Θεωρία Πολυπλοκότητας

Η *χρονική πολυπλοκότητα* ενός αλγορίθμου που επιλύει κάποιο πρόβλημα είναι μια αύξουσα συνάρτηση $T(n)$ όπου n είναι το μέγεθος της εισόδου.

$$T(n) = \max\{\#\text{ steps for input x: } |x| = n\}$$

- Το μέγεθος της εισόδου εξαρτάται από την αναπαράσταση
- δυαδικό/δεκαδικό σύσημα. ΟΧΙ ΕΝΑΔΙΚΟ.

Αποδοτικός αλγόριθμός (efficient)

Υπάρχει πολυώνυμο p τέτοιο ώστε:

$$\forall n \quad T(n) \leq p(n)$$

Δεν μας ενδιαφέρουν

- Το συγκεκριμένο υπολογιστικό μοντέλο
- Η κωδικοποίηση
- Ο βαθμός του πολυωνύμου.

Προβλήματα βελτιστοποίησης

- Ζητάμε λύση που βελτιστοποιεί μια αντικειμενική συνάρτηση
  - Σύνολο εφικτών λύσεων
  - Βέλτιστη λύση

Πρόβλημα πλανόδιου πωλητή (Travelling Salesman Problem)

Δίνονται: πόλεις $C = \{c_1, c_2, \ldots, c_n\}$
απόσταση $d(c_i, c_j) \in \mathcal{Z}^+ \forall (c_i, c_j) \in C^2$

Ζητείται: διαδρομή που περνά από κάθε πόλη, επιστρέφει στην αρχική, έχει ελάχιστο μήκος

Μετάθεση $< c_{\pi_1}, c_{\pi_2}, \ldots, c_{\pi_n} >$:

$\sum_{i=1}^{n-1} d(c_{\pi_i}, c_{\pi_{i+1}}) + d(c_{\pi_n}, c_{\pi_1})$ είναι ελάχιστο.

Προβλήματα απόφασης

- Επιδέχονται απαντήσεις της μορφής ΝΑΙ ή ΟΧΙ
- Εάν A το σύνολο των εισόδων x για τις οποίες η απάντηση είναι ΝΑΙ, το πρόβλημα ισοδυναμεί με το ερώτημα

  "$x \in A$?"

  Πρόβλημα βελτιστοποίησης $\longrightarrow$ Απόφασης

  "Για είσοδο x, n υπάρχει εφικτή λύση s για το x με $c(s) > n$"

Μέγιστη Κλίκα (Clique)

- Γράφημα $G(V, E)$
- Ποιά η μέγιστη κλίκα· $\longleftarrow$ *Βελτιστοποίηση*
- Γράφημα $G(V, E)$
- ακέραιος n
- Υπάρχει κλίκα μεγάθους $\geq n$ $\longleftarrow$ *Απόφασης*

- Το πρόβλημα απόφασης ΔΕΝ ΕΙΝΑΙ ΠΙΟ ΔΥΣΚΟΛΟ από το πρόβλημα βελτιστοποίησης
- Το πρόβλημα βελτιστοποίησης είναι ΤΟΥΛΑΧΙΣΤΟΝ ΤΟΣΟ ΔΥΣΚΟΛΟ ΟΣΟ και το πρόβλημα απόφασης

Οι κλάσεις P και NP

- P **(POLYNOMIAL):**

  Η κλάση προβλημάτων που επιλύονται σε πολυωνυμικό χρόνο από κάποιον ντετερμινιστικό αλγόριθμο (DTM: Deterministic Turing Machine)

- (NP **Non-deterministic POLYNOMIAL):**

  Η κλάση προβλημάτων που επιλύονται σε πολυωνυμικό χρόνο από κάποιο μη-ντετερμινιστικό αλγόριθμο (NDTM)

Θεωρούμε ότι ένας μη-ντετερμινστικός αλγόριθμος αποτελείται από 2 στάδια

- μαντεύει μια λύση s για το στιγμιότυπο I
- επαληθεύει ότι η s είναι πράγματι λύση

