NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

BSc THESIS

Consequences of Polynomial Hierarchy in Parameterized Complexity: Tight Lower Bounds

Vasileios K. Vasilakis

Supervisor: **Archontia Giannopoulou,** Assistant Professor

ATHENS

OCTOBER 2022

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Συνέπειες της Πολυωνυμικής Ιεραρχίας στην Παραμετρική Πολυπλοκότητα: Σφιχτά Κάτω Φράγματα

Βασίλειος Κ. Βασιλάκης

Επιβλέπων: **Αρχοντία Γιαννοπούλου,** Επίκουρη Καθηγήτρια

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2022

BSc THESIS

Consequences of Polynomial Hierarchy in Parameterized Complexity: Tight Lower Bounds

Vasileios K. Vasilakis

S.N.: 1115201800018

SUPERVISOR: **Archontia Giannopoulou,** Assistant Professor

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Συνέπειες της Πολυωνυμικής Ιεραρχίας στην Παραμετρική Πολυπλοκότητα: Σφιχτά Κάτω Φράγματα

Βασίλειος Κ. Βασιλάκης

Α.Μ.: 1115201800018

ΕΠΙΒΛΕΠΩΝ: **Αρχοντία Γιαννοπούλου,** Επίκουρη Καθηγήτρια

ABSTRACT

An abstract 2-person communication model is presented and defined, where the 2 participants use a predetermined communication protocol between them, in order to decide a predetermined language. With each protocol, a cost is defined and quantified, and the goal is to minimize the cost across all protocols. In this direction, trivial protocols are presented for the NP-Complete problems of d-Sat and d-Vertex-Cover. These trivial protocols, assuming the polynomial hierarchy does not collapse, are proven to be cost-optimal. This fact has interesting consequences regarding areas of Parameterized Complexity for these problems, and in particular the areas of sparsification, kernelization and lossy compression. These consequences are presented as corollaries of the main results.

SUBJECT AREA: Computational Complexity

KEYWORDS: Computation by Abstract Devices, Circuit Complexity, Polynomial Reductions, Polynomial Hierarchy, Communication Protocol

ΠΕΡΙΛΗΨΗ

Παρουσιάζεται και ορίζεται ένα αφηρημένο μοντέλο υπολογισμού που συνίσταται στην επικοινωνία μεταξύ δύο παιχτών, βασιζόμενοι σε κάποιο προκαθορισμένο πρωτόκολλο επικοινωνίας, με σκοπό την αναγνώριση μιας γλώσσας. Με κάθε πρωτόκολλο, ορίζεται και ποσοτικοποιείται ένα κόστος, και σκοπός μας είναι η ελαχιστοποίηση του κόστους ως προς όλα τα πρωτόκολλα. Προς αυτήν την κατεύθυνση, παρουσιάζονται τετριμμένα πρωτόκολλα για τα NP-πλήρη προβλήματα των d-SAT και d-Vertex-Cover. Αυτά τα τετριμμένα πρωτόκολλα αποδεικνύονται και βέλτιστου κόστους, υπό την υπόθεση ότι η πολυωνυμική ιεραρχία δεν καταρρέει. Αυτό το γεγονός έχει ενδιαφέρουσες επιπτώσεις σε τομείς της Παραμετρικής Πολυπλοκότητας αυτών των προβλημάτων και συγκεκριμένα στην αραιοποίηση, πυρηνοποίηση και συμπίεση, οι οποίες και παρουσιάζονται ως πορίσματα των κεντρικών αποτελεσμάτων.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Υπολογιστική Πολυπλοκότητα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Αφηρημένα Μοντέλα Υπολογισμού, Κυκλωματική Πολυπλοκότητα, Πολυωνυμική Αναγωγή, Πολυωνυμική Ιεραρχία, Πρωτόκολλο Επικοινωνίας

CONTENTS

LIST OF FIGURES

1. ΕΙΣΑΓΩΓΗ

1.1 Ιστορικό Πλαίσιο

Όλα ξεκίνησαν με το πρώτο θεωρητικό μοντέλο υπολογισμού, την μηχανή Turing, που αναπτύχθηκε από τον Alan Turing το 1936. Παρά την απλότητά της και την θεωρητική φύση της, η μηχανή Turing απεδείχθη ένα ισχυρό μοντέλο υπολογισμού, στο οποίο βασίστηκαν οι πρώτοι ηλεκτρονικοί υπολογιστές που αναπτύχθηκαν στις δεκαετίες του 1940, 1950. Ωστόσο το μοντέλο του Turing, δεν λάμβανε υπόψιν, τον χρόνο ή την μνήμη που χρειαζόνταν ένας υπολογιστής για τους υπολογισμούς. Η ιδέα να μετρηθεί ο χρόνος και ο χώρος των υπολογισμών συναρτήσει του μεγέθους της εισόδου ήρθε στις αρχές της δεκαετίας του 1960 και οδήγησε ουσιαστικά στην αρχή και θεμελίωση του κλάδου της Υπολογιστικής Πολυπλοκότητας. Έτσι δημιουργήθηκε η ιδέα του αποδοτικού υπολογισμού, μέσω του πολυωνυμικού χρόνου εκτέλεσης ως προς το μέγεθος εισόδου, και οδηγηθήκαμε στις κλάσεις **P, NP**, την ιδέα της **NP**-πληρότητας με το θεώρημα των Cook-Levin, και το θεμελιώδες ανοιχτό πρόβλημα εάν **P = NP**. Έκτοτε, έχουν αναδυθεί άλλες κλάσεις πολυπλοκότητας από την προσπάθεια των ερευνητών να μελετήσουν άλλα μοντέλα υπολογισμού. Έτσι είχαμε την ανάπτυξη περιοχών όπως η κυκλωματική πολυπλοκότητα, οι πιθανοτικές κλάσεις πολυπλοκότητας, οι κλάσεις Παραμετρικής Πολυπλοκότητας, κβαντικά μοντέλα υπολογισμού κλπ.

1.2 Εισαγωγικοί Ορισμοί

Σε αυτήν την ενότητα παρουσιάζουμε και ορίζουμε κάποιες γενικές προκαταρκτικές έννοιες, σαν υπενθύμιση στον αναγνώστη, καθώς θα μας είναι χρήσιμες στη συνέχεια στην ανάλυση που θα κάνουμε.

Για αυτά που αναφέρουμε παρακάτω και για περισσότερες λεπτομέρειες και τυπικούς ορισμούς περί μηχανών Turing, Κλάσεων Πολυπλοκότητας, Κυκλωματικής Πολυπλοκότητας και Πολυωνυμικής Ιεραρχίας ανατρέξτε στα παρακάτω βιβλία Υπολογιστικής Πολυπλοκότητας: [1], [3], [10].

Επιπλέον, για αυτά που αναφέρουμε παρακάτω περί ορισμών Παραμετρικής Πολυπλοκότητας και για περισσότερες λεπτομέρειες ανατρέξτε στα παρακάτω βιβλία Παραμετρικής Πολυπλοκότητας: [4], [7].

1.2.1 Γενικοί Ορισμοί

- **Αλφάβητο** είναι ένα μη κενό, πεπερασμένο σύνολο. Τα στοιχεία του ονομάζονται σύμβολα, ενώ το αλφάβητο συμβολίζεται συνήθως με Σ.
- **Συμβολοσειρά (String)** ενός αλφάβητου Σ είναι μια πεπερασμένη ακολουθία συμβόλων του Σ. Αν η ακολουθία αυτή είναι κενή, αναφερόμαστε στην κενή συμβολοσειρά ϵ. Το μήκος μιας συμβολοσειράς x, είναι απλά το πλήθος συμβόλων που αυτή περιέχει και συμβολίζεται με $|x|$.
- Δεδομένου ενός αλφάβητου Σ, με Σ^*, συμβολίζουμε το σύνολο όλων των συμβολοσειρών του Σ. Το αλφάβητο που θα έχουμε στην παρούσα εργασία θα είναι το

$\Sigma = \{0,1\}$ και θα αναφερόμαστε στο $\Sigma^* = \{0,1\}^*$.

- Δεδομένου ενός αλφάβητου Σ, **γλώσσα** του Σ, ονομάζουμε οποιοδήποτε υποσύνολο του Σ^*.
- Μια $\boldsymbol{d}$**-CNF** φόρμουλα πάνω στις δυαδικές μεταβλητές $x_1, x_2, ..., x_n$ είναι μια σύζευξη όρων (clauses) όπου κάθε όρος είναι η διάζευξη ακριβώς d λεκτικών (literals), όπου ένα λεκτικό είναι μια μεταβλητή ή η άρνηση μιας μεταβλητής.
- $\boldsymbol{d}$**-SAT** είναι το πρόβλημα, δεδομένης μιας d-CNF, να αποφασιστεί αν αυτή είναι ικανοποιήσιμη, δηλαδή αν υπάρχει ανάθεση τιμών αλήθειας στις μεταβλητές, ώστε κάθε όρος να αποτιμάται ως αληθής.
- Ένα **υπεργράφημα (hypergraph)** είναι ένα ζεύγος $G = (V(G), E(G))$, όπου $V(G)$ ένα πεπερασμένο σύνολο στοιχείων, οι λεγόμενες κορυφές του υπεργραφήματος και $E(G)$ ένα σύνολο υποσυνόλων του $V(G)$, οι λεγόμενες ακμές του υπεργραφήματος.
- Ένα υπεργράφημα $G = (V(G), E(G))$ λέγεται $\boldsymbol{d}$**-ομοιόμορφο** ($\boldsymbol{d}$**-uniform**), αν κάθε ακμή, κάθε στοιχείο-σύνολο του $E(G)$ έχει ακριβώς d στοιχεία.
- **Κάλυμμα κορυφών (vertex cover)** ενός υπεργραφήματος $G = (V(G), E(G))$ είναι ένα $S \subseteq V(G)$ τέτοιο ώστε $\forall e \in E(G)$ να είναι $e \cap S \neq \emptyset$.
- $\boldsymbol{d}$**-VERTEX COVER** είναι το πρόβλημα, δεδομένου ενός d-ομοιόμορφου υπεργραφήματος G και ενός $k \in \mathbb{N}$, να αποφασιστεί αν υπάρχει ένα κάλυμμα κορυφών του G πληθάριθμου μικρότερου ή ίσου του k.
- **Κλίκα (clique)** ενός d-ομοιόμορφου υπεργραφήματος $G = (V(G), E(G))$ είναι ένα $S \subseteq V(G)$ τέτοιο ώστε κάθε υποσύνολο του S πληθάριθμου ακριβώς d να είναι ακμή του G, δηλαδή $\forall e,\ e \subseteq S,\ |e| = d$ να ισχύει ότι $e \in E(G)$.
- $\boldsymbol{d}$**-CLIQUE** είναι το πρόβλημα, δεδομένου ενός d-ομοιόμορφου υπεργραφήματος G και ενός $k \in \mathbb{N}$, να αποφασιστεί αν υπάρχει κλίκα του G πληθάριθμου μικρότερου ή ίσου του k.
- Έστω $L \subseteq \{0,1\}^*$. Ορίζουμε την γλώσσα $\boldsymbol{OR(L)}$ ως εξής:

$$(x_1, x_2, ..., x_t) \in OR(L) \Leftrightarrow \exists i \in [t] \text{ τέτοιο ώστε } x_i \in L$$

- Μια **πολυωνυμική αναγωγή (polynomial reduction ή $\boldsymbol{\leq^p_m}$ reduction)** από μια γλώσσα $L \subseteq \{0,1\}^*$ σε μία άλλη $L' \subseteq \{0,1\}^*$, είναι μια πολυωνυμικού χρόνου αντιστοίχιση $\tau : \{0,1\}^* \to \{0,1\}^*$, τέτοια ώστε $x \in L \Leftrightarrow \tau(x) \in L'$. Συμβολίζουμε με $L \leq^p_m L'$. Πρόκειται δηλαδή για μια πολυωνυμική μετατροπή ενός οποιουδήποτε στιγμιότυπου της L σε ένα ισοδύναμο στιγμιότυπο της L'.

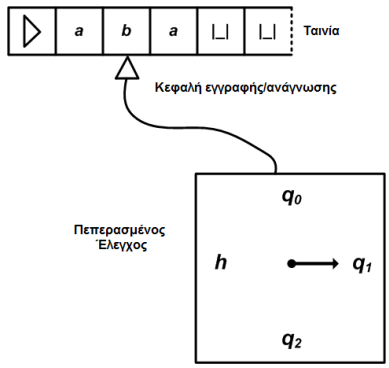
1.2.2 Ορισμοί από Κλασική Πολυπλοκότητα

Μηχανή Turing

Η μηχανή Turing, αποτελεί το πιο θεμελιώδες μοντέλο υπολογισμού. Παρά την απλότητά της, μπορεί να προσομοιώσει και τα πιο πολύπλοκα υπολογιστικά μοντέλα και είναι ικανή να περιγράψει οποιοδήποτε αλγόριθμο και να προσομοιώσει οποιαδήποτε γλώσσα προγραμματισμού.

Ουσιαστικά, η πιο απλή μηχανή Turing, αποτελείται από μία μονάδα ελέγχου πεπερασμένων καταστάσεων και μία ταινία. Η επικοινωνία μεταξύ τους επιτυγχάνεται με μία κεφαλή ανάγνωσης/εγγραφής, η οποία διαβάζει σύμβολα από την ταινία και χρησιμοποιείται επίσης για να μεταβάλει τα σύμβολα στην ταινία. Σε κάθε βήμα της μηχανής, δεδομένης της τωρινής κατάστασης της μηχανής και του συμβόλου που μόλις διαβάστηκε από την κεφαλή, γίνονται τα εξής: γράφεται ένα σύμβολο στην ταινία αντικαθιστώντας το ήδη υπάρχον που μόλις σαρώθηκε, η κεφαλή μετακινείται είτε μια θέση στα αριστερά είτε μια θέση στα δεξιά είτε δεν μετακινείται, ενημερώνεται η κατάσταση της μηχανής. Όπως βλέπουμε η λειτουργία της μηχανής είναι πράγματι στοιχειώδης και προσομοιάζει αρκετά τη λειτουργία ενός σύγχρονου ηλεκτρονικού υπολογιστή.

Τυπικά, μια **μηχανή Turing** είναι μια τετράδα $M = (K, \Sigma, \delta, s)$. Εδώ K είναι ένα πεπερασμένο σύνολο καταστάσεων της μηχανής. $s \in K$ είναι η αρχική κατάσταση, εκεί που ξεκινάει τη λειτουργία της η μηχανή. Σ είναι το αλφάβητο της μηχανής, το οποίο θεωρούμε πάντα περιέχει τα ειδικά σύμβολα $\sqcup$ και $\triangleright$, που συμβολίζουν τον κενό χαρακτήρα και τον πρώτο χαρακτήρα της ταινίας αντίστοιχα. Τέλος δ είναι η συνάρτηση μετάβασης, με $\delta : K \times \Sigma \to (K \cup \{y, n\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}$, όπου y, n είναι καταστάσεις αποδοχής, απόρριψης αντίστοιχα και τα σύμβολα $\leftarrow, \rightarrow, -$ συμβολίζουν κίνηση της κεφαλής μια θέση προς τα αριστερά, δεξία ή παραμονή στην ίδια θέση αντίστοιχα. Επίσης υποθέτουμε ότι $\leftarrow, \rightarrow, - \notin K \cup \Sigma$. Ο ορισμός της δ ακολουθεί πλήρως την περιγραφή της λειτουργίας της μηχανής που περιγράψαμε παραπάνω και αποτελεί το πρόγραμμα της μηχανής, αφού καθορίζει πλήρως κάθε βήμα της.



Σχήμα 1.1: Αναπαράσταση μιας απλής μηχανής Turing

Μια μηχανή Turing M αποδέχεται ή απορρίπτει μια είσοδο x, αν τερματίζει στην κατάσταση αποδοχής y ή στην κατάσταση απόρριψης n αντίστοιχα, με είσοδο την x γραμμένη στην ταινία της. Και θα συμβολίζουμε με $M(x) = 1$ ή $M(x) = 0$ αντίστοιχα.

Σημείωση: Επικεντρωνόμαστε σε μηχανές Turing που αποφασίζουν προβλήματα απόφασης, δηλαδή που σαν τελικές καταστάσεις τερματισμού έχουν μόνο αποδοχή/απόρριψη.

Μια μηχανή Turing M αποφασίζει ή αναγνωρίζει μια γλώσσα $L \subseteq \{0,1\}^*$ αν για κάθε $x \in \{0,1\}^*$ ισχύει: $x \in L \Leftrightarrow M(x) = 1$.

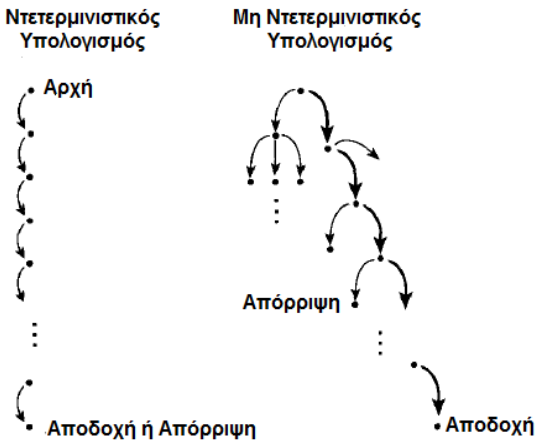
Μια μηχανή Turing M τρέχει σε χρόνο $T(n)$ εάν για κάθε $x \in \{0,1\}^*$, η M τερματίζει εντός $T(|x|)$ βημάτων υπολογισμού.

Παρατηρήστε ότι στον παραπάνω ορισμό της μηχανής Turing, λόγω της συνάρτησης δ, η

λειτουργία της μηχανής σε κάθε είσοδο και σε κάθε βήμα υπολογισμού με την συγκεκριμένη είσοδο είναι πλήρως καθορισμένη και ντετερμινιστική. Η αλληλουχία υπολογισμού είναι απλά μια αλυσίδα. Πράγματι, οι ορισμοί που δώσαμε παραπάνω περιγράφουν **ντετερμινιστικές μηχανές Turing**.

