' \subseteq A$ με $w(A) = ((m+1)^{3n} - 1)/m$.

Ακολουθία Αναγωγών

