Υπολογοστική Πολυπλοκότητα

Το Θεώρημα των Cook-Levin

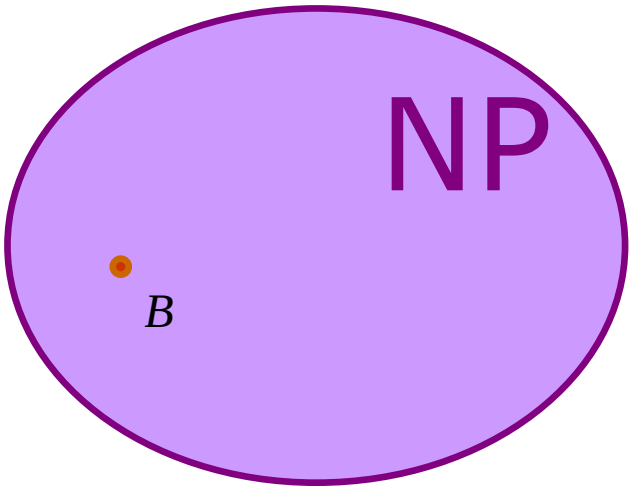
Cook–Levin (1971-1973)

Θεώρημα: Υπάρχει γλώσσα $S \in NP$ έτσι ώστε $S \in P$ αν και μόνο αν $P = NP$.

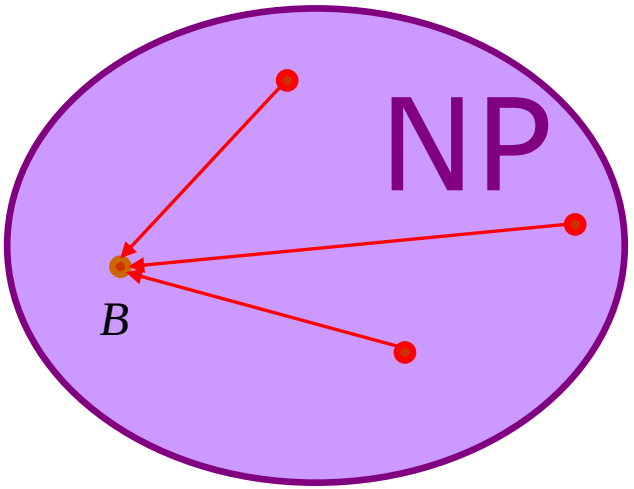
- Αυτό το θεώρημα καθορίζει την κλάση των *NP*-πλήρων γλωσσών.
- Αυτές οι γλώσσες, όπως και ο Frodo Baggins, «κουβαλάνε στην πλάτη τους» το βάρος όλης της κλάσης *NP*.

NP-Πληρότητα

Ένα πρόβλημα B είναι NP-πλήρες αν:

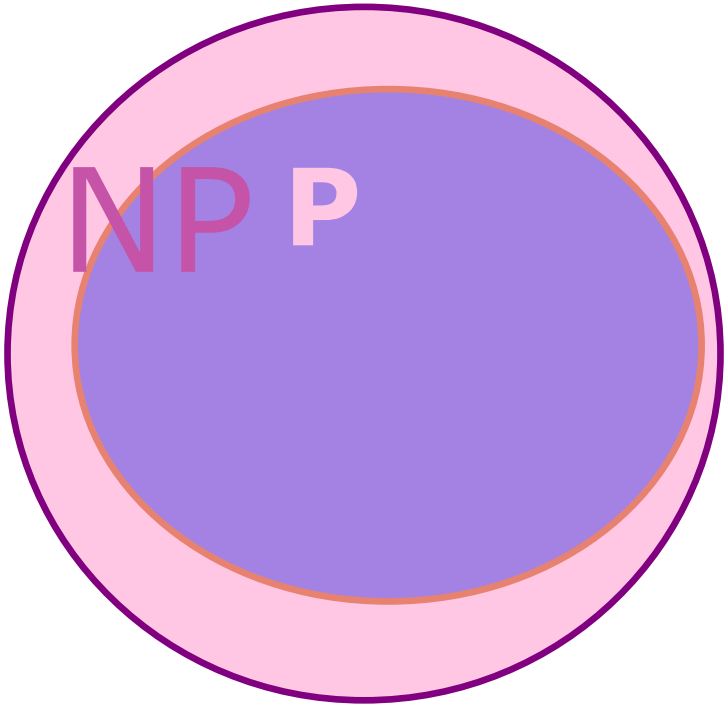


1. $B \in \mathbf{NP}$

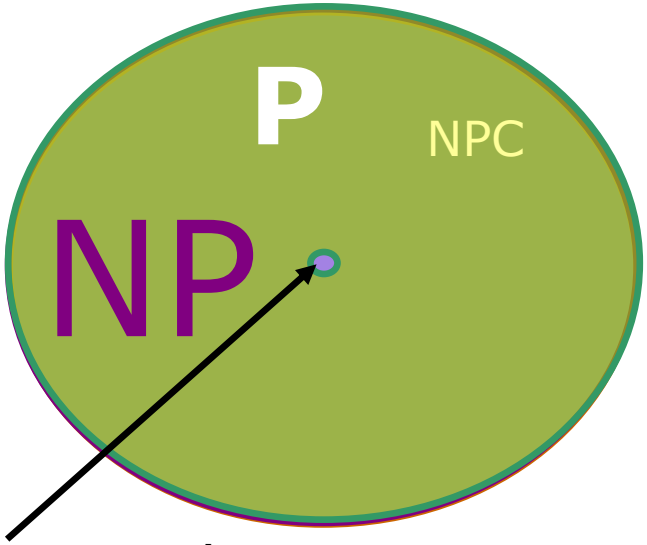


2. Υπάρχει πολυωνυμικού χρόνου αναγωγή από **κάθε** πρόβλημα $A \in \mathbf{NP}$ στο B.