Μια **μη ντετερμινιστική μηχανή Turing** είναι μια τετράδα $M = (K, \Sigma, \Delta, s)$, όπως και στον ορισμό της ντετερμινιστικής μηχανής Turing. Τα K, Σ, s είναι τα ίδια με πριν. Δεδομένου ότι σε μια μη ντετερμινιστική μηχανή Turing, δεν υπάρχει μια μοναδικά καθορισμένη επόμενη ενέργεια, αλλά ενδεχομένως πολλές επόμενες ενέργειες, η Δ δεν είναι πλέον συνάρτηση αλλά μία σχέση $\Delta \subset (K \times \Sigma) \times [(K \cup \{y, n\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}]$. Δηλαδή για κάθε συνδυασμό κατάστασης-συμβόλου, υπάρχουν ενδεχομένως παραπάνω από μία επιλογές για την επόμενη ενέργεια της μηχανής, ή και καμία.

Δηλαδή, για μια δεδομένη είσοδο, οι πιθανοί υπολογισμοί δεν είναι πλέον μια αλυσίδα, αλλά σχηματίζουν ένα δέντρο με πολλά "κλαδιά" υπολογισμού. Συνεπώς, η λειτουργία μιας μη ντετερμινιστικής μηχανής Turing για μια δεδομένη είσοδο δεν είναι απαραίτητα πάντα η ίδια. Αυτή η αντιπαράθεση φαίνεται στο παρακάτω σχήμα που προέρχεται από τον εξής σύνδεσμο.



Σχήμα 1.2: Αντιπαράθεση ντετερμινιστικού και μη ντετερμινιστικού υπολογισμού

Μια μη ντετερμινιστική μηχανή Turing M αποδέχεται μια είσοδο x, αν τερματίζει με είσοδο την x, στην κατάσταση αποδοχής y, για τουλάχιστον ένα κλαδί υπολογισμού. Διαφορετικά απορρίπτει την x. Και θα συμβολίζουμε με $M(x) = 1$ ή $M(x) = 0$ αντίστοιχα.

Μια μη ντετερμινιστική μηχανή Turing M αποφασίζει ή αναγνωρίζει μια γλώσσα $L \subseteq \{0, 1\}^*$ αν για κάθε $x \in \{0, 1\}^*$ ισχύει: $x \in L \Leftrightarrow M(x) = 1$.

Μια μη ντετερμινιστική μηχανή Turing M τρέχει σε χρόνο $T(n)$ εάν για κάθε $x \in \{0, 1\}^*$, και κάθε ακολουθία μη ντετερμινιστικών επιλογών, η M τερματίζει εντός $T(|x|)$ βημάτων υπολογισμού.

Υπάρχουν παραλλαγές της κλασικής μονοταινιακής ντετερμινιστικής μηχανής Turing, με πολλαπλές ταινίες. Αυτές οι παραλλαγές αποδεικνύονται ισοδύναμες υπολογιστικά με την απλή μονοταινιακή μηχανή Turing, καθώς η απλή μηχανή Turing μπορεί να τις προσομοιώσει, με μια μικρή πολυωνυμική χρονική επιβάρυνση. Εφόσον αυτή η επιβάρυνση είναι πολυωνυμική, δεν μας επηρεάζει τις κλάσεις πολυπλοκότητας που ορίζουμε παρακάτω,

είτε θεωρούμε απλές μονοταινιακές είτε θεωρούμε μηχανές Turing πολλαπλών ταινιών.

Κλάσεις Πολυπλοκότητας
Μια κλάση πολυπλοκότητας είναι ένα σύνολο γλωσσών, με κριτήριο ομαδοποίησης συνήθως τον υπολογισμό τους δεδομένου κάποιου πόρου (χρονικού, χωρικού κλπ).

Έστω $T : \mathbb{N} \to \mathbb{N}$ μια συνάρτηση. Τότε ορίζουμε την κλάση **DTIME**$(T(n))$ ως όλες τις γλώσσες που αποφασίζονται από μια ντετερμινιστική μηχανή Turing χρόνου $O(T(n))$.

Ορίζουμε ως **P** την κλάση όλων των γλωσσών που αποφασίζονται από πολυωνυμικά φραγμένες ντετερμινιστικές μηχανές Turing. Δηλαδή: **P** = $\bigcup_{c\geq 1}$**DTIME**(n^c).

Έστω $T : \mathbb{N} \to \mathbb{N}$ μια συνάρτηση. Τότε ορίζουμε την κλάση **NTIME**$(T(n))$ ως όλες τις γλώσσες που αποφασίζονται από μια μη ντετερμινιστική μηχανή Turing χρόνου $O(T(n))$.

Ορίζουμε ως **NP** την κλάση όλων των γλωσσών που αποφασίζονται από πολυωνυμικά φραγμένες μη ντετερμινιστικές μηχανές Turing. Δηλαδή: **NP** = $\bigcup_{c\in\mathbb{N}}$**NTIME**(n^c).

Ισοδύναμα η κλάση **NP** ορίζεται ως εξής: Μια γλώσσα $L \subseteq \{0,1\}^*$ ανήκει στην κλάση **NP**, εάν υπάρχει πολυώνυμο $p : \mathbb{N} \to \mathbb{N}$ και μια πολυωνυμικά φραγμένη ντετερμινιστική μηχανή Turing M ώστε $\forall x \in \{0,1\}^*$ να είναι: $x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}$ ώστε $M(x,u) = 1$.

Μια γλώσσα L λέγεται **NP-δύσκολη (NP-hard)** εάν $L' \leq_m^p L,\ \forall L' \in$ **NP**.

Μια γλώσσα L λέγεται **NP-πλήρης (NP-complete)** εάν L είναι **NP**-δύσκολη και επιπλέον $L \in$ **NP**.

Με αντίστοιχο τρόπο ορίζονται δύσκολα και πλήρη προβλήματα για οποιαδήποτε κλάση πολυπλοκότητας.

Εάν $L \subseteq \{0,1\}^*$ μια γλώσσα με $\overline{L}$ συμβολίζουμε το συμπλήρωμα της γλώσσας, δηλαδή $\overline{L} = \{0,1\}^* \backslash L$.

Ορίζουμε ως **coNP** την εξής κλάση πολυπλοκότητας: **coNP** = $\{L : \overline{L} \in$ **NP**$\}$.

Με αντίστοιχο τρόπο ορίζεται το συμπλήρωμα οποιασδήποτε κλάσης πολυπλοκότητας.

Ισοδύναμα η κλάση **coNP** ορίζεται ως εξής: Μια γλώσσα $L \subseteq \{0,1\}^*$ ανήκει στην κλάση **coNP**, εάν υπάρχει πολυώνυμο $p : \mathbb{N} \to \mathbb{N}$ και μια πολυωνυμικά φραγμένη ντετερμινιστική μηχανή Turing M ώστε $\forall x \in \{0,1\}^*$ να είναι: $x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)}$ ώστε $M(x,u) = 1$.

Κυκλωματική Πολυπλοκότητα (Circuit Complexity)
Εστιάζουμε στον ισοδύναμο ορισμό των κλάσεων κυκλωματικής πολυπλοκότητας, που χρησιμοποιεί μηχανές Turing που δέχονται συμβουλές.

Έστω C μια κλάση γλωσσών, και $l : \mathbb{N} \to \mathbb{N}$ μια συνάρτηση. Ορίζουμε την κλάση γλωσσών $C/l(n) \coloneqq \{L : \exists L' \in C$, ακολουθία συμβολοσειρών $a_0, a_1, ...$ με $|a_n| \leq l(n)$ τέτοια ώστε $\forall x : x \in L \Leftrightarrow (x, a_{|x|}) \in L'\}$.

Δηλαδή στην κλάση $C/l(n)$ ανήκουν όλες οι γλώσσες $L \subseteq \{0,1\}^*$, για τις οποίες υπάρχει μηχανή Turing M' που αποφασίζει κάποια γλώσσα $L' \in C$, την οποία αν εφοδιάσουμε με μία ακολουθία συμβολοσειρών συμβουλής (advice string sequence), να μπορεί να αποφασίσει την L. Δηλαδή να ισχύει: $x \in L \Leftrightarrow M'(x, a_{|x|}) = 1$.

Παρατηρήστε αφενός ότι κάθε συμβολοσειρά της ακολουθίας είναι φραγμένη σε μέγεθος από την l και αφετέρου ότι η συμβολοσειρά συμβουλής για μια είσοδο, εξαρτάται μόνο από το μέγεθος της εισόδου και όχι από την είσοδο. Δηλαδή δύο διαφορετικά στιγμιότυπα της L ίδιου μήκους, θα έχουν την ίδια συμβολοσειρά συμβουλής στην M'.

Πολυωνυμική Ιεραρχία (Polynomial Hierarchy - PH)
Η πολυωνυμική ιεραρχία είναι μια ένωση κλάσεων γλωσσών που περιέχει όλες τις γλώσσες που μπορούν να οριστούν μέσω ενός πολυωνυμικά υπολογίσιμου κατηγορήματος, το οποίο θα είναι μια πολυωνυμικά φραγμένη μηχανή Turing ουσιαστικά, και ενός σταθερού πλήθους εναλλασσόμενων $\forall, \exists$ ποσοδεικτών. Πιο τυπικά:

Για κάθε $i \geq 0$, ορίζεται η κλάση Σ_i^p, ως το σύνολο όλων των γλωσσών $L \subseteq \{0,1\}^*$ για τις οποίες υπάρχει μια πολυωνυμικά φραγμένη μηχανή Turing M και ένα πολυώνυμο p ώστε:

$$x \in L \Leftrightarrow \exists u_1 \in \{0,1\}^{p(|x|)}\ \forall u_2 \in \{0,1\}^{p(|x|)}\ ...\ Q_i u_i \in \{0,1\}^{p(|x|)}\ M(x, u_1, u_2, ..., u_i) = 1$$

Όπου ο τελικός ποσοδείκτης Q_i είναι είτε $\exists$ είτε $\forall$ ανάλογα με το αν i περιττός ή άρτιος αντίστοιχα.

Όμοια για κάθε $i \geq 0$, ορίζεται η κλάση Π_i^p, ως το σύνολο όλων των γλωσσών $L \subseteq \{0,1\}^*$ για τις οποίες υπάρχει μια πολυωνυμικά φραγμένη μηχανή Turing M και ένα πολυώνυμο p ώστε:

$$x \in L \Leftrightarrow \forall u_1 \in \{0,1\}^{p(|x|)}\ \exists u_2 \in \{0,1\}^{p(|x|)}\ ...\ Q_i u_i \in \{0,1\}^{p(|x|)}\ M(x, u_1, u_2, ..., u_i) = 1$$

Όπου ο τελικός ποσοδείκτης Q_i είναι είτε $\forall$ είτε $\exists$ ανάλογα με το αν i περιττός ή άρτιος αντίστοιχα.

Η πολυωνυμική ιεραρχία όπως είπαμε είναι η ένωση των παραπάνω κλάσεων, δηλαδή $\boldsymbol{PH} = \bigcup_i \Sigma_i^p = \bigcup_{i>0} \Pi_i^p$.

Επίσης έχουμε $\Pi_0^p = \Sigma_0^p =$ **P**, $\Sigma_1^p =$ **NP** και $\Pi_1^p =$ **coNP**.

Θεώρημα Κατάρρευσης της PH [1]. Για $i \geq 1$, αν $\Sigma_i^p = \Pi_i^p$, τότε $PH = \Sigma_i^p$, δηλαδή η πολυωνυμική ιεραρχία καταρρέει στο i-οστό της επίπεδο.

Σκιαγράφηση της απόδειξης μπορείτε να βρείτε στο [1].

Πόρισμα [1]. Για $i \geq 1$, αν $\Sigma_i^p = \Sigma_{i+1}^p$, τότε $PH = \Sigma_i^p$

Απόδειξη. Εύκολα βλέπουμε από τους ορισμούς ότι γενικά ισχύει $\Pi_i^p \subseteq \Sigma_{i+1}^p$ και συνεπώς από υπόθεση $\Pi_i^p \subseteq \Sigma_i^p$. Και επειδή για οποιαδήποτε κλάση πολυπλοκότητας K, ισχύει $K \subseteq co\text{-}K \Leftrightarrow K = co\text{-}K$, έπεται ότι $\Sigma_i^p = \Pi_i^p$ και άρα από προηγούμενο Θεώρημα $PH = \Sigma_i^p$ ■

Μπορούμε να ορίσουμε και τις κλάσεις κυκλωματικής ιεραρχίας αντίστοιχα με τις κλάσεις της πολυωνυμικής ιεραρχίας ως $\Pi_i^p/poly,\ \Sigma_i^p/poly$ για $i \geq 1$. Και εκεί ισχύει κάτι αντίστοιχο με το πόρισμα που δείξαμε για την πολυωνυμική ιεραρχία: Για $i \geq 1$, αν $\Sigma_i^p/poly = \Sigma_{i+1}^p/poly$, τότε $PH/poly = \Sigma_i^p/poly$ [11].

Όταν είναι προφανές ότι αναφερόμαστε σε κλάσεις της πολυωνυμικής ιεραρχίας, οι εκθέτες θα παραλείπονται και θα γράφουμε Π_i, Σ_i, αντί για Π_i^p, Σ_i^p.

1.2.3 Ορισμοί από Παραμετρική Πολυπλοκότητα

Ένα **παραμετροποιημένο πρόβλημα (parameterized problem)** είναι μια γλώσσα $L \subseteq \Sigma^* \times \mathbb{N}$, όπου Σ ένα συγκεκριμένο αλφάβητο. Για ένα στιγμιότυπο $(x, k) \in \Sigma^* \times \mathbb{N}$ του προβλήματος, k λέγεται η παράμετρος του στιγμιότυπου.

Στην παραμετρική πολυπλοκότητα ιδιαίτερο ενδιαφέρον έχουν οι μέθοδοι επίτευξης χρόνων εκτέλεσης της μορφής $O(f(k) \cdot poly(|(x, k)|))$, σε στιγμιότυπα (x, k) όπου x η είσοδος και k η παράμετρος, και f μια συνάρτηση μόνο της παραμέτρου k. Η ιδέα είναι ότι για σταθερές μικρές τιμές της παραμέτρου, η εξάρτηση του χρόνου εκτέλεσης από την f, η οποία f μπορεί να είναι και συνήθως είναι μια "κακά συμπεριφερόμενη" συνάρτηση, είναι σχετικά μικρή, καθιστώντας τέτοιου τύπου χρόνους εκτέλεσης αρκετά ελκυστικούς.

Ένα παραμετροποιημένο πρόβλημα $L \subseteq \Sigma^* \times \mathbb{N}$ για το οποίο το ερώτημα $(x, k) \in L$ απαντάται σε χρόνο $O(f(k) \cdot poly(|(x, k)|))$, ανήκει στην κλάση FPT.

Μια άλλη πολύ χρήσιμη έννοια είναι αυτή της πυρηνοποίησης, δεδομένου ότι είναι μια κατεξοχήν μέθοδος επίτευξης τέτοιων χρόνων.

Η **πυρηνοποίηση** ενός παραμετροποιημένου προβλήματος $L \subseteq \Sigma^* \times \mathbb{N}$, είναι μια πολυωνυμική $\leq_m^p$ αναγωγή από την L στον εαυτό της που αντιστοιχεί στιγμιότυπα (x, k) σε (x', k') ώστε: $(x, k) \in L \Leftrightarrow (x', k') \in L$ και το μέγεθος του ανηγμένου στιγμιοτύπου, δηλαδή το $|(x', k')|$, να είναι φραγμένο από μια υπολογίσιμη συνάρτηση h ως προς το k. Το ανηγμένο στιγμιότυπο (x', k') αναφέρεται και ως ο πυρήνας, και αν η h είναι πολυώνυμο, λέμε ότι η L επιδέχεται πολυωνυμικό πυρήνα. Η ύπαρξης πυρηνοποίησης για την L, την καθιστά πυρηνοποιήσιμη.

Έπειτα το ανηγμένο στιγμιότυπο επιλύεται με κάποια συνάρτηση g, συνήθως ωμής βίας. Αυτό δίνει έναν χρόνο εκτέλεσης της μορφής $O(g(h(k)) + poly(|(x, k)|))$, δηλαδή για $f = g \circ h$, χρόνο εκτέλεσης $O(f(k) + poly(|(x, k)|))$, για να αποφασίσουμε εάν $(x, k) \in L$. Προφανώς θέλουμε οι g, h να συμπεριφέρονται καλά, ώστε το $g(h(k))$ να είναι όσο μικρό γίνεται.

Η κλάση FPT και η πυρηνοποίηση μοιάζουν σαν έννοιες, έχουν ίδιο σκοπό και έχουν παρόμοιους χρόνους εκτέλεσης $O(f(k) \cdot poly(|(x, k)|))$ και $O(f(k) + poly(|(x, k)|))$ αντίστοιχα. Στην ουσία είναι ισοδύναμες έννοιες σύμφωνα με το παρακάτω λήμμα.

Λήμμα (Λήμμα Ισοδυναμίας)**.** *Έστω παραμετροποιημένη γλώσσα $L \subseteq \Sigma^* \times \mathbb{N}$. Τότε έχουμε ότι $L \in FPT \Leftrightarrow L$ αποφασίσιμη και πυρηνοποιήσιμη.*

Για την απόδειξη ανατρέξτε στο Παράρτημα Β.

1.3 Το Αφηρημένο Επικοινωνιακό Μοντέλο Υπολογισμού

Σε αυτήν την ενότητα συνεχίζουμε με την περιγραφή του προαναφερόμενου επικοινωνιακού μοντέλου υπολογισμού μεταξύ 2 παιχτών, τον τυπικό ορισμό ενός πρωτοκόλλου επικοινωνίας πάνω στο μοντέλο, τις λεπτομέρειες μοντελοποίησης των παιχτών μέσω μηχανών Turing και συναρτήσεων καθώς και τον ορισμό του κόστους ενός πρωτοκόλλου και του κόστους αναγνώρισης γενικά. Κλείνοντας, αναφέρουμε το κίνητρο και τον σκοπό μελέτης του συγκεκριμένου αφηρημένου επικοινωνιακού μοντέλου.