Εύρεση Στοιχείου (searching)

choose $a[i]$
verify: if $a[i] = x$ **then found** $\Theta(1)$

Ταξινόμηση Διανύσματος (sorting)

choose a permutation
verify: $a[i] < a[i+1]$ **for all** i $\Theta(n)$

SAT (SATisfiability)

- x_i προτασιακή μεταβλητή
- literals: $x_i, \bar{x}_i$
- φράσεις (clauses): διαζεύξεις από literals $lit_1 \vee lit_2 \vee \ldots \vee lit_m$
- *CNF (Conjuctive Normal Form)* συζεύξεις από φράσεις

$$cl_1 \wedge cl_2 \wedge \ldots \wedge cl_n$$

SAT-πρόβλημα

Είσοδος: μια λογική έκφραση σε CNF

Έξοδος: Υπάρχει ανάθεση τιμών που ικανοποιεί την έκφραση;

choose: **μια απονομή αληθείας**

verify: **έλεγξε εάν η απονομή ικανοποιεί την έκφραση**

$NP = \{L | \exists$ NDTM πρόγραμμα M το οποίο
σε πολυωνυμικό χρόνο αποδέχεται τη γλώσσα $L\}$

Σχέση μεταξύ P και NP

- $P \subseteq NP$
- $P = NP$;
- $NP \subseteq DEXPTIME$

Αναγωγή $(\leq, \propto)$

$A \leq_m^p B$: *A ανάγεται πολυωνυμικά κατά Karp* σε ένα πρόβλημα B

P_f: συναρτήσεις που υπολογίζονται σε πολυωνυμικό χρόνο

$A \leq_m^p B$: $\exists f \in P_f : \forall x (x \in A \iff f(x) \in B)$

Ιδιότητες

1. Ανακλαστική $A \leq_m^p A$
2. Μεταβατική $A \leq_m^p B \wedge B \leq_m^p C \Rightarrow A \leq_m^p C$
3. $A \leq_m^p B \wedge B \leq_m^p A \Rightarrow A \equiv_m^p B$
4. $A \leq_m^p B \wedge B \in P \Rightarrow A \in P$

Hardness-Completeness

- C: κλάση προβλημάτων
- $\forall B \in C : B \leq A$

} Το A ονομάζεται C-**δύσκολο** (C-**hard**) ως προς $\leq$

- $A \in C$
- $A : C - \text{hard}$

} Το A ονομάζεται C-**πλήρες** (C-**complete**)

Ένα πρόβλημα L είναι NP-**complete** ως προς $\leq_m^p$ αν:

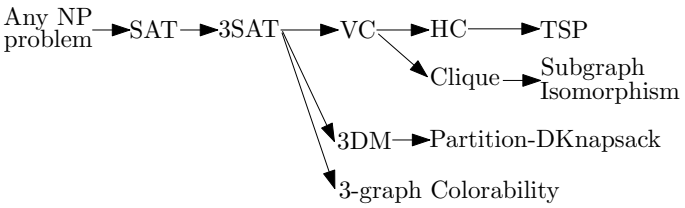
$$(L \in NP) \wedge (\forall L' \in NP : L' \leq_m^p L)$$

Αν ένα NP-complete πρόβλημα αποδειχθεί ότι ανήκει στο P, τότε όλα τα προβλήματα του NP θα ανήκουν στο P.

Λήμμα Αν: $L_1 \leq_m^p L_2$, $L_1 : NP$-complete, $L_2 \in NP$ } $L_2 \in NP$-complete

Θεώρημα (Cook): Το πρόβλημα SAT είναι NP-complete

Αναγωγές:



Για να δείξω ότι ένα πρόβλημα Π είναι NP-complete:

1. $\Pi \in NP$
2. Έστω $\Pi' \in NP - \text{complete}$
   Κατασκευάζω συνάρτηση f που μετασχηματίζει το Π' στο Π
3. Ο μετασχηματισμός f γίνεται σε πολυωνυμικό χρόνο
4. $x \in \Pi' \iff f(x) \in \Pi$