NP-Πληρότητα



Περίπτωση 1: $\mathbf{P} \subset \mathbf{NP}$

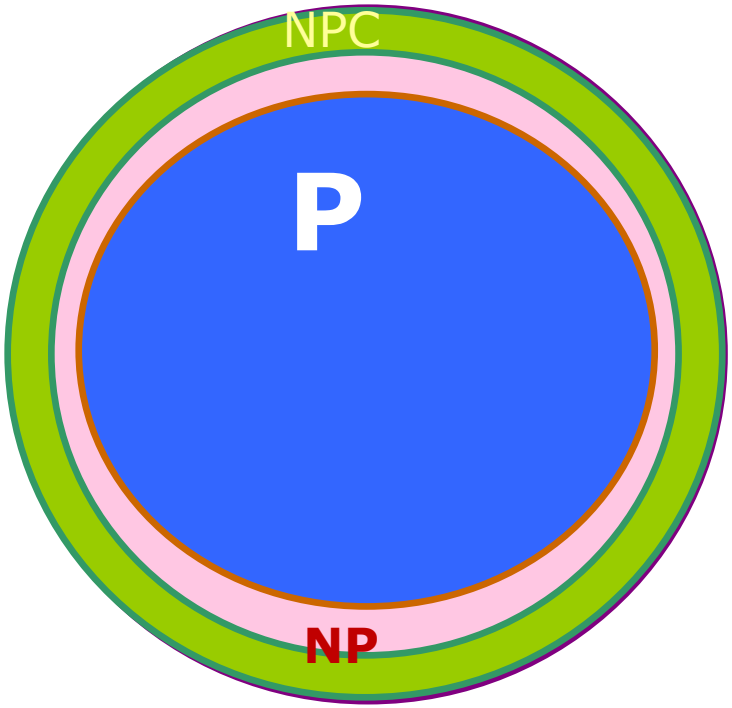


Τετριμμένα Προβλήματα
$A = \{\}; A = \Sigma^*$

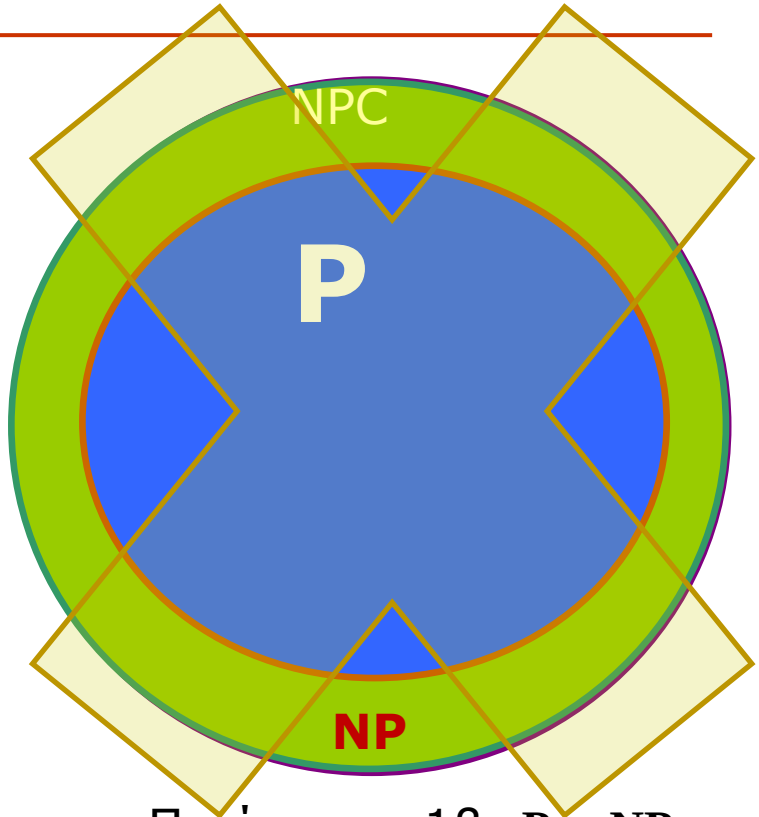
Περίπτωση 2: $\mathbf{P} = \mathbf{NP}$

$= \mathbf{NP}$-Πλήρη $\cup$ Τετριμμένα

NP-Πληρότητα



Περίπτωση 1α: $\mathbf{P} \subset \mathbf{NP}$, $\mathbf{NPC} \cup \mathbf{P} \subset \mathbf{NP}$

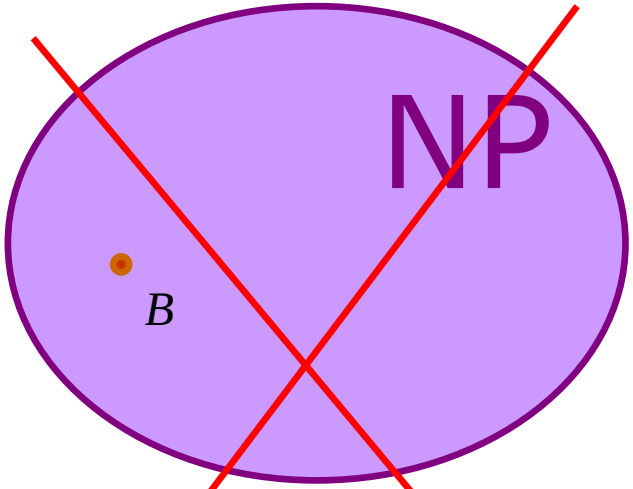


Περίπτωση 1β: $\mathbf{P} \subset \mathbf{NP}$, $\mathbf{NPC} \cup \mathbf{P} = \mathbf{NP}$

Θεώρημα Ladner

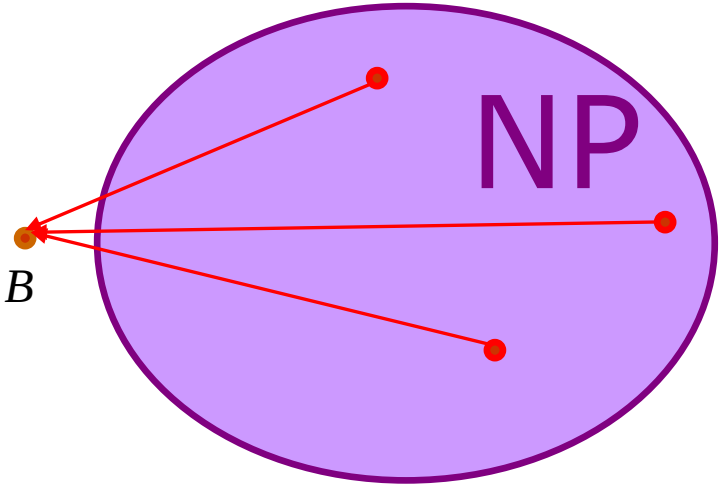
NP-~~Πλήρης~~ Δυσχερής (Hard)

Μία γλώσσα B είναι στην NPC αν:



1. $B \in \mathbf{NP}$

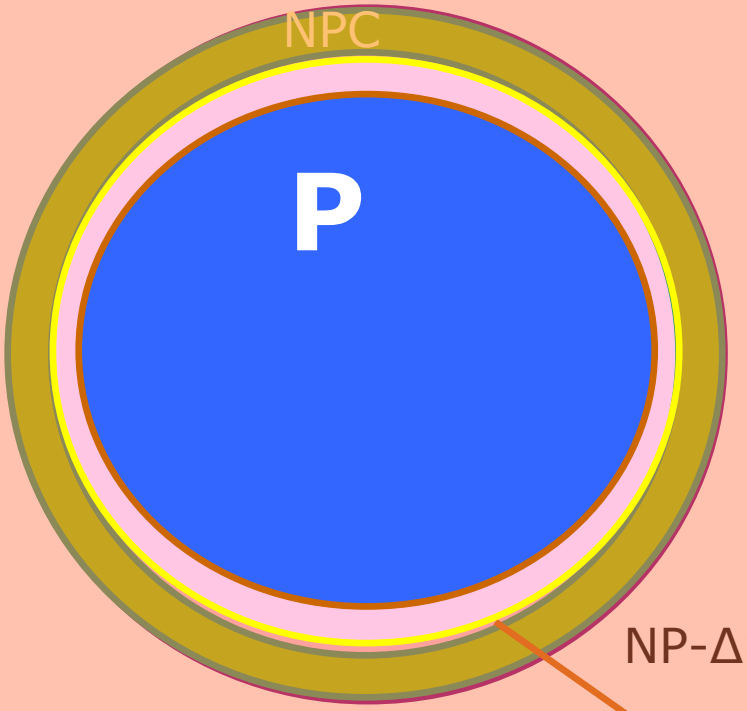
Όχι *απαραίτητο* για τα NP-δυσχερή



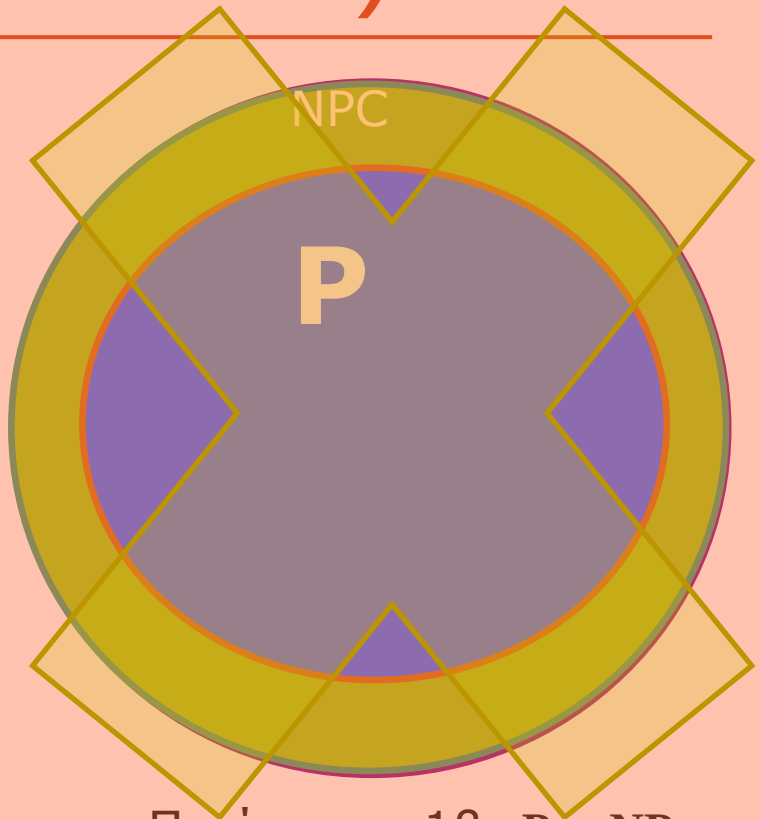
2. Υπάρχει πολυωνυμικού χρόνου αναγωγή από **κάθε** πρόβλημα $A \in \mathbf{NP}$ στο B.