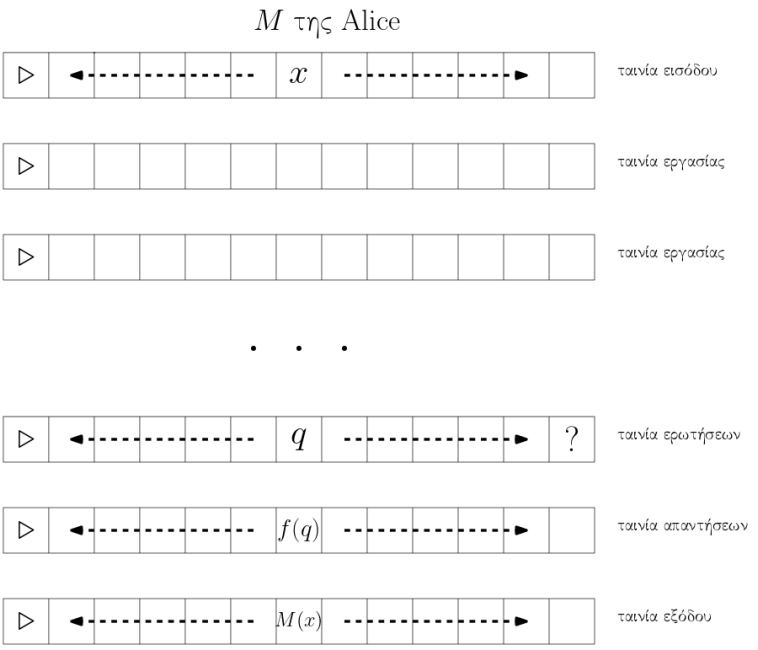
1.3.1 Περιγραφή επικοινωνιακού μοντέλου

Θεωρήστε τον εξής αφηρημένο τρόπο επικοινωνίας μεταξύ 2 συνεργατικών παιχτών της Alice και του Bob, με σκοπό την αναγνώριση μιας γλώσσας $L \subseteq \Sigma^*$. Η Alice έχει σαν είσοδο μια συμβολοσειρά x, αλλά τρέχει σε πολυωνυμικό χρόνο ως προς το μέγεθος εισόδου $|x|$, ενώ ο Bob είναι υπολογιστικά απεριόριστος, αλλά δεν γνωρίζει την x. Οι παίχτες επικοινωνούν ανταλλάσσοντας μηνύματα-bits, σύμφωνα με κάποιο πρωτόκολλο, και στο τέλος της επικοινωνίας, η Alice πρέπει να είναι σε θέση να αποφασίσει αν $x \in L$. Σαν κόστος του πρωτοκόλλου ορίζουμε το συνολικό πλήθος bits που στέλνει η Alice στον Bob κατά της διάρκεια της επικοινωνίας.

1.3.2 Τυπική μοντελοποίηση των παιχτών

Πιο τυπικά, ο υπολογιστικά περιορισμένος παίχτης, δηλαδή η Alice, μοντελοποιείται ως μια πολυωνυμικά φραγμένη μηχανή Turing M. Ο υπολογιστικά απεριόριστος παίχτης, δηλαδή ο Bob, μοντελοποιείται ως μια υπολογίσιμη συνάρτηση f. Η M, πέρα των ταινιών εισόδου, εργασίας και εξόδου που διαθέτει, είναι εφοδιασμένη και με μια ταινία ερωτήσεων, μια ταινία απαντήσεων και ένα ειδικό σύμβολο ερώτησης $?$ στο αλφάβητό της. Κάθε φορά που η Alice θέλει να χρησιμοποιήσει τον Bob, γράφει μια συμβολοσειρά-ερώτημα στο τέλος της ταινίας ερωτήσεων και αμέσως μετά το ειδικό σύμβολο ερώτησης $?$. Με το που γράφει το $?$, τα τωρινά περιεχόμενα της ταινίας απαντήσεων, αντικαθίστανται μονομιάς, σε ένα βήμα υπολογισμού, από το $f(q)$, όπου $q \in \{0,1\}^*$ τα τωρινά περιεχόμενα της ταινίας ερωτήσεων. Η ταινία ερωτήσεων δεν διαγράφεται, ό,τι νέο ερώτημα προσαρτάται στο τέλος της ταινίας, ώστε η στρατηγική και οι απαντήσεις του Bob να εξαρτώνται από όλο το ιστορικό ερωτημάτων. Επίσης, η f εξαρτάται μόνο από το q, δηλαδή τα περιεχόμενα της ταινίας ερωτήσεων, και όχι άμεσα από το x, όπως ακριβως υποθέσαμε.

Υπάρχουν και παραλλαγές του ορισμού, όπου η Alice, δηλαδή η M είναι μη ντετερμινιστική.



Σχήμα 1.3: Η μοντελοποίηση της Alice ως μηχανή Turing

1.3.3 Ορισμός πρωτοκόλλου επικοινωνίας

Όπως είδαμε ο Bob και η f λειτουργούν ως ένα "μαντείο". Απλά δέχονται και απαντούν ερωτήματα. Για αυτό και η f, αναφέρεται και σαν συνάρτηση μαντείου (Oracle Function).

Όταν αναφερόμαστε σε ένα πρωτόκολλο εποικοινωνίας, αναφερόμαστε στην ακολουθία ερωτήσεων και απαντήσεων της επικοινωνίας των δύο παιχτών.

Δεδομένης μιας συνάρτησης μαντείου f λοιπόν, ένα πρωτόκολλο επικοινωνίας t γύρων P (t round oracle communication protocol), δεν είναι τίποτα άλλο παρά μια ακολουθία t δυάδων της μορφής: $(q_1(.), f(q_1(.))),\ (q_2(.), f(q_2(.))),\ ...\ (q_t(.), f(q_t(.)))$.

Κάθε q_i είναι μια συνάρτηση που εξαρτάται άμεσα από την M, αφού αντιστοιχίζει μια οποιαδήποτε είσοδο x, στα περιεχόμενα της ταινίας ερωτήσεων της M με είσοδο x, μέχρι και την i-οστή εμφάνιση του συμβόλου $?$, περιέχει δηλαδή τις i πρώτες ερωτήσεις που κάνει η M με είσοδο x.

Επίσης θεωρούμε ομοιόμορφα πρωτόκολλα, δηλαδή που ανεξάρτητα από την είσοδο, έχουν ίδιο πλήθος ερωτήσεων και απαντήσεων. Παρατηρήστε ότι κάθε πρωτόκολλο μπορεί να μετατραπεί σε ένα ισοδύναμο ομοιόμορφο. Αυτό διότι για κάθε είσοδο το πλήθος ερωτήσεων/απαντήσεων είναι πεπερασμένο ή φραγμένο άρα μπορούμε να θεωρήσουμε ότι t θα είναι το μέγιστο πλήθος ερωτήσεων/απαντήσεων που γίνονται για οποιαδήποτε είσοδο ή ένα άνω φράγμα στο μέγιστο πλήθος. Έτσι για οποιαδήποτε είσοδο απαιτεί λιγότερες από t ερωτήσεις/απαντήσεις, θα γίνεται συμπλήρωση με "κενές" ερωτήσεις/απαντήσεις. Όπου μια "κενή" ερώτηση/απάντηση ουσιαστικά θα θέτει $f(q) = \epsilon$, δηλαδή την κενή συμβολοσειρά. Και για να σηματοδοτηθεί η κενή ερώτηση/απάντηση, μπορούμε να εισάγουμε ένα άλλο ειδικό σύμβολο τερματισμού #, ώστε $f(q) = \epsilon$ αν και μόνο αν το σύμβολο # εμφανίζεται στην q.

Επιπλέον, είναι προφανές, ότι αυτή η ακολουθία για οποιαδήποτε είσοδο, προσδιορίζεται πλήρως από την επιλογή των M, f, για αυτό και όταν αναφερόμαστε σε ένα πρωτόκολλο θα εννοούμε απλώς μια δυάδα $P = (M, f)$.

Θα λέμε ότι το μοντέλο αποφασίζει μια παραμετροποιημένη γλώσσα $L \subseteq \Sigma^* \times \mathbb{N}$ αν υπάρχει κάποιο πρωτόκολλο επικοινωνίας των δύο παιχτών, ώστε δεδομένου ενός οποιουδήποτε $x \in \Sigma^* \times \mathbb{N}$ στην είσοδο, στο τέλος του πρωτοκόλλου η Alice να δέχεται την x αν και μόνο αν $x \in L$. Δηλαδή να υπάρχει μηχανή Turing M και να υπάρχει υπολογίσιμη συνάρτηση f, ώστε η M με πρόσβαση στην συνάρτηση μαντείου f να δέχεται την είσοδο x αν και μόνο αν $x \in L$. Ισοδύναμα το μοντέλο αποφασίζει την $L \subseteq \Sigma^* \times \mathbb{N}$ όταν:

$$\exists M, f \text{ ώστε } x \in L \Leftrightarrow M(f, x) = 1$$

1.3.4 Ορισμός κόστους πρωτοκόλλου

Έστω μια παραμετροποιημένη γλώσσα $L \subseteq \Sigma^* \times \mathbb{N}$, και ένα πρωτόκολλο t γύρων που αποφασίζει την L. Σαν κόστος ενός στιγμιοτύπου $x = (w, k)$, ορίζουμε το συνολικό πλήθος bits που στέλνει η Alice στον Bob κατά την διάρκεια του πρωτοκόλλου με είσοδο x, δηλαδή ισοδύναμα το συνολικό πλήθος bits που γράφονται από την M στην ταινία ερωτήσεων της, με είσοδο x, δηλαδή ισοδύναμα το $|q_t(x)|$.

Όταν μιλάμε γενικά για το κόστος του πρωτοκόλλου, αναφερόμαστε στο πώς συμπεριφέρεται στη χειρότερη περίπτωση, το κόστος των στιγμιοτύπων σαν συνάρτηση της παραμέτρου k της γλώσσας, για όλα τα στιγμιότυπα της γλώσσας με παράμετρο k.

Και όταν μιλάμε για το κόστος αναγνώρισης της γλώσσας L γενικά από το μοντέλο, αναφερόμαστε στην μικρότερη ασυμπτωτικά συνάρτηση κόστους από όλα τα πρωτόκολλα που αποφασίζουν την L.

1.3.5 Κίνητρο μελέτης του μοντέλου

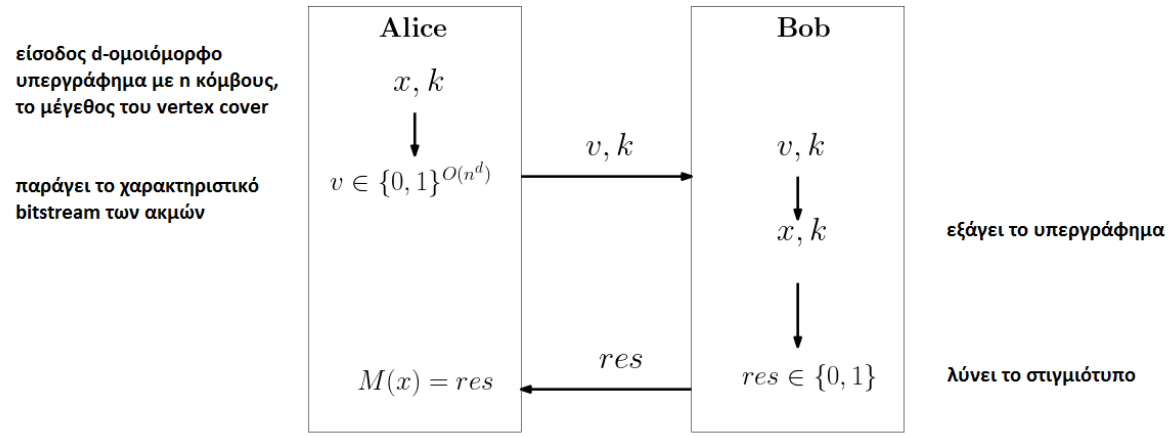
Δεδομένης μιας παραμετροποιημένης γλώσσας $L \subseteq \Sigma^* \times \mathbb{N}$, ο σκοπός γενικά είναι η εύρεση του πρωτοκόλλου που ελαχιστοποιεί την συνάρτηση κόστους ως προς την παράμετρο της γλώσσας. Για την γνωστή μας κλάση **P**, των γλωσσών που αποφασίζονται από πολυωνυμικά φραγμένες ντετερμινιστικές μηχανές Turing, υπάρχουν τετριμμένα "κενά" πρωτόκολλα μηδενικού κόστους. Και αυτό διότι η Alice μπορεί από μόνη της να αποφασίσει οποιαδήποτε πολυωνυμικά αποφασίσιμη γλώσσα δίχως τη βοήθεια του Bob. Το ενδιαφέρον λοιπόν υπάρχει σε προβλήματα-γλώσσες για τα οποία δεν είναι γνωστοί ντετερμινιστικοί πολυωνυμικοί αλγόριθμοι που να τα αποφασίζουν. Η μελέτη λοιπόν επικεντρώνεται στα **NP**-πλήρη και **NP**-δύσκολα προβλήματα. Το ερώτημα είναι λοιπόν, πόσο αποδοτικά πρωτόκολλα μπορούν να κατασκευαστούν για τέτοιου είδους προβλήματα, πώς δηλαδή μπορεί η Alice να εκμεταλλευτεί την απεριόριστη υπολογιστική δύναμη του Bob, ώστε να κατασκευάσει φτηνά πρωτόκολλα που αποφασίζουν δύσκολες γλώσσες.

2. ΤΕΤΡΙΜΜΕΝΑ ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΚΕΝΤΡΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

2.1 Πρωτόκολλο για το d- VERTEX COVER

Θεωρούμε το πρόβλημα του d- VERTEX COVER παραμετροποιημένο ως προς το πλήθος των κορυφών n του υπεργραφήματος. Μπορούμε να φτιάξουμε ένα πρωτόκολλο κόστους $O(n^d)$ για το πρόβλημα ως εξής: Παρατηρήστε ότι υπάρχουν $\binom{n}{d} = O(n^d)$ διακριτά υποσύνολα d στοιχείων ως προς τις κορυφές, άρα και $O(n^d)$ πιθανές ακμές σε ένα οποιοδήποτε d ομοιόμορφο υπεργράφημα. Τόσο η Alice όσο και ο Bob μπορούν να θεωρήσουν μια δεδομένη σειρά, πχ λεξικογραφική, αυτών των $O(n^d)$ ακμών. Η Alice λοιπόν με είσοδο ένα d- ομοιόμορφο υπεργράφημα G με n κορυφές και $k \leq n$ το μέγεθος του καλύμματος κορυφών, ελέγχει για κάθε μία εκ των $O(n^d)$ ακμών, με τη δεδομένη σειρά, αν εμφανίζεται ή όχι στο G και παράγει ένα bit 1 ή 0 αντίστοιχα. Έτσι συνολικά παράγει ένα bitstream $v \in \{0,1\}^{O(n^d)}$ το οποίο και στέλνει μετά στον Bob, μαζί με το k. Αυτός από το bitstream, εξάγει το G και μαζί με το k, λύνει εξαντλητικά το στιγμιότυπο, αφού είναι απεριόριστος υπολογιστικά, και επιστρέφει 1 ή 0 στην Alice, ανάλογα αν το στιγμιότυπο είναι καταφατικό ή όχι αντίστοιχα.

Το κόστος του πρωτοκόλλου είναι προφανώς $O(n^d + logn) = O(n^d)$.



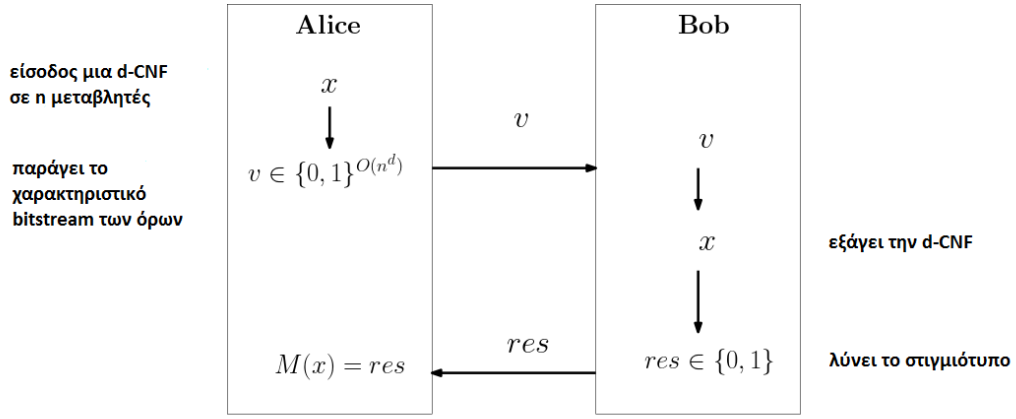
Σχήμα 2.1: Το τετριμμένο πρωτόκολλο για το d-VERTEX COVER

2.2 Πρωτόκολλο για το d- SAT

Θεωρούμε το πρόβλημα του d- SAT παραμετροποιημένο ως προς το πλήθος των μεταβλητών n της λογικής φόρμουλας. Με αντίστοιχη λογική με πριν, το εξής πρωτόκολλο αποφασίζει το d- SAT: Παρατηρήστε ότι υπάρχουν $\binom{n}{d} \cdot 2^d = O(n^d)$ διακριτοί όροι (clauses) σε μια d-CNF, δηλαδή διακριτοί όροι με ακριβώς d λεκτικά (literals) πάνω σε n μεταβλητές.

Τόσο η Alice όσο και ο Bob μπορούν να θεωρήσουν μια δεδομένη πχ λεξικογραφική σειρά αυτών των $O(n^d)$ όρων. Η Alice λοιπόν, με είσοδο x μια d-CNF πάνω σε n μεταβλητές, για κάθε ένα εκ των $O(n^d)$ όρων, με τη δεδομένη σειρά, ελέγχει αν εμφανίζεται ή όχι στην x και παράγει ένα bit 1 ή 0 αντίστοιχα. Έτσι συνολικά παράγει ένα bitstream $v \in \{0,1\}^{O(n^d)}$ το οποίο και στέλνει μετά στον Bob. Αυτός, από το bitstream, εξάγει την d-CNF που αναπαριστά η x, και πάλι εξαντλητικά, δεδομένου ότι είναι απεριόριστος υπολογιστικά, λύνει το στιγμιότυπο, στέλνοντας στην Alice την τελική απάντηση 1 ή 0, ανάλογα αν η x είναι τελικά ικανοποιήσιμη ή όχι.

Το κόστος του πρωτοκόλλου είναι $O(n^d)$.