Προβλήματα Απόφασης

SAT(Satisfiability)

Δεδομένα: Λογική έκφραση σε CNF μορφή

Ερώτηση: Είναι η λογική έκφραση ικανοποιήσιμη;
Υπάρχει απονομή αληθείας στις μεταβλητές της έκφρασης τέτοια ώστε η έκφραση να αποτιμάται σε τιμή True;

3-SAT

Δεδομένα: Λογική έκφραση σε CNF, κάθε φράση έχει 3 literals

Ερώτηση: Είναι η λογική έκφραση ικανοποιήσιμη;

VC(Vertex Cover)

Δεδομένα: Γράφημα $G(V, E)$
Θετικός ακέραιος $k \leq |V|$

Ερώτηση: Υπάρχει ένα κάλυμμα κορυφών όλων των ακμών του E μεγέθους $\leq k$;
Δηλαδή: υπάρχει $V' \subseteq V : |V'| \leq k$ **και**
$\forall (u, v) \in E : u \in V'$ ή $v \in V'$;

3DM (3-dimensional Matching)

Δεδομένα: Σύνολο $M \subseteq W \times X \times Y$ όπου
$|W| = |X| = |Y| = q$ και W, X, Y ξένα μεταξύ τους

Ερώτηση: Περιέχει το M ένα ταίριασμα (matching);
Δηλαδή υπάρχει σύνολο $M' \subseteq M : |M'| = q$ έτσι ώστε
2 οποιαδήποτε στοιχεία του M' δεν έχουν καμία κοινή συντεταγμένη;

3-Colorability

Δεδομένα: Γράφημα $G(V, E)$

Ερώτηση: Μπορούμε να χρωματίσουμε τους κόμβους με 3 χρώματα έτσι ώστε
2 οποιοιδήποτε γειτονικοί κόμβοι να έχουν διαφορετικό χρώμα i;
δηλ. $\exists f : V \to \{1, 2, 3\} : \forall (u, v) \in E : f(u) \neq f(v)$;

HC(Hamilton Circuit)

Δεδομένα: Γράφημα $G(V, E)$

Ερώτηση: Υπάρχει στον G ένας κύκλος Hamilton;
δηλ. υπάρχει μια διάταξη των κόμβων του G
$< v_1, v_2, \ldots, v_n >$, $n = |V|$ τέτοια ώστε
$(v_i, v_{i+1}) \in E$, $1 \leq i \leq n - 1$ **και** $(v_n, v_1) \in E$;

TSP (Traveling Salesman Problem)

Δεδομένα: Γράφημα $G(V, E)$ με θετικά βάρη
Θετικός αριθμός B

Ερώτηση: Υπάρχει κλειστή διαδρομή που περνά από όλους τους κόμβους του G
$< v_{\pi(1)}, v_{\pi(2)}, \ldots, v_{\pi(n)} >$ έτσι ώστε
$\sum_{i=1}^{n-1} w(v_{\pi(i)}, v_{\pi(i+1)}) + w(v_{\pi(n)}, v_{\pi(1)}) \leq B$;

CLIQUE

Δεδομένα: Γράφημα $G(V, E)$
Θετικός ακέραιος $J \leq |V|$

Ερώτηση: Περιέχει ο G κλίκα μεγάθους $\geq J$;
δηλαδή, υπάρχει $V' \subseteq V : |V'| \geq J$ **και**
$\forall u, v \in V', (u, v) \in E$;

SUBGRAPH-ISOMORPHISM

Δεδομένα: Γραφήματα $G(V_1, E_1)$, $H(V_2, E_2)$

Ερώτηση: Έχει ο G υπογράφημα ισομορφικό με τον H;
δηλ. $\exists V \subseteq V_1, E \subseteq E_1 : |V| = |V_2|, |E| = |E_2|$ και συνάρτηση
$f : V_2 \to V$ "1-1"και "επί"ώστε να ισχύει
$(u, v) \in E_2 \Leftrightarrow (f(u), f(v)) \in E$;