Πώς μοιάζει η κλάση των NP-δυσχερών προβλημάτων;

NP-Δυσχερής (αν $\mathbf{P \subset NP}$)

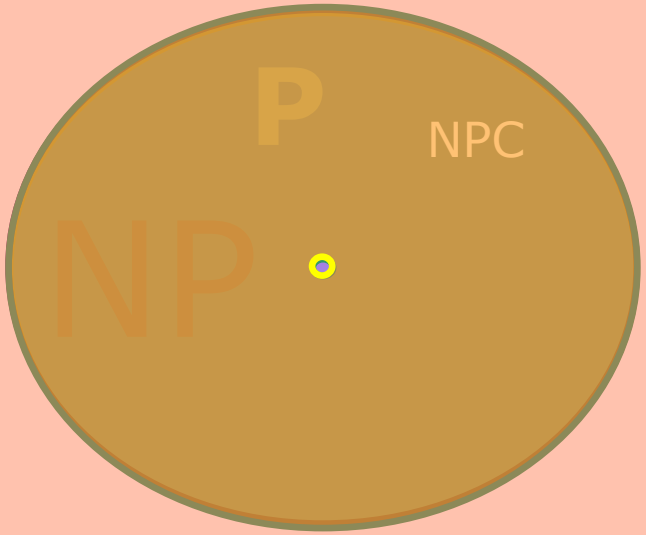


Περίπτωση 1α: $\mathbf{P \subset NP}$, $\mathbf{NPC \cup P \subset NP}$



Περίπτωση 1β: $\mathbf{P \subset NP}$, $\mathbf{NPC \cup P = NP}$

NP-Δυσχερής (αν **P = NP**)



Περίπτωση 2: **P** = **NP**

≈ **NP**-Πλήρες

NP-Δυσχερή = Όλα τα προβλήματα − {A = {}; A = Σ*}

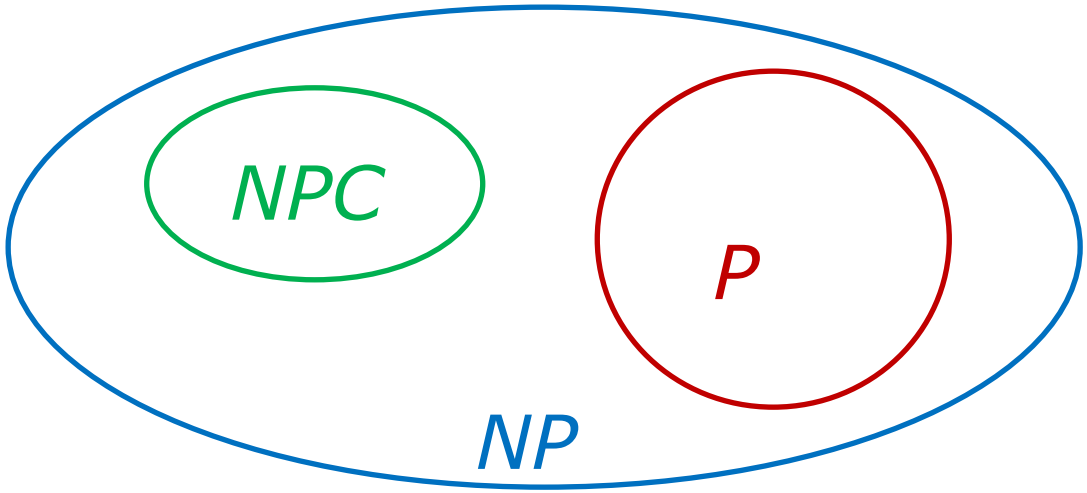
NP-Δυσχερής

- Αν P = NP:
  - Για να δείξετε ότι ένα πρόβλημα είναι NP-δυσχερές: δείξτε ότι για κάποια είσοδο δίνει ΝΑΙ και για κάποια ΟΧΙ
- Αν $P \subset NP$:
  - Για να δείξετε ότι ένα πρόβλημα είναι NP-δυσχερές: δείξτε ότι υπάρχει πολυωνυμική αναγωγή από κάποιο NP-πλήρες πρόβλημα σε αυτό
  - Αυτό σημαίνει ότι το πρόβλημα μάλλον δεν επιδέχεται πολυωνυμικής λύσης

NP Πληρότητα

Η κλάση των NP-πλήρων προβλημάτων είναι:

- «δυσκολότερες» γλώσσες στην *NP*
- «λιγότερο πιθανό» να είναι στην *P*
- Αν κάποιο NP-πλήρες $A \in P$, τότε $NP=P$.