Σχήμα 2.2: Το τετριμμένο πρωτόκολλο για το d-SAT

2.3 Κάτω Φράγματα

Οπότε λοιπόν, έχουμε ήδη κάποια πολυωνυμικά ως προς την παράμετρο πρωτόκολλα για τα παραπάνω δύσκολα προβλήματα. Μπορούμε να κάνουμε καλύτερα; Τα παρακάτω δύο θεωρήματα, που αποτελούν και τα βασικά αποτελέσματα από τα οποία θα προκύψουν κάποιες ωραίες συνέπειες σαν πορίσματα μας λένε ότι η απάντηση στο ερώτημά μας είναι αρνητική. Εκτός αν η πολυωνυμική ιεραρχία καταρρέει, κάτι που θεωρείται ευρέως ότι δεν ισχύει, τα παραπάνω κόστη αποτελούν σφιχτά κάτω όρια για οποιοδήποτε πρωτόκολλο των παραπάνω προβλημάτων. Τα παρακάτω θεωρήματα προέρχονται από το [5].

Θεώρημα 1. *Έστω $d \in \mathbb{N}$, $d \geq 2$, και $\epsilon \in \mathbb{R}^+$. Δεν υπάρχει πρωτόκολλο κόστους $O(n^{d-\epsilon})$ για να αποφασιστεί εάν ένα d-ομοιόμορφο υπεργράφημα n κορυφών, έχει ένα κάλυμμα κορυφών μεγέθους το πολύ k, για δεδομένο $k \in \mathbb{N}$, εκτός αν ισχύει $coNP \subseteq NP/poly$.*

Θεώρημα 2. *Έστω $d \in \mathbb{N}$, $d \geq 3$, και $\epsilon \in \mathbb{R}^+$. Δεν υπάρχει πρωτόκολλο κόστους $O(n^{d-\epsilon})$ για να αποφασιστεί εάν μια d-CNF n μεταβλητών είναι ικανοποιήσιμη, εκτός αν ισχύει $coNP \subseteq NP/poly$.*

3. ΑΠΟΔΕΙΞΗ ΚΕΝΤΡΙΚΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Πρώτα θα αποδείξουμε το Θεώρημα 1 και στη συνέχεια το Θεώρημα 2 θα προκύψει από μια πολυωνυμική αναγωγή d- VERTEX COVER $\leq_m^p$ d-SAT.

3.1 Χρήσιμα Λήμματα

Εδώ παρουσιάζουμε κάποια λήμματα που θα μας είναι χρήσιμα στην απόδειξη για το Θεώρημα 1. Οι αποδείξεις των λημμάτων βρίσκονται στο Παράρτημα Α.

Λήμμα 1 (**Packing Lemma**). *Για ακέραιους $s \geq d \geq 2$ και $t > 0$, υπάρχει d-ομοιόμορφο υπεργράφημα P, με $|P| = O(s \cdot max\{s, t^{1/d+o(1)}\})$, με τις εξής ιδιότητες:*

(i) Οι ακμές του P διαμερίζονται σε t κλίκες $K_1, K_2, ..., K_t$, κάθε μία με ακριβώς s κόμβους

(ii) Το P δεν έχει άλλες κλίκες πέρα από τα K_i

Επίσης για σταθερό d, τα P, K_i με αυτές τις ιδιότητες κατασκευάζονται σε πολυωνυμικό χρόνο.

Το παραπάνω λήμμα προέρχεται από το [5], και αυτό που μας δίνει, είναι ένας, σχεδόν βέλτιστος ως προς το πλήθος των κορυφών, τρόπος να κατασκευάσουμε ένα υπεργράφημα που θα περιέχει ακριβώς t κλίκες s κόμβων. Παρατηρήστε ότι ο τετριμμένος τρόπος να πετυχαίναμε κάτι τέτοιο θα ήταν να παίρναμε ως P την ένωση t ξένων κλικών κάθε μία με ακριβώς s κόμβους. Όμως τότε το τελικό υπεργράφημα θα είχε $s \cdot t$ κόμβους που είναι αρκετά περισσότεροι από αυτούς του λήμματος και δεν ικανοποιούν τις ανάγκες μας όπως θα δούμε στη συνέχεια.

Λήμμα 2 (**Complementary Witness Lemma**). *Έστω γλώσσα $L \subseteq \{0,1\}^*$ και πολυωνυμικά φραγμένη συνάρτηση $t : \mathbb{N} \to \mathbb{N}\backslash\{0\}$, έτσι ώστε δεδομένων $t(s)$ στιγμιότυπων της L, μεγέθους το πολύ s το κάθενα, το να αποφασίσουμε αν τουλάχιστον ένα εκ αυτών ανήκει στην L, να έχει πρωτόκολλο κόστους $O(t(s) \cdot log(t(s)))$. Τότε $L \in coNP/poly$.*

Το παραπάνω λήμμα μας λέει ότι αν για κάποια L, η $OR(L)$ έχει σχετικά φτηνό πρωτόκολλο (γραμμικό-λογαριθμικού (linearithmic) κόστους), τότε η L ανήκει στην κλάση $coNP/poly$. Το λήμμα προέρχεται από το [5], όπου και μπορείτε να ανατρέξετε για την απόδειξή του.

Λήμμα 3. $(co\text{-}K)/poly = co\text{-}(K/poly)$

Λήμμα 4. *Για* $i > 0$, $\Pi_i \subseteq \Sigma_i/poly \Rightarrow \Sigma_i/poly = \Sigma_{i+1}/poly$

Λήμμα 5. *Για* $i > 0$, $\Pi_i \subseteq \Sigma_i/poly \Rightarrow \Sigma_i/poly = \Pi_i/poly$

Λήμμα 6. *Για* $i > 0$, $\Sigma_i/poly = \Pi_i/poly \Rightarrow PH/poly = \Sigma_i/poly$

Το λήμμα 6 παρουσιάζει μια ικανή συνθήκη για την κατάρρευση της πολυωνυμικής ιεραρχίας των κλάσεων με συμβουλές, αντίστοιχης αυτής της κλασικής πολυωνυμικής ιεραρχίας. Τα παραπάνω λήμματα προέρχονται από το [11].

Λήμμα 7. *Για* $i > 0$, $\Sigma_i/poly = \Pi_i/poly \Rightarrow \Sigma_{i+2} = \Pi_{i+2}$

Παρατηρήστε ότι το τελευταίο λήμμα υπονοεί την κατάρρευση της πολυωνυμικής ιεραρχίας στο $i + 2$ οστό της επίπεδο. Και αυτό προέρχεται από το [11].

3.2 Απόδειξη Θεωρήματος 1

Η απόδειξη προέρχεται από το [5]. Με δεδομένο ότι η πολυωνυμική ιεραρχία δεν καταρρέει, έστω προς άτοπο ότι υπάρχει καλύτερο πρωτόκολλο από το τετριμμένο που παρουσιάσαμε για το d-VERTEX COVER, παραμετροποιημένο ως προς το πλήθος κόμβων του γραφήματος. Δηλαδή έστω ότι υπάρχει πρωτόκολλο τάξης $O(n^c), c < d$.

Λόγω δυϊκότητας των d-VERTEX COVER και d-CLIQUE (υπάρχει η γνωστή πολυωνυμική αναγωγή που αντιστοιχεί στιγμιότυπα (G, k) του d-CLIQUE όπου G είναι d ομοιόμορφο υπεργράφημα και $k \in \mathbb{N}$ σε στιγμιότυπα $(\overline{G}, |G| - k)$ του d-VERTEX-COVER όπου $\overline{G}$ το συμπληρωματικό ως προς τις ακμές υπεργράφημα του G), και επειδή αυτή η αναγωγή διατηρεί το πλήθος των κόμβων, δηλαδή την τιμή της παραμέτρου στο ανηγμένο στιγμιότυπο, έχουμε ότι θα υπάρχει πρωτόκολλο τάξης $O(n^c), c < d$ και για το d-CLIQUE, προφανώς πάλι παραμετροποιημένο ως προς το πλήθος των κόμβων. Σε αυτό το πρωτόκολλο απλά η Alice, ο πολυωνυμικός παίχτης δηλαδή, εκτελεί την παραπάνω πολυωνυμική αναγωγή και έπειτα εφαρμόζει το $O(n^c)$ πρωτόκολλο του d-VERTEX COVER στο ανηγμένο στιγμιότυπο.

Ισχυρισμός. Υπάρχει πολυωνυμική ανάγωγη $OR(3SAT) \leq_m^p d$-CLIQUE, $\forall d \geq 2$. Μάλιστα αυτή η αναγωγή αντιστοιχεί το στιγμιότυπο του $OR(3SAT)$, δηλαδή την t-άδα στιγμιοτύπων του $3SAT$, μεγέθους $O(s)$ το καθένα, σε ένα d-ομοιόμορφο υπεργράφημα G, στιγμιότυπο του d-CLIQUE, με $O(s \cdot max\{s, t^{1/d+o(1)}\})$ κορυφές.

Απόδειξη. Έστω $(\phi_1, \phi_2, ..., \phi_t)$ στιγμιότυπο του $OR(3SAT)$, με χωρίς βλάβη της γενικότητας, ακριβώς s όρους ανά πρόταση, και προφανώς 3 λεκτικά ανά όρο. Το μέγεθος της εισόδου λοιπόν είναι $O(s \cdot t)$. Επίσης, έστω σταθερό $d \geq 2$. Η αναγωγή έχει ως εξής:

1. Δεδομένου των s, t, d, από το Λήμμα 1, κατασκευάζουμε τα υπεργραφήματα του λήμματος $P, K_1, ..., K_t$ με τις δεδομένες ιδιότητες.

2. Για όλα τα i, με $1 \leq i \leq t$, κατασκεύασε/αντιστοίχισε κάθε πρόταση ϕ_i σε ένα d ομοιόμορφο υπεργράφημα $G_i = (V(G_i), E(G_i))$. Θα είναι $V(G_i) = V(K_i) \times [3]$, δηλαδή διαισθητικά κάθε κόμβος αντιστοιχεί σε κάποιο όρο της ϕ_i και σε κάποιο λεκτικό από αυτόν τον όρο. Στο $E(G_i)$ θα ανήκει κάθε υποσύνολο του $V(G_i)$, πληθάριθμου d, τέτοιο ώστε οποιαδήποτε δύο στοιχεία/κόμβοι του, να μην αντιστοιχούν στον ίδιο όρο και να μην αντιστοιχούν σε συμπληρωματικά λεκτικά. Δηλαδή αν με $\phi_i(u, l)$ συμβολίζουμε το l-οστό λεκτικό του u-οστού όρου της ϕ_i, θα είναι:

   $$E(G_i) = \{e : e \subseteq V(G_i),\ |e| = d,\ \text{έτσι ώστε } \forall v, v' \in e,$$
   $$\text{με } v = (u, l),\ v' = (u', l'),\ \text{να είναι } u \neq u' \text{ και } \phi_i(u, l) \neq \overline{\phi_i(u', l')}\}$$

   Η κατασκευή του G_i από το ϕ_i, δηλαδή, ουσιαστικά ακολουθεί την κλασική αναγωγή από το $3SAT$ στο 2-CLIQUE.

3. Κατασκεύασε το $G = (V(G), E(G))$, με $V(G) = \bigcup_{i \in [t]} V(G_i) \subseteq V(P) \times [3]$ και $E(G) = \bigcup_{i \in [t]} E(G_i)$.

4. Θέσε το (G, s) ως το προκύπτον στιγμιότυπο για το d-CLIQUE.

Επειδή $V(G) \subseteq V(P) \times [3]$, θα είναι $|V(G)| \leq 3 \cdot |V(P)| = O(s \cdot max\{s, t^{1/d+o(1)}\})$, όπως ακριβώς ισχυριστήκαμε (με την τελευταία ισότητα να προκύπτει από το Λήμμα 1).

Για το ότι η αναγωγή είναι πράγματι πολυωνυμική, παρατηρήστε τα εξής:

1. Για το βήμα 1, το ότι η κατασκευή αυτή είναι πολυωνυμική ως προς τα s, t το παίρνουμε από το Λήμμα 1, άρα θα είναι και πολυωνυμική ως προς το μέγεθος της εισόδου που είναι $O(s \cdot t)$.

2. Για το βήμα 2, για την κατασκευή κάθε G_i, θέλουμε $|V(K_i) \times [3]| = 3s = O(s)$, άρα πολυωνυμικά πολλούς ως προς την είσοδο κόμβους και για την κατασκευή των ακμών έχουμε το εξής: $\binom{3s}{d}$ πιθανές ακμές, όπου για κάθε μία πρέπει να ελέγξουμε για κάθε ζεύγος στοιχείων της, τα οποία είναι $\binom{d}{2}$ στο πλήθος, να μην αντιστοιχούν στον ίδιο όρο της ϕ_i και να μην αντιστοιχούν σε συμπληρωματικά λεκτικά. Η πρώτη από αυτές τις ιδιότητες ελέγχεται σε σταθερό χρόνο, απλά συγκρίνοντας την πρώτη συντεταγμένη των δύο κόμβων, ενώ η δεύτερη απλά διατρέχοντας την ϕ_i και συγκρίνοντας τα λεκτικά που αντιστοιχούν οι κόμβοι. Αυτό γίνεται σε χρόνο $O(s)$, αφού τόσο είναι το μέγεθος κάθε ϕ_i. Άρα συνολικά για την κατασκευή του $E(G_i)$, θέλουμε χρόνο: $O(\binom{3s}{d} \cdot \binom{d}{2} \cdot s) = O((3s)^d \cdot d^2 \cdot s) = O(s^{d+1})$, αφού θεωρούμε το d σταθερό.

3. Για το βήμα 3, λοιπόν, όπου ουσιαστικά κάνουμε το βήμα 2 τόσες φορές όσα είναι τα G_i, δηλαδή t φορές, θέλουμε χρόνο $O(t \cdot s^{d+1})$, ο οποίος είναι πολυωνυμικός προφανώς ως προς τα s, t και ως προς το μήκος της εισόδου.

Άρα η αναγωγή είναι πράγματι πολυωνυμικού κόστους.

Μένει η ορθότητα: $(\phi_1, \phi_2, ..., \phi_t) \in OR(3SAT) \Leftrightarrow (G, s) \in d$-CLIQUE

$(\Rightarrow)$: Έστω ότι $(\phi_1, \phi_2, ..., \phi_t) \in OR(3SAT)$. Τότε εξ ορισμού, $\exists i \in [t]$ ώστε $\phi_i \in 3SAT$. Δηλαδή η ϕ_i έχει κάποια ικανοποιούσα ανάθεση T, η οποία θα καθιστά προφανώς τουλάχιστον ένα από τα 3 λεκτικά κάθε όρου αληθές. Θεώρησε λοιπόν ένα ακριβώς αληθές λεκτικό από κάθε όρο της ϕ_i, συνολικά δηλαδή s λεκτικά, και έστω $V \subseteq V(G_i)$, το υποσύνολο κόμβων του G_i, στο οποίο αντιστοιχούν τα επιλεγμένα λεκτικά. Ισχυριζόμαστε ότι το V είναι μια κλίκα μεγέθους s του G_i. Πράγματι, έστω $e \subseteq V, |e| = d$. Οποιοιδήποτε 2 κόμβοι της e, αντιστοιχούν σε διαφορετικούς όρους εκ κατασκευής του V και επίσης δεν αντιστοιχούν σε συμπληρωματικά λεκτικά, διότι η T είναι μια έγκυρη ανάθεση τιμών αλήθειας, που δίνει και στα δύο λεκτικά που αντιστοιχούν οι κόμβοι την τιμή αληθές. Συνεπώς $\forall e \subseteq V, |e| = d$ έχουμε $e \in E(G_i)$, συνεπώς V κλίκα μεγέθους s του G_i και άρα κλίκα μεγέθους s και του G, άρα $(G, s) \in d$-CLIQUE.

$(\Leftarrow)$: Έστω K κλίκα μεγέθους s του G, δηλαδή $(G, s) \in d$-CLIQUE. Θεωρούμε την προβολή K' του K πάνω στο P. Όπου η προβολή ορίζεται με τον προφανή τρόπο ως εξής: Για $v = (u, i) \in V(G) \subseteq V(P) \times [3]$, έχουμε $Proj_P(v) = u$. Δηλαδή ουσιαστικά θα είναι : $K' = \{Proj_P(v) : v \in K\}$. Ισχυριζόμαστε ότι K' κλίκα μεγέθους s του P. Για να το δούμε αυτό κάνουμε 2 παρατηρήσεις. Πρώτον, αν $u, v \in K$, με $u \neq v$, τότε $Proj_P(u) \neq Proj_P(v)$. Δηλαδή το K' αποτελείται από s διακριτούς κόμβους του P. Και αυτό διότι επειδή ακριβώς K κλίκα του G, κάθε υποσύνολο του $V(K)$ μεγέθους d θα είναι ακμή του G, συνεπώς για ένα τέτοιο υποσύνολο e που περιέχει τα u, v (υπάρχει τέτοιο αφού $d \geq 2$) θα ισχύει $e \in E(G) \Rightarrow e \in E(G_i)$ για κάποιο $i \in [t]$. Όμως, εκ κατασκευής των G_i, $e \in E(G_i)$ αν και μόνο αν $\forall x, y \in e$, με $x \neq y$, τα x, y δεν αντιστοιχούν αφενός σε συμπληρωματικά λεκτικά και δεν αντιστοιχούν αφετέρου στον ίδιο όρο, δηλαδή έχουν διαφορετική πρώτη συντεταγμένη, δηλαδή $Proj_P(x) \neq Proj_P(y)$. Συνεπώς παίρνουμε ότι πράγματι $Proj_P(u) \neq Proj_P(v)$. Δεύτερον, $\forall e' \subseteq K', |e'| = d$, έχουμε $e' \in E(P)$. Για να το δούμε αυτό, έστω ένα τέτοιο e'. Από την πρώτη παρατήρηση, υπάρχει μοναδικό

$e \subseteq K, |e| = d$, ώστε η προβολή της e στο P να είναι η e'. Επειδή όμως K κλίκα του G θα είναι $e \in E(G) \Rightarrow e \in E(G_i)$ για κάποιο $i \in [t] \Rightarrow$ οποιοιδήποτε δύο κόμβοι της e έχουν διαφορετική πρώτη συντεταγμένη $\Rightarrow$ e' είναι ένα σύνολο d διακεκριμένων κορυφών του $V(K_i) \Rightarrow e' \in E(P)$, αφού K_i κλίκα του P από Λήμμα 1.

Από την τελευταία αυτή παρατήρηση έχουμε ότι πράγματι K' κλίκα μεγέθους s του P. Από Λήμμα 1 πάλι, από την δεύτερη ιδιότητα, παίρνουμε ότι $K' = K_i$ για κάποιο $i \in [t]$.