Partition

Δεδομένα: Πεπερασμένο σύνολο A με βάρη $w(\alpha) \in \mathcal{Z}^+, \forall \alpha \in A$

Ερώτηση: Μπορεί το A να μοιραστεί σε 2 ισοβαρή υποσύνολα;
δηλ. $\exists A' \subseteq A : \sum_{\alpha \in A'} w(\alpha) = \sum_{\alpha \in (A' - A)} w(\alpha)$;

D-KNAPSACK (Discrete Knapsack)

Δεδομένα: • Πεπερασμένο σύνολο U
• συνάρτηση βάρους $w(u) \in \mathcal{Z}^+, \forall u \in U$
• συνάρτηση κόστους $p(u) \in \mathcal{Z}^+, \forall u \in U$
• θετικοί ακέραιοι W, P

Ερώτηση: Μπορούμε να διαλέξουμε μερικά αντικείμενα του U με συνολικό βάρος $\leq W$ και αξία $\geq P$;
δηλ. $\exists U' \subseteq U : \sum_{u \in U'} w(u) < W$ **και** $\sum_{u \in U'} p(u) \geq P$;

Θεώρημα : Το 3-SAT είναι NP-complete

Απόδειξη:

- 3-SAT $\in NP$ ✓
- SAT $\leq_m^p$ 3-SAT

SAT		**3-SAT**
$C = \{c_1, c_2, \ldots, c_m\}$ $U = \{z_1, z_2, \ldots, z_n\}$	$\Longleftrightarrow$	$C', V' : \lvert c\rvert = 3 \forall c \in C'$

i) $c \in C : |c| = 1$. Έστω $c = z$
Φτιάχνω 4 clauses
$(z + y_1 + y_2) \cdot (z + \bar{y}_1 + y_2) \cdot (z + y_1 + \bar{y}_2) \cdot (z + \bar{y}_1 + \bar{y}_2)$

ii) $c \in C : |c| = 2$. Έστω $c = z_1 + z_2$
Φτιάχνω 2 clauses $(z_1 + z_2 + y_1) \cdot (z_1 + z_2 + \bar{y}_1)$

iii) $c \in C : |c| = 3$. Παραμένουν ως έχουν

iv) $c \in C : |c| > 3$. Έστω $c = (z_1 + z_2 + \ldots + z_k)$
Φτιάχνω τα clauses
$(z_1 + z_2 + y_1) \cdot (\bar{y}_1 + z_3 + y_2) \cdot (\bar{y}_2 + z_4 + y_3) \cdot \ldots \cdot$
$\cdot (\bar{y}_{k-4} + z_{k-2} + y_{k-3}) \cdot (\bar{y}_{k-3} + z_{k-1} + z_k)$ □

Θεώρημα : Το 2-SAT $\in P$

Θεώρημα : To Vertex Cover $\in NP$-complete

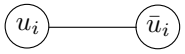
Απόδειξη:

- VC $\in NP$
- 3SAT $\leq_m^p$ VC

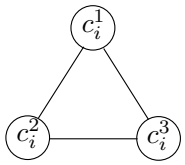
$$\left.\begin{array}{l} C = \{c_1, c_2, \ldots, c_m\} \\ U = \{u_1, u_2, \ldots, u_n\} \end{array}\right\} \Longrightarrow G = (V, E), k \in \mathcal{Z}^+, k \leq |V| :$$

$c_1 \cdot c_2 \cdot \ldots \cdot c_m$ είναι ικανοποιήσιμη $\Longleftrightarrow$ G έχει VC μεγέθους $\leq k$