Θεώρημα Αναγωγής

Αν το B είναι NP-πλήρες, $C \in NP$, και $B \leq_P C$, τότε και το C είναι NP-πλήρες.

Γνωρίζουμε ότι $C \in NP$ – θα πρέπει να δείξουμε ότι κάθε πρόβλημα A στο NP είναι πολυωνυμικά αναγώγιμο στο C.

Αφού το B είναι NP-πλήρες, κάθε γλώσσα στην NP είναι πολυωνυμικά αναγώγιμη στη B. Επίσης η B είναι πολυωνυμικά αναγώγιμη στη C.

Άρα η A είναι πολυωνυμικά αναγώγιμη στη C.

Στρατηγική

Από την στιγμή που θα έχουμε ένα «αποδεδειγμένο» NP-πλήρες πρόβλημα, μπορούμε να παράγουμε επιπλέον μέσω πολυωνυμικών αναγωγών.

Το να φτιάξουμε όμως το πρώτο χρειάζεται αρκετή δουλειά. Αυτή τη δουλειά την έκαναν οι Steve Cook (τότε στο Berkeley, τώρα στο Τορόντο) και Leonid Levin (τότε στη Μόσχα, τώρα στην Βοστόνη) στις αρχές της δεκαετίας του 70.

ΘΕΌΡΗΜΑ COOK-LEVIN

Το Πρόβλημα της Αληθευσιμότητας

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

Ασχολούμαστε με συγκεκριμένη μορφή:

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

Αληθευσιμότητα

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

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

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

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

Θεώρημα Cook-Levin

Το SAT είναι NP-πλήρες.

Απόδειξη:

- Εύκολο να δείξετε ότι $SAT \in NP$
- Πρέπει να δείξουμε ότι κάθε NP πρόβλημα ανάγεται στο SAT σε πολυωνυμικό χρόνο.

Ιδέα: Έστω $L \in NP$, και M η NTM που την επιλύει.

Σε είσοδο w μήκους n, η M τρέχει σε χρόνο $t(n) = n^c$.

Ορίζουμε το μητρώο της μηχανής ως έναν πίνακα $n^c \times n^c$ που περιγράφει τον υπολογισμό της M σε είσοδο w.

SAT και $_3$SAT

Θα δείξουμε μία πολυωνυμική αναγωγή που αντιστοιχεί λογικούς τύπους μορφής CNF σε λογικούς τύπους μορφής $_3$CNF.

Τι γίνεται αν έχουμε μία φράση με 1–2 λεξιγράμματα;

Μία φράση με x λεξιγράμματα αντιστοιχείται σε x-2 φράσεις με τα αρχικά λεξιγράμματα καθώς και με x-3 καινούργια.

Παράδειγμα: $(x_1 \vee x_2 \vee x_3 \vee x_4 \vee x_8)$

$\Rightarrow (x_1 \vee x_2 \vee y_1) \wedge (\neg y_1 \vee x_3 \vee y_2) \wedge (\neg y_2 \vee x_4 \vee x_8)$

SAT $\leq_P$ 3SAT

Η φ έχει αληθοποιός τιμοδοσία αν και μόνο αν η φ_3 έχει.

Απόδειξη:

$\Leftarrow$ Μία τιμοδοσία που ικανοποιεί την φ_3 δεν μπορεί να στηρίζεται μόνο σε νέα λεξιγράμματα – τουλάχιστον ένα αρχικό λεξίγραμμα σε κάθε φράση πρέπει να ικανοποιείται.

$\Rightarrow$ Μία τιμοδοσία που ικανοποιεί την φ κάνει τουλάχιστον ένα λεξίγραμμα αληθές για κάθε φράση. Στην αντίστοιχη φράση φ_3 με αυτό το λεξίγραμμα οι νέες μεταβλητές μπορούν να πάρουν οποιαδήποτε τιμή. Αυτό μας επιτρέπει μία διάδοση κατάλληλων τιμών στις νέες μεταβλητές έτσι ώστε όλες οι αντίστοιχες φράσεις να ικανοποιούνται.

Η αναγωγή είναι πολυωνυμική και άρα SAT $\leq_P$ 3SAT.