Από αυτό έχουμε αμέσως $V(K) \subseteq V(K_i) \times [3] = V(G_i)$. Θα δείξουμε τώρα ότι και $E(K) \subseteq E(G_i)$, όπου $E(K)$ όλα τα υποσύνολα του K μεγέθους ακριβώς d. Έστω $e \in E(K) \subseteq E(G)$, άρα $e \in E(G_j)$ για κάποιο $j \in [t]$. Αν $j \neq i$ τότε επειδή e σύνολο d κορυφών και του G_i και του G_j, θα είναι $|V(G_i) \cap V(G_j)| \geq d$ και συνεπώς παίρνοντας τις προβολές στην πρώτη διάσταση θα είναι $|V(K_i) \cap V(K_j)| \geq d$, κάτι που υποδηλώνει ότι υπάρχει ακμή του $E(P)$ που ανήκει και στο $E(K_i)$ και στο $E(K_j)$, κάτι που είναι άτοπο λόγω της ιδιότητας 2 του Λήμματος 1. Άρα θα είναι $j = i$, και άρα παίρνουμε ότι $E(K) \subseteq E(G_i)$. Οπότε λοιπόν από το ότι K κλίκα, $V(K) \subseteq V(K_i)$ και $E(K) \subseteq E(G_i)$, παίρνουμε προφανώς ότι K κλίκα μεγέθους s του G_i. Η K θα έχει ακριβώς μια κορυφή από κάθε τριάδα κορυφών του G_i με ίδια πρώτη συντεταγμένη, διότι $|K| = s$, και δεν γίνεται να έχει δύο κορυφές με ίδια πρώτη συντεταγμένη, διότι τότε αυτές οι δύο κορυφές δεν θα άνηκαν σε καμία ακμή, πόσο μάλλον στην κλίκα K. Για τον ίδιο λόγο δεν γίνεται δύο κορυφές της K να αντιστοιχούν σε συμπληρωματικά λεκτικά. Άρα η K θα έχει ακριβώς ένα λεκτικό από κάθε όρο της ϕ_i, και τα λεκτικά αυτά ανά δύο δεν αντιστοιχούν σε συμπληρωματικά λεκτικά. Αυτό υπονοεί προφανώς μια ανάθεση τιμών αλήθειας που καθιστά τα λεκτικά αυτά αληθή, άρα και την ϕ_i ικανοποιήσιμη $\Rightarrow \phi_i \in 3SAT \Rightarrow (\phi_1, \phi_2, ..., \phi_t) \in OR(3SAT)$. ■

Έχοντας παρουσιάσει την αναγωγή, χρησιμοποιώντας το πρωτόκολλο τάξης $O(n^c)$ για το d-CLIQUE με $n = O(s \cdot max\{s, t^{1/d+o(1)}\})$ κόμβους, παίρνουμε, για αρκετά μεγάλο πολυώνυμο t ως προς s, ένα πρωτόκολλο τάξης $O(t \cdot \log t)$ για το $OR(3SAT)$:

Έστω $t = s^k$, για k που θα επιλέξουμε εμείς. Και $n = s \cdot max\{s, t^{1/d+o(1)}\}$ για ευκολία.

Αν $max\{s, t^{1/d+o(1)}\} = s$ έχουμε: $n^c = s^{2c} = t^{2c/k} = O(t) = O(t \cdot \log t)$ για $k \geq 2c$.

Αν $max\{s, t^{1/d+o(1)}\} = t^{1/d+o(1)}$ έχουμε: $n^c = (s \cdot t^{1/d+o(1)})^c = t^{c/k} \cdot t^{c \cdot (1/d+o(1))} = t^{\frac{c}{k}+\frac{c}{d}+o(1) \cdot c} = O(t) = O(t \cdot \log t)$ για $k \geq \frac{c}{1-\frac{c}{d}-o(1) \cdot c}$

Άρα αρκεί $k \geq max(2c, \frac{c}{1-\frac{c}{d}-o(1) \cdot c})$ και έχουμε το ζητούμενο.

Εφαρμόζουμε τώρα το Λήμμα 2, για $L = 3SAT$ και $t(s) = s^{max(2c, \frac{c}{1-\frac{c}{d}-o(1) \cdot c})}$ και παίρνουμε $3SAT \in coNP/poly$. Από το Λήμμα 3 τότε, $\overline{3SAT} \in co\text{-}(coNP/poly) = NP/poly$.

Και επειδή $\overline{3SAT}$ είναι $coNP$ πλήρες, παίρνουμε $coNP \subseteq NP/poly$, δηλαδή $\Pi_1 \subseteq \Sigma_1/poly$. Από Λήμμα 5, παίρνουμε ότι $\Pi_1/poly = \Sigma_1/poly$ και έπειτα από Λήμμα 7 παίρνουμε ότι $\Sigma_3 = \Pi_3$ και άρα η πολυωνυμική ιεραρχία καταρρέει στο τρίτο της επίπεδο, κάτι άτοπο, βάσει της αρχικής μας υπόθεσης ότι η πολυωνυμική ιεραρχία δεν καταρρέει. Και έτσι ολοκληρώνεται η απόδειξη του Θεωρήματος 1. ■

3.3 Απόδειξη Θεωρήματος 2

Η απόδειξη προέρχεται από το [5].

Το Θεώρημα 2, το αντίστοιχο του Θεωρήματος 1, αλλά για το d-SAT παραμετροποιημένο ως προς το πλήθος των λογικών μεταβλητών, προκύπτει μέσω της ύπαρξης πολυωνυμικής αναγωγής d-VERTEX COVER $\leq_m^p$ d-SAT για $d \geq 3$, η οποία αυξάνει το μέγεθος της παραμέτρου κατά έναν σταθερό παράγοντα μόνο. Η αναγωγή αυτή είναι η τετριμμένη, αντιστοιχίζει απλά ένα (G, k), όπου $k \in \mathbb{N}$ και G ένα d-ομοιόμορφο υπεργράφημα σε n κόμβους, η παράμετρος, σε μία d-CNF z με $O(n)$ μεταβλητές, η νέα παράμετρος. Επιγραμματικά, απλά εισάγουμε μια δυαδική μεταβλητή x_i για κάθε κόμβο του γραφήματος, η οποία δηλώνει αν ο i-οστός κόμβος ανήκει ή όχι στο κάλυμμα κορυφών. Έπειτα ορίζουμε την d-CNF $\phi = \bigwedge_{e \in E(G)} \bigvee_{i \in e} x_i$, η οποία επιβάλλει να έχουμε όντως ένα κάλυμμα κορυφών και την d-CNF ψ, η οποία υλοποιεί ένα boolean κύκλωμα με $O(n)$ επιπλέον μεταβλητές, που απλά ελέγχει ότι $\sum_{i \in [n]} x_i \leq k$. Τέλος θέτουμε $z = \phi \wedge \psi$.

Έστω τώρα προς άτοπο ότι δεν ισχύει το Θεώρημα 2, και υπάρχει πρωτόκολλο κόστους $O(n^c),\ c < d$, για το d-SAT. Μέσω της παραπάνω πολυωνυμικής αναγωγής, παίρνουμε ένα πρωτόκολλο κόστους $O((k \cdot n)^c) = O(n^c), c < d$, για το d-VERTEX COVER, όπου k ο σταθερός παράγοντας που κρύβεται πίσω από την $O(n)$ αύξηση των μεταβλητών λόγω της αναγωγής. Αυτό βέβαια αντιφάσει το Θεώρημα 1. ■

4. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΣΥΝΕΠΕΙΕΣ-ΕΠΙΠΛΕΟΝ ΚΑΤΩ ΦΡΑΓΜΑΤΑ

4.1 Πόρισμα Θεωρήματος 2

Το πόρισμα και η απόδειξη προέρχονται από το [5].

Πόρισμα 2.1. *Έστω $d \geq 3$. Δεδομένου ότι δεν ισχύει ότι $coNP \subseteq NP/poly$, δεν υπάρχει πολυωνυμική αναγωγή από το d-SAT σε οποιοδήποτε πρόβλημα, το οποίο έχει πρωτόκολλο με $O(n^b)$ ερωτήσεις, και κάθε ερώτηση να έχει μήκος (bitlength) $O(n^c)$, με $b + c < d$.*

Απόδειξη. Έστω ότι υπάρχει γλώσσα $L \subseteq \{0,1\}^*$, η οποία να έχει πρωτόκολλο με $O(n^b)$ ερωτήσεις, μήκους $O(n^c)$ η καθεμία, με $b + c < d$, και έστω ότι d-SAT $\leq_m^p L$. Τότε, μέσω της αναγωγής, παίρνουμε ένα πρωτόκολλο για το d-SAT κόστους: $O(n^b \cdot n^c) = O(n^{b+c}) = O(n^k),\ k < d$, το οποίο βέβαια αντιφάσκει το Θεώρημα 2. ■

4.2 Αραιοποίηση (Sparsification)

Αραιές (sparse) ονομάζονται οι d-CNF φόρμουλες n μεταβλητών, οι οποίες έχουν σχετικά λίγους όρους, σε σχέση με τους $\binom{n}{d} \cdot 2^d$ που είναι το μέγιστο. Θα θέλαμε δηλαδή να ανάγουμε σε πολυωνυμικό χρόνο, οποιοδήποτε στιγμιότυπο του d-SAT πάνω σε n μεταβλητές, σε ένα ισοδύναμο στιγμιότυπο πάλι του d-SAT, πάλι πάνω σε n μεταβλητές, αλλά με λιγότερους όρους. Αυτή η διαδικασία, λέγεται αραιοποίηση (sparsification) ως προς πολυωνυμικές αναγωγές, επειδή αραιώνουμε το πλήθος των όρων, μέσω μιας πολυωνυμικής αναγωγής. Το ερώτημα είναι, πόσους λίγους όρους μπορεί να έχει το ισοδύναμο ανηγμένο στιγμιότυπο. Μια τετριμμένη, απλή αραιοποίηση, θα ήταν απλώς η αφαίρεση διπλότυπων όρων. Αυτή η αραιοποίηση, δεδομένου ότι υπάρχουν $\binom{n}{d} \cdot 2^d = O(n^d)$ διακεκριμένοι όροι για μια d-CNF πάνω σε n μεταβλητές, πετυχαίνει $O(n^d)$ όρους. Υπάρχει καλύτερη αραιοποίηση για το d-SAT, που να πετυχαίνει δηλαδή $O(n^c),\ c < d$ όρους; Η απάντηση είναι αρνητική, διότι αν υπήρχε πολυωνυμική αναγωγή, η οποία μετέτρεπε οποιοδήποτε στιγμιότυπο του d-SAT πάνω σε n μεταβλητές, σε ένα ισοδύναμο με $O(n^c),\ c < d$ όρους, τότε συνδυάζοντας αυτήν την αναγωγή και το τετριμμένο πρωτόκολλο για το d-SAT, θα παίρναμε ένα πρωτόκολλο για το d-SAT, παραμετροποιημένο ως προς το πλήθος των μεταβλητών, κόστους $O(n^c),\ c < d$, κάτι που αντιφάσκει το Θεώρημα 2. Άρα το d-SAT, δεν επιτρέπει μη τετριμμένη αραιοποίηση, η τετριμμένη αραιοποίηση είναι η βέλτιστη.

4.3 Πυρηνοποίηση (Kernelization)

Κάτω φράγματα στους πυρήνες για τα d-SAT και d-VERTEX COVER

1. Για το d-SAT παραμετροποιημένο ως προς το πλήθος των μεταβλητών n, η τετριμμένη αναγωγή που απλά αφαιρεί διπλότυπους όρους, οδηγεί σε ένα στιγμιότυπο με $O(n^d)$ όρους, καθένας με d λεκτικά, άρα οδηγεί σε πυρήνα μεγέθους $O(n^d \cdot d \cdot logn) = O(n^d \cdot logn)$. Το ερώτημα τώρα είναι αν μπορούμε για οποιοδήποτε στιγμιότυπο, να μειώσουμε το μέγεθος του πυρήνα σε $O(n^{d-\epsilon}),\ \epsilon > 0$. Και η απάντηση είναι αρνητική, διότι τότε συνδυάζοντας την αναγωγή της πυρηνοποίησης, μαζί με το τετριμμένο πρωτόκολλο για το d-SAT εφαρμοσμένο στον πυρήνα, θα παίρναμε πρωτόκολλο τάξης $O(n^{d-\epsilon}),\ \epsilon > 0$ για το d-SAT, κάτι που αντιφάσκει το Θεώρημα 2. Άρα η τετριμμένη πυρηνοποίηση είναι βέλτιστη.

2. Όμοια για το d-VERTEX COVER παραμετροποιημένο ως προς το πλήθος των κόμβων n, η τετριμμένη ταυτοτική αναγωγή οδηγεί σε ένα στιγμιότυπο με $O(n^d)$ ακμές και άρα μέγεθος πυρήνα $O(n^d \cdot d \cdot logn + logn) = O(n^d \cdot logn)$. Και για τους ίδιους λόγους με πριν, δεν υπάρχει πυρηνοποίηση που οδηγεί σε μέγεθος πυρήνα $O(n^{d-\epsilon}),\ \epsilon > 0$, διότι τότε θα παίρναμε πρωτόκολλο τάξης $O(n^{d-\epsilon}),\ \epsilon > 0$ για το d-VERTEX COVER κάτι που αντιφάσκει το Θεώρημα 1. Άρα η τετριμμένη πυρηνοποίηση είναι η βέλτιστη.

3. Ιδιαίτερο ενδιαφέρον έχει η περίπτωση του 2-VERTEX COVER, δηλαδή το κάλυμμα κορυφών στα απλά γραφήματα, παραμετροποιημένο ως προς το μέγεθος k του καλύμματος κορυφών όμως τώρα. Είναι γνωστοί πυρήνες μεγέθους $O(k^2)$, όπως παρουσιάζεται στο Παράρτημα Β. Το ερώτημα είναι λοιπόν, αν μπορούμε να μειώσουμε ακόμα παραπάνω το μέγεθος του πυρήνα, σε κάτι μεγέθους $O(k^{2-\epsilon}),\ \epsilon > 0$. Αν μπορούσαμε να κάνουμε κάτι τέτοιο, για οποιοδήποτε στιγμιότυπο, τότε επειδή $k \leq n$, όπου n το πλήθος κορυφών του γραφήματος, για την περίπτωση $d = 2$ του d-VERTEX COVER με παράμετρο το πλήθος κορυφών n, θα παίρναμε πυρήνες μεγέθους $O(k^{2-\epsilon}) = O(n^{2-\epsilon})$, κάτι που αντιφάσκει αυτά που είπαμε στην προηγούμενη παράγραφο, άτοπο. Άρα οι $O(k^2)$ μεγέθους πυρήνες είναι βέλτιστοι.

4.4 Συμπίεση (Lossy Compression)

Η ιδέα της συμπίεσης είναι παρόμοια με αυτή της πυρηνοποίησης. Θέλουμε να ανάγουμε το αρχικό στιγμιότυπο ενός προβλήματος, σε ένα ισοδύναμο μικρότερου μεγέθους, το οποίο να λύνεται πιο αποδοτικά. Η μόνη διαφορά εδώ είναι ότι η $\leq_m^p$ αναγωγή μπορεί να παράγει ένα ισοδύναμο στιγμιότυπο οποιουδήποτε προβλήματος/γλώσσας, όχι απαραίτητα του αρχικού προβλήματος. Το μόνο που μας ενδιαφέρει είναι να διατηρείται η ισοδυναμία, δηλαδή η ναι/όχι απάντηση. Για το d-SAT με παράμετρο το πλήθος των μεταβλητών n, το χαρακτηριστικό bitstream $\{0,1\}^{O(n^d)}$, που παράγει το τετριμμένο πρωτόκολλο, που δηλώνει κατά πόσο ανήκει ή όχι ένας όρος στο δεδομένο στιγμιότυπο, αποτελεί ένα είδος συμπίεσης του αρχικού προβλήματος d-SAT, σε μια νέα διαφορετική γλώσσα. Επίσης η συμπίεση αυτή πετυχαίνει μέγεθος συμπιεσμένου στιγμιότυπου $O(n^d)$. Μπορούμε να κάνουμε καλύτερη συμπίεση; Και η απάντηση εδώ είναι προφανώς αρνητική πάλι, διότι τότε θα είχαμε μια συμπίεση για το d-SAT με μέγεθος συμπιεσμένου στιγμιότυπου $O(n^{d-\epsilon}),\ \epsilon > 0$, άρα συνδυάζοντας την αναγωγή της συμπίεσης και το τετριμμένο πρωτόκολλο για το d-SAT θα παίρναμε πρωτόκολλο κόστους $O(n^{d-\epsilon}),\ \epsilon > 0$ για το d-SAT, που αντιφάσκει το Θεώρημα 2. Τα ανάλογα ισχύουν και για το d-VERTEX COVER με παράμετρο το πλήθος κόμβων n. Και εδώ με παρόμοια επιχειρηματολογία έχουμε ότι δεν μπορούμε να πετύχουμε συμπίεση μεγέθους $O(n^{d-\epsilon}),\ \epsilon > 0$.

4.5 Συνθεσιμότητα (Compositionality)

Για να αποδείξουμε τα σφιχτά κάτω φράγματα των κεντρικών θεωρημάτων για τα NP-πλήρη προβλήματα d-SAT και d-VERTEX COVER, χρησιμοποιήσαμε μια γνωστή τεχνική στην Παραμετρική Πολυπλοκότητα, αυτήν της Συνθεσιμότητας (Compositionality). Αυτή η τεχνική αποτελεί το κατεξοχήν εργαλείο για την απόδειξη αρνητικών αποτελεσμάτων για την ύπαρξη πυρήνα πολυωνυμικού μεγέθους για ένα πρόβλημα, ή για την απόδειξη σφιχτών κάτω ορίων στο μέγεθος του πυρήνα που επιδέχεται ένα πρόβλημα. Αρχίζουμε παρουσιάζοντας τη διαίσθηση πίσω από την μεθοδολογία πριν τους τυπικούς ορισμούς.

Η ανάλυση που ακολουθεί, μαζί με τα θεωρήματα και τους ορισμούς, προέρχονται από το [7].