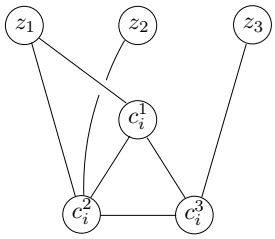
α) $\forall u_i \in U :$ στο G εισάγω



β) $\forall c_i \in C :$ εισάγω στο G



γ) $\forall c_i = (z_1 + z_2 + z_3)$: στο G εισάγω



δ) $k = n + 2m$

$G :$ $|V| = 2m + 3n$

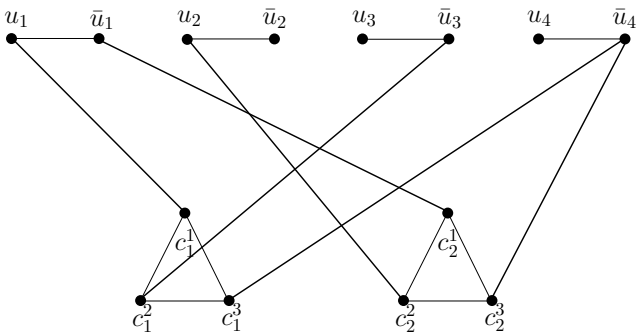
$|E| = m + 6n$

Παράδειγμα:

$\Phi : (u_1 + \bar{u}_3 + \bar{u}_4)(\bar{u}_1 + u_2 + \bar{u}_4)$

$\Downarrow$

G :



$k = n + 2m = 4 + 2 \cdot 2 = 8$

Θεώρημα : Το πρόβλημα CLIQUE είναι NP-complete

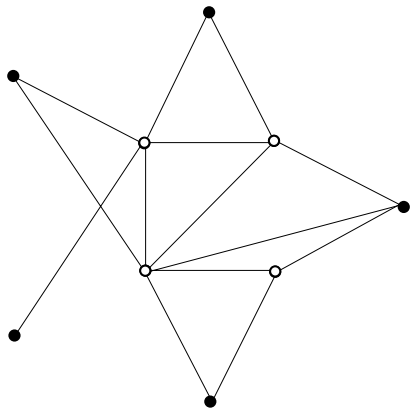
- CLIQUE $\in NP$
- VC $\leq_m^p$ Clique

$$\left\{\begin{array}{c}\textbf{VC}\\ G=(V,E)\\ k\in\mathcal{Z}^+\\ k\leq|V|\end{array}\right\} \qquad \left\{\begin{array}{c}\textbf{Clique}\\ G'=(V',E')\\ J\in\mathcal{Z}^+\\ J\leq|V'|\end{array}\right\}$$

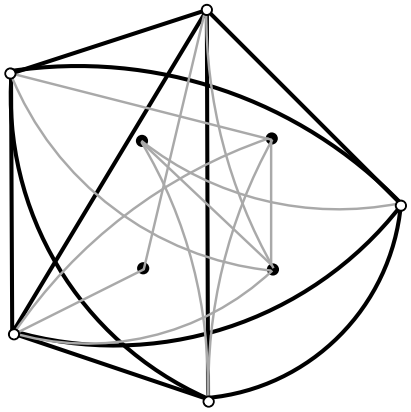
G έχει VC μεγέθους $\leq k$ $\iff$ G' περιέχει Clique μεγέθους $\geq J$

- $G' = \bar{G}$ $\qquad V' = V,\ E' = \{(u,v) : u, v \in V$ **και** $(u,v) \notin E\}$
  $J = |V| - k$

Παράδειγμα



$k = 4$



$J = 9 - 4 = 5$

Θεώρημα : Το Traveling Salesman Problem είναι NP-complete

- TSP $\in NP$
- Hamilton Circuit$\leq_m^p$TSP

HC		TSP
$\left\{ \; G = (V, E) \; \right\}$		$\left\{ \begin{array}{l} G' = (V', E'), \text{ πλήρης, με βάρη} \\ B \in \mathcal{Z}^+ \end{array} \right\}$
G έχει κύκλο Hamilton	$\Longleftrightarrow$	G' έχει tour με βάρος $\leq B$

$G' = (V, E')$: $\quad E' = \{(u, v) | u, v \in V\}$

$$w(u, v) = \left\{ \begin{array}{ll} 1 & (u, v) \in E \\ +\infty & (u, v) \notin E \end{array} \right\}$$