OR-Διύλιση (OR-Distillation)

Έστω ένα γνωστό NP-πλήρες πρόβλημα, για παράδειγμα το Πρόβλημα Μέγιστου Μονοπατιού, όπου δεδομένου ενός γραφήματος G και ενός φυσικού k, αναζητούμε αν υπάρχει ένα απλό μονοπάτι k κορυφών στο G. Το συγκεκριμένο πρόβλημα ανήκει στην κλάση FPT και μάλιστα επιδέχεται εκθετικού μεγέθους πυρήνες. Το ερώτημα που τίθεται είναι εάν επιδέχεται πυρήνες πολυωνυμικού μεγέθους. Έστω ότι υπάρχει πολυωνυμικού μεγέθους πυρήνας για το πρόβλημα, δηλαδή πολυωνυμικός αλγόριθμος που ανάγει το αρχικό στιγμιότυπο (G, k) σε ένα ισοδύναμο στιγμιότυπο του προβλήματος μεγέθους k^c. Παράγουμε ένα νέο στιγμιότυπο του προβλήματος, παίρνοντας την ξένη ένωση μικρότερων στιγμιότυπων του προβλήματος. Δηλαδή δεδομένων $(G_1, k), (G_2, k), ..., (G_t, k)$, με $|V(G_i)| = n,\ k \leq n$, θέτουμε το G ως την ξένη ένωση των επιμέρους $G_i,\ i \in [t]$. Προφανώς θα ισχύει ότι (G, k) είναι ένα καταφατικό στιγμιότυπο του προβλήματος αν και μόνο αν (G_i, k) είναι ένα καταφατικό στιγμιότυπο του προβλήματος για τουλάχιστον ένα $i \in [t]$. Ο αλγόριθμος της πυρηνοποίησης εφαρμοσμένος πάνω στο (G, k) θα επιστρέφει σε χρόνο πολυωνυμικό, ένα νέο ισοδύναμο στιγμιότυπο (G', k') του προβλήματος, για το οποίο θα είναι $|(G', k')| \leq k^c$, δηλαδή $|V(G')| \leq k^c \leq n^c$, το οποίο n^c μπορεί να είναι αυθαίρετα μικρότερο από το t, το πλήθος δηλαδή των στιγμιοτύπων G_i. Αυτό σημαίνει, διαισθητικά, ότι ο αλγόριθμος της πυρηνοποίησης, με κάποιο τρόπο, πρέπει να μπορεί να φιλτράρει, να μπορεί να λύσει γρήγορα κάποια από τα στιγμιότυπα (G_i, k), ώστε να είναι σε θέση να επιστρέψει σε πολυωνυμικό χρόνο έναν μικρό πυρήνα. Αυτό βέβαια μάλλον είναι δύσκολο να συμβεί, δεδομένου ότι το Πρόβλημα του Μέγιστου Μονοπατιού είναι NP-πλήρες, και άρα η διαίσθησή μας, μας υπονοεί ότι τέτοιος πολυωνυμικός πυρήνας μάλλον δεν υπάρχει.

Πιο τυπικά:

OR-Διύλιση: Έστω $L, R \subseteq \{0,1\}^*$ γλώσσες και $t : \mathbb{N} \to \mathbb{N}\backslash\{0\}$ συνάρτηση. Τότε ένας αλγόριθμος OR-Διύλισης από την L στην R είναι ένας πολυωνυμικός αλγόριθμος όπου για κάθε n, δεδομένων $t(n)$ στιγμιότυπων $x_1, x_2, ..., x_{t(n)}$ της L, με $|x_i| = n$, έχει σαν έξοδο ένα στιγμιότυπο y της R, με $|y| \leq t(n) \cdot logn$, ώστε $y \in R \Leftrightarrow x_i \in L$ για κάποιο $i \in [t(n)]$.

Το θεώρημα που καθιστά χρήσιμη την έννοια της OR-Διύλισης είναι το εξής:

Θεώρημα 3. *Αν υπάρχει ένας αλγόριθμος OR-Διύλισης από μία $L \subseteq \{0,1\}^*$ σε μία $R \subseteq \{0,1\}^*$, για κάποια πολυωνυμική συνάρτηση t, τότε $\overline{L} \in NP/poly$. Μάλιστα αν η L είναι NP-δύσκολη, έχουμε $coNP \subseteq NP/poly$.*

Συνεπώς, η ύπαρξη ενός πολυωνυμικού αλγόριθμου OR-Διύλισης για οποιοδήποτε NP-δύσκολο πρόβλημα, υπονοεί ότι $coNP \subseteq NP/poly$, και συνεπώς όπως έχουμε δει, ότι η πολυωνυμική ιεραρχία καταρρέει.

Μια μεθοδολογία λοιπόν, για την απόδειξη μη ύπαρξης πολυωνυμικού πυρήνα για ένα παραμετροποιημένο πρόβλημα, είναι να δείξουμε ότι αν μπορούσαμε να έχουμε έναν τέτοιο αλγόριθμο πυρηνοποίησης, θα μπορούσαμε να βρούμε έναν αλγόριθμο OR-Διύλισης για ένα NP-δύσκολο πρόβλημα.

Θεώρημα 4. *Το Πρόβλημα Μέγιστου Μονοπατιού, με παράμετρο το μήκος του μονοπατιού k, δεν επιδέχεται πολυωνυμικό πυρήνα, εκτός αν $coNP \subseteq NP/poly$.*

Απόδειξη. Έστω ότι δεν ισχύει ότι $coNP \subseteq NP/poly$ και έστω ότι υπάρχει πολυωνυμικός πυρήνας για το Πρόβλημα Μέγιστου Μονοπατιού, δηλαδή πολυωνυμικός αλγόριθμος πυρηνοποίησης K, που σε είσοδο (G, k) στιγμιότυπο του προβλήματος, παράγει ένα ισοδύναμο στιγμιότυπο μεγέθους το πολύ k^c, για σταθερά c. Θέτουμε ως L τη γλώσσα που αντιστοιχεί στο Πρόβλημα του Χαμιλτονιανού Μονοπατιού, ένα πρόβλημα που είναι ως γνωστόν NP-δύσκολο, και ως R τη γλώσσα που αντιστοιχεί στο Πρόβλημα Μέγιστου Μονοπατιού. Έστω $t(n) = n^c$. Ο εξής αλγόριθμος A, αποτελεί έναν πολυωνυμικό αλγόριθμο OR-Διύλισης από την L στην R. Ο αλγόριθμος, για οποιοδήποτε n, έχοντας ως είσοδο $x_1, ..., x_{t(n)}$ στιγμιότυπα της L, που αντιστοιχούν σε γραφήματα $G_1, ..., G_{t(n)}$, που έχουν χωρίς βλάβη της γενικότητας όλα ακριβώς $p \leq n$ κόμβους, φτιάχνει το G ως την ξένη ένωση των G_i. Έπειτα τρέχει τον K πάνω στο (G, p), στιγμιότυπο της R, για να πάρει ένα ισοδύναμο στιγμιότυπο (G', k') το οποίο θέτει και ως y. Προφανώς θα είναι $|y| \leq p^c \leq n^c \leq t(n) \cdot logn$.

Για να αποδείξουμε ότι ο A πράγματι αποτελεί πολυωνυμικό αλγόριθμο OR-Διύλισης από την L στην R, αρκεί να δείξουμε πρώτον ότι είναι πολυωνυμικός κάτι που είναι προφανές αφού τόσο η κατασκευή του G όσο και η εκτέλεση του K είναι πολυωνυμικές, και δεύτερον ότι $y \in R \Leftrightarrow x_i \in L$ για κάποιο $i \in [t(n)]$. Αυτό όμως θα ισχύει καθώς $y \in R$ αν και μόνο αν $(G, p) \in R$ από ορισμό του αλγόριθμου πυρηνοποίησης K και $(G, p) \in R$ αν και μόνο αν $x_i \in L$ για κάποιο $i \in [t(n)]$, αφού το G εκ κατασκευής έχει μέγιστο μονοπάτι μήκους τουλάχιστον p αν και μόνο αν κάποιο G_i έχει Χαμιλτονιανό μονοπάτι.

Συνεπώς, αφού υπάρχει ένας πολυωνυμικός αλγόριθμος OR-Διύλισης από ένα NP-δύσκολο πρόβλημα (Πρόβλημα Χαμιλτονιανού Μονοπατιού) στο Πρόβλημα Μέγιστου Μονοπατιού, από Θεώρημα 3, παίρνουμε $coNP \subseteq NP/poly$, άτοπο. ■

Διασταυρούμενη OR-Σύνθεση (OR-Cross-Composition)

Ένα άλλο εργαλείο παρόμοιο με αυτό που αναπτύξαμε στην προηγούμενη ενότητα είναι αυτό της διασταυρούμενης OR-σύνθεσης. Ακολουθούν οι ορισμοί.

Πολυωνυμική Σχέση Ισοδυναμίας είναι μια σχέση ισοδυναμίας R ορισμένη πάνω στο Σ^* για την οποία ισχύουν τα εξής:

- Υπάρχει αλγόριθμος, που δεδομένου $x, y \in \Sigma^*$, αποφασίζει σε χρόνο πολυωνυμικό ως προς $|x| + |y|$, αν τα x, y είναι ισοδύναμα μεταξύ τους ως προς την R.
- Για οποιοδήποτε πεπερασμένο $S \subseteq \Sigma^*$, η R διαμερίζει τα στοιχεία του S το πολύ σε $(max_{x \in S}|x|)^{O(1)}$ κλάσεις ισοδυναμίας.

Διασταυρούμενη OR-Σύνθεση. Δεδομένων μιας γλώσσας $L \subseteq \{0, 1\}^*$ και μιας παραμετροποιημένης γλώσσας $Q \subseteq \{0, 1\}^* \times \mathbb{N}$, η L έχει μια διασταυρούμενη OR-σύνθεση στην Q αν υπάρχει μια πολυωνυμική σχέση ισοδυναμίας R και ένας αλγόριθμος A με τις εξής ιδιότητες.

- Ο αλγόριθμος A παίρνει ως είσοδο t στιγμιότυπα της L, $x_1, x_2, ..., x_t$, όλα ισοδύναμα μεταξύ τους ως προς την R.
- Τρέχει σε χρόνο πολυωνυμικό ως προς το $\sum_{i=1}^{t} |x_i|$.
- Έχει σαν έξοδο ένα στιγμιότυπο $(y, k) \in \{0, 1\}^* \times \mathbb{N}$ της Q τέτοιο ώστε:

- $k \leq p(max_{i=1}^{t}|x_i| + logt)$ για κάποιο πολυώνυμο p.
- $(y,k) \in Q \Leftrightarrow \exists i \in [t]$ με $x_i \in L$.

Η βασική διαφορά είναι ότι πλέον η παράμετρος του ανηγμένου στιγμιοτύπου φράσσεται όχι από ένα πολυώνυμο της παραμέτρου του αρχικού στιγμιότυπου, αλλά από ένα πολυώνυμο που εξαρτάται από το μέγιστο μέγεθος στιγμιότυπου της εισόδου καθώς και από το λογάριθμο του πλήθους των στιγμιοτύπων στην είσοδο. Επίσης δεν μας ενδιαφέρει τόσο να είναι μικρό το μέγεθος του ανηγμένου στιγμιότυπου, όπως στην OR-Διύλιση, αλλά να είναι μικρό μόνο το μέγεθος της παραμέτρου του ανηγμένου στιγμιότυπου.

Το θεώρημα που καθιστά χρήσιμη τη διασταυρούμενη OR-σύνθεση είναι το εξής:

Θεώρημα 5. *Έστω $L \subseteq \{0,1\}^*$ μια NP-δύσκολη γλώσσα. Εάν υπάρχει διασταυρούμενη OR-σύνθεση της L σε κάποια παραμετροποιημένη γλώσσα $Q \subseteq \{0,1\}^* \times \mathbb{N}$, η οποία επιδέχεται και πολυωνυμικό πυρήνα (ή γενικότερα πολυωνυμική συμπίεση), τότε θα είναι $coNP \subseteq NP/poly$.*

Απόδειξη. Έστω ότι υπάρχει πολυωνυμική συμπίεση της Q σε κάποια γλώσσα $R \subseteq \{0,1\}^*$. Θα δείξουμε ότι για κάποια πολυωνυμική συνάρτηση t, υπάρχει αλγόριθμος OR-Διύλισης από την L στην $OR(R)$. Έχοντας αυτό, σε συνδυασμό με το ότι η L είναι NP-δύσκολη, παίρνουμε από το Θεώρημα 3, ότι $coNP \subseteq NP/poly$.

Προς αυτήν την κατεύθυνση κάνουμε τις εξής παρατηρήσεις από τους ορισμούς:

1. Από το ότι υπάρχει διασταυρούμενη OR-σύνθεση της L στην Q, έστω D η πολυωνυμική σχέση ισοδυναμίας. Δηλαδή, δεδομένων $x_1, x_2, ..., x_p$ στιγμιότυπων της L, ισοδύναμων ως προς την D, παίρνουμε σε πολυωνυμικό χρόνο ένα (y,k) στιγμιότυπο της Q για το οποίο θα ισχύει $k \leq (max_{i=1}^{p}|x_i| + logp)^{c_1}$, για κάποια σταθερά c_1, και $(y,k) \in Q \Leftrightarrow \exists i \in [p]$ με $x_i \in L$.

2. Από το ότι υπάρχει πολυωνυμική συμπίεση από την Q στην R, δεδομένου ενός $(y,k) \in Q$, σε χρόνο πολυωνυμικό ως προς $|y| + |k|$ παίρνουμε ένα ισοδύναμο στιγμιότυπο z της R, με $|z| \leq k^{c_2}$, για κάποια σταθερά c_2.

3. Εφαρμόζοντας τον ορισμό της πολυωνυμικής σχέσης ισοδυναμίας στην D, έχουμε ότι για οποιοδήποτε ακέραιο n και πεπερασμένο σύνολο S, στιγμιότυπων μήκους n, μπορούμε σε πολυωνυμικό χρόνο να διαμερίσουμε το S σε το πολύ n^{c_3} κλάσεις ισοδυναμίας, για κάποια σταθερά c_3.

Έστω κατάλληλη πολυωνυμική συνάρτηση $t(n)$ που θα επιλέξουμε σε λίγο. Ο αλγόριθμος OR-Διύλισης από την L στην $OR(R)$ έχει ως εξής:

Εφαρμόζουμε την Παρατήρηση 3, για δεδομένο n, και για ένα οποιοδήποτε σύνολο $S = \{x_1, ..., x_{t(n)}\}$, $t(n)$ στιγμιότυπων της L, μήκους n το καθένα. Παίρνουμε ότι σε πολυωνυμικό χρόνο, διαμερίζεται το S σε κλάσεις ισοδυναμίας $X_1, X_2, ..., X_r$ ως προς την D, με $r \leq n^{c_3}$.

Παρατηρήστε ότι σε κάθε κλάση X_i, το υποσύνολο του S που ανήκει στην συγκεκριμένη κλάση έχει στοιχεία που είναι ισοδύναμα ως προς την D. Συνεπώς μπορούμε σε κάθε κλάση X_i, $i \in [r]$ να εφαρμόσουμε τον πολυωνυμικό αλγόριθμο της διασταυρούμενης

OR-σύνθεσης της υπόθεσης. Έτσι για κάθε κλάση X_i, ο αλγόριθμος δίνει ένα (y_i, k_i) στιγμιότυπο της Q. Και από την Παρατήρηση 1, προκύπτει ότι $k_i \leq (n + log(t(n)))^{c_1}$.

Έχουμε τώρα πλέον r στιγμιότυπα της Q, ένα από κάθε κλάση. Συμπιέζουμε τώρα καθένα από αυτά, χρησιμοποιώντας τον αλγόριθμο πολυωνυμικής συμπίεσης από την Q στην R που έχουμε από υπόθεση. Από την Παρατήρηση 2, για τα ανηγμένα συμπιεσμένα στιγμιότυπα z_i, $i \in [r]$, θα ισχύει $|z_i| \leq {k_i}^{c_2}$.

Προφανώς το $y = (z_1, z_2, ...z_r)$ είναι ένα έγκυρο στιγμιότυπο της $OR(R)$. Αυτό ολοκληρώνει τον αλγόριθμο.

Ο αλγόριθμος είναι προφανώς πολυωνυμικός αφού οι r κλάσεις ισοδυναμίας κατασκευάζονται όπως είπαμε σε πολυωνυμικό χρόνο, και μετά εφαρμόζουμε απλά r, δηλαδή πολυωνυμικά πολλές φορές, έναν πολυωνυμικό αλγόριθμο διασταυρούμενης OR-σύνθεσης και έναν πολυωνυμικό αλγόριθμο συμπίεσης.

Επίσης για την ορθότητα θέλουμε να δείξουμε ότι $y \in OR(R) \Leftrightarrow x_i \in L$ για κάποιο $i \in [t(n)]$.

($\Leftarrow$): Έστω $x_i \in L$ για κάποιο $i \in [t(n)]$. Έστω X_j, $j \in [r]$, η κλάση ισοδυναμίας που μπαίνει η x_i από τον αλγόριθμο. Όταν εφαρμοστεί ο αλγόριθμος διασταυρούμενης OR-σύνθεσης στην X_j, επειδή $x_i \in X_j$ και $x_i \in L$ θα έπεται εξ ορισμού της διασταυρούμενης OR-σύνθεσης ότι $(y_j, k_j) \in Q$, και άρα μετά από ορισμό της συμπίεσης εφαρμοσμένης στο (y_j, k_j), επειδή $(y_j, k_j) \in Q$, θα πάρουμε ότι $z_j \in R$, και άρα ότι πράγματι $y \in OR(R)$.

($\Rightarrow$): Αποδεικνύεται πανομοιότυπα.

Άρα ο αλγόριθμος που παρουσιάσαμε αποτελεί έναν έγκυρο αλγόριθμο OR-Διύλισης από την L στην $OR(R)$. Αρκεί τώρα να διαλέξουμε πολυωνυμική $t(n)$.

Από ορισμό OR-Διύλισης, αρκεί $|y| \leq t(n)$. Θα είναι:

$|y| \leq r + |z_1| + ... + |z_r| \leq r + r \cdot max\{|z_i|\} \leq r + r \cdot max\{{k_i}^{c_2}\} \leq r + r \cdot (n + log(t(n)))^{c_1 \cdot c_2} \leq n^{c_3} + n^{c_3} \cdot (n + log(t(n)))^{c_1 \cdot c_2} \leq n^{2c_3} \cdot (nlog(t(n)))^{c_1 \cdot c_2} \leq n^{2 \cdot (c_3 + c_1 \cdot c_2)}$

Άρα αρκεί $t(n) = n^{2 \cdot (c_3 + c_1 \cdot c_2)}$. Και έτσι ολοκληρώνεται η απόδειξη. ■

Το παραπάνω θεώρημα μας λέει ότι έχοντας μια διασταυρούμενη OR-σύνθεση μιας γλώσσας L σε μια παραμετροποιημένη γλώσσα Q η οποία επιδέχεται πολυωνυμικό πυρήνα, παίρνουμε μια πολυωνυμική OR-Διύλιση της L. Συνδυάζοντας το αποτέλεσμα της προηγούμενης ενότητας, αυτό είναι μάλλον αδύνατο, αν η L είναι NP-δύσκολη. Άρα ένας νέος τρόπος να δείξουμε ότι ένα παραμετροποιημένο πρόβλημα δεν επιδέχεται πολυωνυμικό πυρήνα, είναι να δείξουμε μια διασταυρούμενη OR-σύνθεση από μια NP-δύσκολη γλώσσα σε αυτό.

AND-Διύλιση και Διασταυρούμενη AND-Σύνθεση

Αντικαθιστώντας το λογικό Η, με το λογικό ΚΑΙ, στους παραπάνω ορισμούς μπορούμε να ορίσουμε αντίστοιχα τις έννοιες της AND-Διύλισης και διασταυρούμενης AND-σύνθεσης.

AND-Διύλιση: Έστω $L, R \subseteq \{0,1\}^*$ γλώσσες και $t : \mathbb{N} \to \mathbb{N}\backslash\{0\}$ συνάρτηση. Τότε ένας αλγόριθμος AND-Διύλισης από την L στην R είναι ένας πολυωνυμικός αλγόριθμος όπου για κάθε n, δεδομένων $t(n)$ στιγμιότυπων $x_1, x_2, ..., x_{t(n)}$ της L, με $|x_i| = n$, έχει σαν έξοδο ένα στιγμιότυπο y της R, με $|y| \leq t(n) \cdot logn$, ώστε $y \in R \Leftrightarrow x_i \in L$ για κάθε $i \in [t(n)]$.

Διασταυρούμενη AND-Σύνθεση. Δεδομένων μιας γλώσσας $L \subseteq \{0,1\}^*$ και μιας παραμετροποιημένης γλώσσας $Q \subseteq \{0,1\}^* \times \mathbb{N}$, λέμε ότι η L έχει μια διασταυρούμενη AND-σύνθεση στην Q αν υπάρχει μια πολυωνυμική σχέση ισοδυναμίας R και ένας αλγόριθμος A με τις εξής ιδιότητες.

- Ο αλγόριθμος A παίρνει ως είσοδο t στιγμιότυπα της L, $x_1, x_2, ..., x_t$, όλα ισοδύναμα μεταξύ τους ως προς την R.
- Τρέχει σε χρόνο πολυωνυμικό ως προς το $\sum_{i=1}^{t} |x_i|$.
- Έχει σαν έξοδο ένα στιγμιότυπο $(y, k) \in \{0,1\}^* \times \mathbb{N}$ της Q τέτοιο ώστε:
  - $k \leq p(max_{i=1}^{t}|x_i| + logt)$ για κάποιο πολυώνυμο p.
  - $(y, k) \in Q \Leftrightarrow x_i \in L,\ \forall i \in [t]$.

Και αντίστοιχα έχουμε τα εξής θεωρήματα:

Θεώρημα 6. *Αν υπάρχει ένας αλγόριθμος AND-Διύλισης από μία $L \subseteq \{0,1\}^*$ σε μία $R \subseteq \{0,1\}^*$, για κάποια πολυωνυμική συνάρτηση t, τότε $L \in coNP/poly$.*

Θεώρημα 7. *Έστω $L \subseteq \{0,1\}^*$ μια NP-δύσκολη γλώσσα. Εάν υπάρχει διασταυρούμενη AND-σύνθεση της L σε κάποια παραμετροποιημένη γλώσσα $Q \subseteq \{0,1\}^* \times \mathbb{N}$, η οποία επιδέχεται και πολυωνυμικό πυρήνα (ή γενικότερα πολυωνυμική συμπίεση), τότε θα είναι $NP \subseteq coNP/poly$.*

Α. ΠΑΡΑΡΤΗΜΑ Ι

Προετοιμασία Απόδειξης Λήμματος 1

Αρχίζουμε περιγράφοντας την ιδέα και την κατασκευή για κανονικά γραφήματα $(d = 2)$ για να αποκτήσουμε λίγο διαίσθηση πριν γενικεύσουμε στα υπεργραφήματα $(d > 2)$.

Υπενθυμίζουμε σκοπός μας είναι να κατασκευάσουμε γράφημα P, με σχετικά μικρή τάξη, ώστε να ισχύουν τα εξής:

(i) Οι ακμές του P διαμερίζονται σε t κλίκες, καθεμία με ακριβώς s κόμβους.

(ii) Το P δεν περιέχει άλλες κλίκες μεγέθους s, εκτός από αυτές του (i).

Σκεφτόμαστε το P ως ένα s-μερές (s-partite) γράφημα, με τις κορυφές του εμβαπτισμένες σε ένα δισδιάστατο πίνακα διαστάσεων $p \cdot s$, όπου καθένα εκ των s ανεξάρτητων συνόλων αποτελεί μια στήλη του πίνακα. Θέλουμε η κάθε κλίκα K_i να έχει ακριβώς μια κορυφή από κάθε στήλη. Τετριμμένα, με την ξένη ένωση των κλικών, διαλέγοντας $p = t$ δηλαδή, το πετυχαίνουμε εύκολα αυτό, αλλά χρησιμοποιούμε τότε $t \cdot s$ συνολικά κορυφές. Επίσης ανάμεσα σε δύο οποιεσδήποτε στήλες, από τις πιθανές $p^2 = t^2$ ακμές, μόνο οι p ανήκουν σε κάποιο K_i, δηλαδή πολλές ακμές μένουν αχρησιμοποίητες, κάτι που μας υπονοεί ότι μπορούμε να κάνουμε καλύτερα. Ας διαλέξουμε $p = \sqrt{t}$. Τότε από τις πιθανές $p^2 = t$ ακμές θα χρησιμοποιούνται υποχρεωτικά όλες, αφού όπως είπαμε κάθε K_i έχει ακριβώς μία κορυφή σε κάθε στήλη, άρα ανάμεσα σε δύο στήλες, κάθε K_i συνεισφέρει ακριβώς μία ακμή, άρα t στο σύνολο από όλα τα K_i. Αυτό επίσης μας υπονοεί ότι δεν μπορούμε να μειώσουμε άλλο το p κάτω από το $\sqrt{t}$, διότι τότε θα παραβιαζόταν σίγουρα η (i). Διαλέγουμε λοιπόν το p ως τον μικρότερο πρώτο αριθμό μεγαλύτερο ή ίσο του $max(s, \sqrt{t})$. Τότε κάθε κορυφή και στήλη αντιστοιχίζεται σε ένα στοιχείο του $\mathbb{Z}_p$. Διαλέγουμε τώρα t διαφορετικές γραμμικές συναρτήσεις 2 συντελεστών $h_1, h_2, ..., h_t$ πάνω στο $\mathbb{Z}_p$ ($h_i : \mathbb{Z}_p \to \mathbb{Z}_p$), μία για κάθε κλίκα K_i. Παρατηρήστε κάθε γραμμική συνάρτηση 2 συντελεστών πάνω στο $\mathbb{Z}_p$ είναι της μορφής $a \cdot x + b$ με $a, b \in \mathbb{Z}_p$, άρα υπάρχουν $p^2 \geq t$ διαφορετικές τέτοιες συναρτήσεις, όσες είναι και οι κλίκες, άρα μπορούμε να αναθέσουμε μια συνάρτηση διαφορετική σε κάθε κλίκα. Αυτές οι συναρτήσεις θα μας ορίσουν τα $V(K_i)$ αφού θέτουμε:

$$V(K_i) = \{(j, h_i(j)) : j \in [s]\}, \forall i \in [t]$$

Δηλαδή για κάθε στήλη, η h_i μας δηλώνει ποιο μοναδικό κόμβο της στήλης θα βάλουμε στο $V(K_i)$. Έχοντας ορίσει τα $V(K_i)$, αυτομάτως ορίζεται και το $E(P)$ ως η ένωση των ακμών των K_i. Επίσης θα είναι:

$$\bigcup_{i \in [t]} V(K_i) \subseteq [s] \times \mathbb{Z}_p = V(P)$$

Επίσης, η μέχρι τώρα κατασκευή ικανοποιεί και την ιδιότητα (i). Έστω μία ακμή $(u, v) \in E(P)$, με $u = (a, b)$ και $v = (a', b')$. Αφού P s-μερές, τα u, v ανήκουν σε διαφορετικές στήλες, άρα $a \neq a'$, δηλαδή $a - a' \neq 0_{\mathbb{Z}_p}$, άρα ορίζεται ο $(a - a')^{-1}$. Τα δύο σημεία/κόμβοι u, v ορίζουν μοναδική ευθεία:

$$y = \frac{b - b'}{a - a'} \cdot x + b - \frac{b - b'}{a - a'} \cdot a = (b - b') \cdot (a - a')^{-1} \cdot x + b - (b - b') \cdot (a - a')^{-1} \cdot a$$

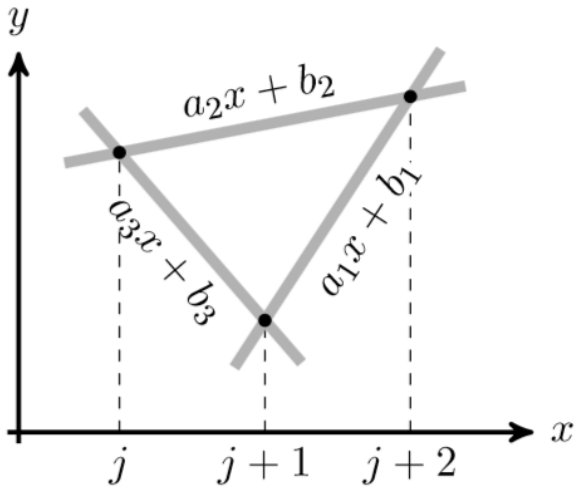
Παρατηρήστε ότι η παραπάνω ευθεία αντιστοιχεί σε μοναδική γραμμική συνάρτηση 2 συντελεστών h, πάνω στο $\mathbb{Z}_p$. Και επειδή $(u, v) \in E(P)$, η h θα ταυτίζεται με κάποια μοναδική

h_i, άρα θα αντιστοιχεί σε μοναδικό K_i, συνεπώς $(u, v) \in E(K_i)$ και μόνο, άρα ικανοποιείται η (i).

Ωστόσο, επειδή το P, όπως το κατασκευάσαμε μέχρι στιγμής είναι πλήρες s-μερές γράφημα, δεν ικανοποιεί την (ii). Θα πρέπει να κάνουμε μια μικρή τροποποίηση.

Έστω μια κλίκα K μεγέθους s του P. Αυτή θα έχει υποχρεωτικά έναν κόμβο από κάθε στήλη του P, άρα υπάρχει συνάρτηση $h : \mathbb{Z}_p \to \mathbb{Z}_p$ ώστε $V(K) = \{(j, h(j)) : j \in [s]\}$. Αρκεί να επιβάλλουμε ότι η K θα αντιστοιχεί σε κάποιο K_i, δηλαδή ισοδύναμα ότι η h θα αντιστοιχεί σε κάποια h_i.

Αν θεωρήσουμε 3 διαδοχικές στήλες $j, j + 1, j + 2$ του P, τα τρία σημεία που τέμνει η K αυτές τις στήλες (ένα σημείο ανά στήλη) ορίζουν ένα τρίγωνο. Οι 3 ακμές του, αντιστοιχούν σε 3 γραμμικές συναρτήσεις πάνω στο $\mathbb{Z}_p$. Οι υψηλόβαθμοι συντελεστές των 3 αυτών γραμμικών συναρτήσεων ορίζουν αριθμητική πρόοδο. Για να το δούμε αυτό, παρατηρήστε ότι από την στήλη j στην στήλη $j + 2$, ακολουθώντας τη μία ακμή του τριγώνου, η τιμή της τεταγμένης αυξάνεται κατά $2 \cdot a_2$, ενώ αν πάμε από την στήλη j στην $j+2$ χρησιμοποιώντας τις δύο ακμές μέσω της στήλης $j + 1$, η τεταγμένη αυξάνεται πρώτα κατά a_3 και μετά κατά a_1, όπως φαίνεται στο παρακάτω σχήμα που προέρχεται από το [5]. Συνεπώς θα πρέπει να ισχύει $2 \cdot a_2 = a_3 + a_1 \iff a_3 - a_2 = a_2 - a_1$, άρα οι υψηλόβαθμοι συντελεστές a_1, a_2, a_3 είναι διαδοχικοί όροι αριθμητικής προόδου.



Σχήμα A□.1: Το τρίγωνο που ορίζουν οι κόμβοι μιας κλίκας σε 3 διαδοχικές στήλες του P

Αν μπορούσαμε να επιβάλλουμε με κάποιο τρόπο αυτή η αριθμητική πρόοδος να ήταν τετριμμένη, δηλαδή να είχε βήμα 0, δηλαδή $a_1 = a_2 = a_3$, τότε τα 3 αυτά σημεία θα ήταν σε μία μόνο ευθεία, και επειδή αυτό θα ίσχυε για οποιεσδήποτε 3 διαδοχικές στήλες, τα σημεία της K θα προέκυπταν από μία γραμμική συνάρτηση πάνω στο $\mathbb{Z}_p$, άρα θα ταυτιζόταν η h με κάποια h_i όπως θέλουμε.

Και αυτό το καταφέρνουμε μέσω του παρακάτω λήμματος:

Λήμμα (Σύνολα χωρίς μη τετριμμένες αριθμητικές προόδους μήκους 3)**.**
$\forall p \in \mathbb{Z}^+$, $\exists\, A \subseteq \mathbb{Z}_p$, *με* $|A| \geq p^{1-o(1)}$*, που δεν περιέχει μη τετριμμένες αριθμητικές πρόοδους μεγέθους 3. Δηλαδή οποιαδήποτε 3 στοιχεία του* A*, είτε αποτελούν τετριμμένη αριθμητική πρόοδο είτε δεν αποτελούν αριθμητική πρόοδο. Επίσης ένα τέτοιο* A *κατασκευάζεται σε πολυωνυμικό χρόνο ως προς το* p*.*

Το παραπάνω λήμμα είναι από το [9], ενώ για την απόδειξη μπορείτε να ανατρέξετε και στο [5].

Άρα αν διαλέξουμε τις a_i των h_i από ένα τέτοιο A, έχουμε και την ιδιότητα (ii).

Το μόνο που πληρώνουμε είναι ότι θα πρέπει να αυξήσουμε λίγο το p, ώστε να εξακολουθούμε να μπορούμε να διαλέξουμε t διαφορετικές h_i, δηλαδή να διαλέξουμε p ώστε να ισχύει $|A| \cdot p \geq t$. Αρκεί το $p \geq (\sqrt{t})^{1+o(1)}$. Άρα τελικά το P έχει τις ιδιότητες (i),(ii) και $p = O(\max(s, (\sqrt{t})^{1+o(1)}))$.

Απόδειξη Λήμματος 1 (Γενίκευση για $d \geq 2$)

Η απόδειξη είναι από το [5].

Δεδομένων των $s \geq d \geq 2$, $t > 0$, έστω p ο ελάχιστος πρώτος με $p \geq s$ και $|A| \cdot p^{d-1} \geq t$ όπου A το σύνολο του λήμματος. Προκύπτει ότι $p = O(\max(s, t^{1/d+o(1)}))$ και τόσο το p όσο και το A υπολογίζονται σε πολυωνυμικό ως προς τα s, t χρόνο.

Η κατασκευή του P έχει ως εξής: Θεωρούμε τα πολυώνυμα βαθμού $d-1$ πάνω στο $\mathbb{Z}_p$, των οποίων ο μεγιστοβάθμιος συντελεστής, ο συντελεστής του x^{d-1} δηλαδή, ανήκει στο A. Για τον μεγιστοβάθμιο συντελεστή έχουμε λοιπόν $|A|$ επιλογές, ενώ για τους υπόλοιπους $d-1$ έχουμε p επιλογές για τον καθένα (αφού ανήκουν στο $\mathbb{Z}_p$). Άρα συνολικά υπάρχουν $|A| \cdot p^{d-1} \geq t$ τέτοια πολυώνυμα, άρα μπορούμε να αναθέσουμε ένα διαφορετικό h_i για κάθε K_i , $i \in [t]$. Τα δε K_i ορίζονται ως πλήρη d ομοιόμορφα υπεργραφήματα με $V(K_i) = \{(j, h_i(j)) : j \in [s]\}$.

Συνεπώς δηλαδή θα είναι: $\bigcup_{i\in[t]} V(K_i) \subseteq [s] \times \mathbb{Z}_p = V(P)$ και $E(P) = \bigcup_{i\in[t]} E(K_i)$. Τα K_i και κατ'επέκταση και το P κατασκευάζονται σε πολυωνυμικό ως προς τα s, t χρόνο, αφού για κάθε K_i χρειαζόμαστε s αποτιμήσεις ενός πολυωνύμου βαθμού $d-1$, κάθε αποτίμηση θέλει $O(d)$ υπολογισμούς με τη μέθοδο του Horner πχ, και έχουμε t K_i, άρα συνολικά θέλουμε περίπου χρόνο $O(s \cdot t \cdot d) = O(s \cdot t)$ αφού d σταθερό, το οποίο είναι προφανώς πολυωνυμικό ως προς s, t.