$B = |V|$

ΨΕΥΔΟΠΟΛΥΩΝΥΜΙΚΗ ΛΥΣΗ ΤΟΥ PARTITION

PARTITION

Δεδομένα: $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$
size $s(\alpha) \in \mathcal{Z}^+, \forall \alpha \in A$

Ερώτηση: Υπάρχει $A' \subset A$:
$A' \subseteq A : \sum_{\alpha \in A'} s(\alpha) = \sum_{\alpha \in (A' - A)} s(\alpha)$·

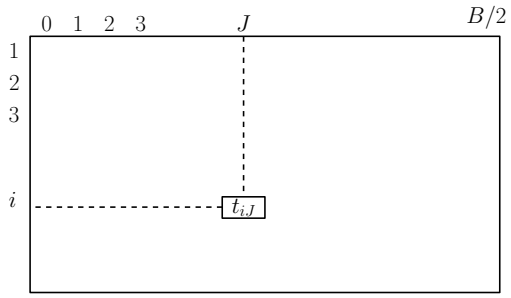
Παράδειγμα

$A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$

$s(\alpha_1) = 1$
$s(\alpha_2) = 9$
$s(\alpha_3) = 5$
$s(\alpha_4) = 3$
$s(\alpha_5) = 8$

Έστω $A' = \{\alpha_3, \alpha_5\}$
$\Rightarrow \sum_{\alpha \in A'} s(\alpha) = s(\alpha_3) + s(\alpha_5) = 5 + 8 = 13$
$\sum_{\alpha \in (A' - A)} s(\alpha) = s(\alpha_1) + s(\alpha_2) + s(\alpha_4) = 1 + 9 + 3 = 13$

- Έστω $B = \sum_{\alpha \in A} s(\alpha)$
- Εάν το B είναι περιττό $\Rightarrow \nexists A'$ που ικανοποιεί το πρόβλημα
- Για $1 \leq i \leq n$, $0 \leq J \leq \frac{B}{2}$ ορίζω την πρόταση:
  "Υπάρχει υποσύνολο του $\{\alpha_1, \alpha_2, \ldots \alpha_i\}$ με
  άθροισμα μεγεθών των στοιχείων του ίσο με J"
  $t(i, J)$ η boolean τιμή της πρότασης
- Οι τιμές $t(i, J)$ μπορεί να διαταχθούν
  σε δισδιάστατο πίνακα διαστάσεων $n \times (\frac{B}{2} + 1)$



(στο παράδειγμα, $n = 5$, $B = 13$)

Ο πίνακας συμπληρώνεται ως εξής:

$$\text{Γραμμή-}1 : t(1, J) = T \iff J = 0 \text{ or } J = s(\alpha_1)$$

$$\text{Γραμμή-}i : t(i, J) = T \iff t(i-1, J) = T \textbf{ or } (s(\alpha_i) < J \text{ and } t(i-1, J - s(\alpha_i)) = T)$$

Παράδειγμα:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	T	T												
2	T	T								T	T			
3	T	T				T	T			T	T			
4	T	T		T	T	T	T		T	T	T		T	T
5	T	T		T	T	T	T		T	T	T	T	T	T

$s(\alpha_1) = 1$ $s(\alpha_2) = 9$ $s(\alpha_3) = 5$ $s(\alpha_4) = 3$ $s(\alpha_5) = 8$

- Πολυπλοκότητα $O(nB)$

Αποδείξαμε ότι $P = NP$;;

ΟΧΙ

- Κάθε ακέραιος $s(\alpha_i)$ αναπαρίσταται με $O(\log s(\alpha_i))$ bits

  $\Rightarrow$ Συνολικό μέγεθος εισόδου:

$$\text{length}(I) = \sum_{i=1}^{n} \log s(\alpha_i) \leq \sum_{i=1}^{n} \log B = O(n \log B)$$

  ** nB δεν φράσεται από πολυωνυμική συνάρτηση του $n \log B$