Για την ιδιότητα (i), έστω μια υπερακμή (hyperedge) e του P, η οποία θα έχει d κορυφές προφανώς αφού P είναι d ομοιόμορφο. Εκ κατασκευής η e θα ανήκει σε τουλάχιστον ένα $E(K_i)$. Για να αποδείξουμε λοιπόν την ιδιότητα (i), αρκεί να δείξουμε ότι η e θα ανήκει το πολύ σε ένα $E(K_i)$. Παρατηρήστε ότι εκ κατασκευής, δύο κορυφές με ίδια πρώτη συντεταγμένη, δεν γίνεται να ανήκουν στην ίδια υπερακμή, άρα οι d κορυφές/ζεύγη στην e έχουν όλες διαφορετική πρώτη συντεταγμένη. Άρα ισοδύναμα έχουμε d αποτιμήσεις μιας συνάρτησης σε d διαφορετικά σημεία. Αν απαιτήσουμε αυτή η συνάρτηση να είναι πολυώνυμο βαθμού $d-1$ πάνω στο $\mathbb{Z}_p$, αυτά τα d σημεία ορίζουν μοναδικό τέτοιο πολυώνυμο h'. Αφού το πολυώνυμο αυτό είναι μοναδικό, θα υπάρχει το πολύ ένα $i \in [t]$ ώστε η h_i να συμφωνεί με την h' σε όλα αυτά τα d σημεία. Άρα αφενός παίρνουμε $i \in [t]$ (αφού

$e \in E(K_b)$ για τουλάχιστον ένα $b \in [t]$) αφετέρου αυτό είναι το μοναδικό i με αυτήν την ιδιότητα, συνεπώς $e \in E(K_i)$ και μόνο.
Για την ιδιότητα (ii), αρκεί να αποδείξουμε το εξής:

Ισχυρισμός (1). *Για οποιαδήποτε $h : [s] \to \mathbb{Z}_p$ με την ιδιότητα ότι για κάθε $D \subseteq [s]$ με $|D| = d$, υπάρχει $j \in [t]$, ώστε $h(x) = h_j(x),\ \forall x \in D$, τότε συνεπάγεται ότι υπάρχει $i \in [t]$ ώστε $h(x) = h_i(x),\ \forall x \in [s]$.*

Με άλλα λόγια αν για μια δεδομένη συνάρτηση h, για κάθε υποσύνολο μεγέθους d του $[s]$ υπάρχει κάποιο $j \in [t]$, ώστε οι h, h_j να ταυτίζονται σε αυτό το υποσύνολο, τότε θα υπάρχει κάποιο $i \in [t]$, ώστε οι h, h_i να ταυτίζονται σε όλο το $[s]$ και συνεπώς $h = h_i$.

Αν δείξουμε τον Ισχυρισμό (1), τότε έστω μια κλίκα K μεγέθους s του P. Επειδή οποιοδήποτε υποσύνολο μεγέθους d του $V(K)$ αποτελεί ακμή του P και συνεπώς ανήκει σε κάποιο K_i, και επειδή κανένα εκ των K_i δεν έχει κόμβους με ίδια πρώτη συντεταγμένη, εκ κατασκευής, και η K δεν θα έχει κόμβους με ίδια πρώτη συντεταγμένη, δηλαδή θα υπάρχει $h : [s] \to \mathbb{Z}_p$ ώστε $V(K) = \{(j, h(j)) : j \in [s]\}$. Για αυτήν την h τώρα, οποιοδήποτε υποσύνολο μεγέθους d του $[s]$, θα αντιστοιχεί σε ένα υποσύνολο μεγέθους d του $V(K)$, και άρα θα αντιστοιχεί σε μια ακμή του P, δηλαδή θα ανήκει σε κάποιο K_j, $j \in [t]$, δηλαδή οι d αυτοί κόμβοι παράγονται από κάποια $h_j, j \in [t]$, δηλαδή οι h, h_j ταυτίζονται σε αυτό το υποσύνολο. Από Ισχυρισμό (1), έπεται ότι θα υπάρχει κάποιο $i \in [t]$, ώστε οι h, h_i να ταυτίζονται σε όλο το $[s]$, άρα $h = h_i$ και συνεπώς $K = K_i$. Δηλαδή πράγματι δεν υπάρχουν άλλες κλίκες μεγέθους s στο P πέρα των K_i.

Πριν την απόδειξη του Ισχυρισμού (1), παρουσιάζουμε και αποδεικνύουμε πρώτα έναν ακόμα ισχυρισμό:

Ισχυρισμός (2). *Για $k \in \{j, j+1, ..., j+d\} \subseteq [s] \subseteq \mathbb{Z}_p$, έστω q_k να είναι πολυώνυμα βαθμού το πολύ $d-1$ πάνω στο $\mathbb{Z}_p$, των οποίων οι υψηλόβαθμοι συντελεστές (δηλαδή οι συντελεστές του x^{d-1}), σαν σύνολο, δεν έχουν μη τετριμμένες αριθμητικές προόδους μήκους 3. Εάν επίσης για όλα τα $k, l \in \{j, j+1, ..., j+d\}$, τα q_k, q_l συμφωνούν στο $\{j, j+1, ..., j+d\}\backslash\{k, l\}$, τότε τα q_k ταυτίζονται, είναι όλα το ίδιο πολυώνυμο δηλαδή.*

Απόδειξη Ισχυρισμού (2):

Απόδειξη. Με επαγωγή στο d.

Επαγωγική Βάση: Για $d = 2$ ισχύει ο ισχυρισμός, όπως επιχειρηματολογήσαμε στην αρχή για τα απλά γραφήματα.

Επαγωγική Υπόθεση: Έστω ότι ισχύει ο ισχυρισμός για $d-1$. Θα δείξουμε ότι ισχύει και για d.

Επαγωγικό Βήμα: Έστω $q_j, q_{j+1}, ..., q_{j+d}$ τα πολυώνυμα βαθμού $d-1$ του Ισχυρισμού (2), των οποίων οι υψηλόβαθμοι συντελεστές (δηλαδή οι συντελεστές του x^{d-1}), σαν σύνολο, δεν έχουν μη τετριμμένες αριθμητικές πρόοδους μήκους 3, και επίσης για όλα τα $k, l \in \{j, j+1, ..., j+d\}$, τα q_k, q_l συμφωνούν στο $\{j, j+1, ..., j+d\}\backslash\{k, l\}$. Θα δείξουμε ότι τα $q_j, q_{j+1}, ..., q_{j+d}$ ταυτίζονται. Ορίζουμε τα $q'_j, q'_{j+1}, ..., q'_{j+d-1}$, με $q'_k : \{j, j+1, ..., j+d-1\} \to \mathbb{Z}_p$ ως εξής:

$$q'_k(x) = \frac{q_k(x) - q_k(j+d)}{x - j - d},\ x \in \{j, j+1, ..., j+d-1\}$$

Παρατηρήστε ότι κάθε q'_k είναι πολυώνυμο αφού το $q_k(x) - q_k(j+d)$ είναι πολυώνυμο και έχει παράγοντα τον $x-j-d$, έχει βαθμό το πολύ $d-2$ αφού το q_k και κατ'επέκταση το $q_k(x) - q_k(j+d)$ έχει βαθμό το πολύ $d-1$ και επίσης ο μεγιστοβάθμιος συντελεστής (δηλαδή ο συντελεστής του x^{d-2}) του q'_k είναι ο ίδιος με τον μεγιστοβάθμιο συντελεστή (δηλαδή τον συντελεστή του x^{d-1}) του q_k. Συνεπώς όλοι οι μεγιστοβάθμιοι συντελεστές των q'_k σαν σύνολο ταυτίζονται με το σύνολο με το σύνολο των μεγιστοβάθμιων συντελεστών των q_k, άρα από υπόθεση δεν θα έχουν μη τετριμμένες αριθμητικές προόδους μήκους 3. Επίσης για όλα τα $k,l \in \{j, j+1, ..., j+d-1\}$, τα q'_k, q'_l συμφωνούν σε όλα τα $x \in \{j, j+1, ..., j+d-1\}\backslash\{k,l\}$ αφού θα είναι:

$$q'_k(x) = \frac{q_k(x) - q_k(j+d)}{x-j-d} = \frac{q_l(x) - q_l(j+d)}{x-j-d} = q'_l(x)$$

όπου χρησιμοποιήσαμε το γεγονός ότι από υπόθεση τα q_k, q_l συμφωνούν στα $x, j+d$ (αφού συμφωνούν στα $\{j, j+1, ..., j+d\}\backslash\{k,l\}$ και $j+d \neq k,l$).

Συνεπώς από Επαγωγική Υπόθεση όλα τα q'_k ταυτίζονται μεταξύ τους, έστω ότι είναι το πολύωνυμο q'. Όμως από τον ορισμό των q'_k έχουμε:

$$q_k(x) = q'_k(x)\cdot(x-j-d) + q_k(j+d) = q'(x)\cdot(x-j-d) + q_k(j+d),\ k \in \{j, j+1, ..., j+d-1\}$$

Επειδή από υπόθεση τα q_k συμφωνούν στο $j+d$, έχουμε ότι όλα τα q_k ταυτίζονται, για $k \in \{j, j+1, ..., j+d-1\}$, έστω ότι είναι το πολυώνυμο q. Μένει να δείξουμε ότι τα q, q_{j+d} ταυτίζονται. Αυτό όμως προκύπτει άμεσα από το ότι τα q, q_{j+d} είναι πολυώνυμα βαθμού το πολύ $d-1$ και συμφωνούν σε d σημεία από υπόθεση, στα σημεία με πρώτη συντεταγμένη στο $\{j, j+1, ..., j+d-1\}$, τα οποία ορίζουν όπως ξέρουμε μοναδικό πολυώνυμο βαθμού $d-1$. ■

Απόδειξη Ισχυρισμού (1):

Απόδειξη. Έστω $h : [s] \to \mathbb{Z}_p$ με την δεδομένη ιδιότητα. Θεωρούμε ένα υποσύνολο του $[s]$ που αποτελείται από $d+1$ διαδοχικά στοιχεία, δηλαδή ένα υποσύνολο της μορφής $\{j, j+1, ..., j+d\}$. Για $k \in \{j, j+1, ..., j+d\}$, θέτουμε ως q_k την h_i, $i \in [t]$ που συμφωνεί με την h στο $\{j, j+1, ..., j+d\}\backslash\{k\}$. Τα q_k όπως τα ορίσαμε εδώ πληρούν τις υποθέσεις του Ισχυρισμού (2), αφού οι μεγιστοβάθμιοι συντελεστές των h_i προέρχονται από το A, το οποίο δεν περιέχει μη τετριμμένες αριθμητικές προόδους μήκους 3, και επίσης για οποιαδήποτε $k,l \in \{j, j+1, ..., j+d\}$, οι $h_i, h_{i'}$ που αντιστοιχούν στις q_k, q_l συμφωνούν μεταξύ τους στο $\{j, j+1, ..., j+d\}\backslash\{k,l\}$, αφού συμφωνούν η καθεμία με την h στα σημεία αυτά. Συνεπώς από Ισχυρισμό (2), όλα τα q_k και κατ'επέκταση τα h_i που τους αντιστοιχούν, ταυτίζονται μεταξύ τους, και ταυτίζονται και με την h στο $\{j, j+1, ..., j+d\}$. Εφαρμόζοντας την παραπάνω λογική διαδοχικά για $j \in [s-d]$, παίρνουμε για $j=1$, ότι υπάρχει $h_z,\ z \in [t]$, ώστε $h_z = h$ στο $\{1, 2, ..., d+1\}$, μετά για $j=2$ θα υπάρχει ένα πολυώνυμο $h_{z'}, z' \in [t]$, που θα αντιστοιχεί σε κάποιο q_k και άρα θα συμφωνεί με την h στο $\{2, 3, ..., d+2\}$. Όμως έπεται ότι θα συμφωνεί και με την h_z στο $\{2, 3, ..., d+1\}$, σε d σημεία δηλαδή, και είναι πολυώνυμα $d-1$ βαθμού το πολύ, άρα τελικά η $h_{z'}$ συμπίπτει με την h_z και άρα θα είναι $h_z = h$ και στο $\{2, 3, ..., d+2\}$ κοκ. Για $j = s-d$, παίρνουμε όμοια ότι $h_z = h$ στο $\{s-d, s-d+1, ..., s\}$. Συνεπώς $h_z = h$ σε όλο το $[s]$. ■

Απόδειξη Λήμματος 3:

Η απόδειξη είναι από το [11].

Απόδειξη. Η απόδειξη προκύπτει άμεσα από τους ορισμούς που δώσαμε.
Έστω $L \in co\text{-}(K/poly)$. Για οποιοδήποτε $x \in L$ θα είναι:

$$x \in L \Leftrightarrow x \notin co\text{-}L, \text{ με } co\text{-}L \in K/poly$$

Από ορισμό θα ισχύει ότι $\exists L' \in K$, ακολουθία συμβολοσειρών a, με $|a_n| \leq poly(n)$, ώστε:

$$x \in co\text{-}L \Leftrightarrow (x, a_{|x|}) \in L', \text{ ή ισοδύναμα } x \in L \Leftrightarrow (x, a_{|x|}) \notin L', \text{ ή ισοδύναμα}$$

$$x \in L \Leftrightarrow (x, a_{|x|}) \in co\text{-}L', \text{ με } co\text{-}L' \in co\text{-}K$$

Από την τελευταία ισοδυναμία, εφαρμόζοντας τον ορισμό, παίρνουμε ότι $L \in (co\text{-}K)/poly$, δηλαδή: $co\text{-}(K/poly) \subseteq (co\text{-}K)/poly$ (1)

Αντίστοιχα, έστω $L \in (co\text{-}K)/poly$. Από ορισμό παίρνουμε ότι $\exists L' \in co\text{-}K$, ακολουθία συμβολοσειρών a, με $|a_n| \leq poly(n)$ ώστε:

$$x \in L \Leftrightarrow (x, a_{|x|}) \in L', \text{ ή ισοδύναμα } x \in co\text{-}L \Leftrightarrow (x, a_{|x|}) \in co\text{-}L', \text{ με } co\text{-}L' \in K$$

δηλαδή έχουμε από ορισμό ότι $co\text{-}L \in K/poly$, δηλαδή ότι $L \in co\text{-}(K/poly)$,
δηλαδή: $(co\text{-}K)/poly \subseteq co\text{-}(K/poly)$ (2)

Από τις (1), (2) έπεται η ζητούμενη ισότητα. ■

Απόδειξη Λήμματος 5:

Η απόδειξη είναι από το [11].

Απόδειξη. Ισχυριζόμαστε αρχικά ότι για $i > 0$: $\Pi_i \subseteq \Sigma_i/poly \Rightarrow \Sigma_{i+1}/poly = \Sigma_i/poly$ (Λήμμα 4). Έχοντας αυτό, η απόδειξη του λήμματος ακολουθεί ως εξής:

Θεωρούμε για $i > 0$ ότι πράγματι $\Pi_i \subseteq \Sigma_i/poly$ και επομένως $\Sigma_{i+1}/poly = \Sigma_i/poly$

Έχουμε: $\Pi_i \subseteq \Sigma_{i+1} \Rightarrow \Pi_i/poly \subseteq \Sigma_{i+1}/poly = \Sigma_i/poly = (co\text{-}\Pi_i)/poly = co\text{-}(\Pi_i/poly)$

Όπου η τελευταία ισότητα προέκυψε από εφαρμογή του Λήμματος 3.

Άρα έχουμε $\Pi_i/poly \subseteq co\text{-}(\Pi_i/poly) \Leftrightarrow^{(*)} \Pi_i/poly = co\text{-}(\Pi_i/poly) = \Sigma_i/poly$, το οποίο είναι και το ζητούμενο.

Για την $(*)$ παρατηρήστε ότι για οποιαδήποτε κλάση πολυπλοκότητας K ισχύει $K \subseteq co\text{-}K \Leftrightarrow K = co\text{-}K$. Το αντίστροφο είναι προφανές. Για το ευθύ παρατηρήστε ότι, αν $K \subseteq co\text{-}K$, για οποιαδήποτε γλώσσα L θα είναι: $L \in co\text{-}K \Rightarrow co\text{-}L \in K \Rightarrow co\text{-}L \in co\text{-}K \Rightarrow L \in K$, άρα $co\text{-}K \subseteq K$ και άρα ισχύει η ισότητα. ■

Απόδειξη Λήμματος 4:

Η απόδειξη είναι από το [11].

Απόδειξη. Μένει η απόδειξη του ισχυρισμού του παραπάνω λήμματος. Έστω λοιπόν ότι για $i > 0$, $\Pi_i \subseteq \Sigma_i/poly$ και έστω $L \in \Sigma_{i+1}/poly$. Αρκεί να δείξουμε ότι $L \in \Sigma_i/poly$, δηλαδή ότι $\Sigma_{i+1}/poly \subseteq \Sigma_i/poly$ (το ότι $\Sigma_i/poly \subseteq \Sigma_{i+1}/poly$ είναι προφανές αφού $\Sigma_i \subseteq \Sigma_{i+1}$).

(1): Λόγω του $L \in \Sigma_{i+1}/poly$ έχουμε:

$$\exists S \in \Sigma_{i+1}, \text{ ακολουθία } a \text{ με} |a_n| \leq poly(n) \text{ ώστε: } \forall x : x \in L \Leftrightarrow x \cdot a_{|x|} \in S \quad \textbf{(1)}$$

(2): Λόγω του $S \in \Sigma_{i+1}$ έχουμε ότι υπάρχει πολυώνυμο p^*, μηχανή Turing M_S ώστε:

$$\forall y : y \in S \Leftrightarrow \exists u_1 \in \{0,1\}^{p^*(|y|)} \; \forall u_2 \in \{0,1\}^{p^*(|y|)} \; ... \; Q_{i+1}u_{i+1} \in \{0,1\}^{p^*(|y|)} \\ M_S(y, u_1, u_2, ..., u_{i+1}) = 1$$

Συνεπώς έχουμε: $\exists P \in \Pi_i, \text{ ώστε } \forall y : y \in S \Leftrightarrow \exists u \in \{0,1\}^{p^*(|y|)}$ ώστε $y \cdot u \in P$.

Μια τέτοια P με αυτήν την ιδιότητα είναι η εξής:

$$y \cdot u \in P \Leftrightarrow \forall u_2 \in \{0,1\}^{p^*(|y|)} \; ... \; Q_{i+1}u_{i+1} \in \{0,1\}^{p^*(|y|)} \; M_S^*(y \cdot u, u_2, ..., u_{i+1}) = 1$$

Όπου η M_S^* είναι η ίδια με την M_S, μόνο που τα δύο πρώτα της ορίσματα είναι συνενωμένα σε ένα, με μια συνάρτηση παράθεσης η οποία είναι αντιστρέψιμη. Προφανώς η P ορισμένη με αυτόν τον τρόπο ανήκει στο Π_i και έχει την επιθυμητή ιδιότητα. Θέτοντας $y = x \cdot a_{|x|}$ παίρνουμε:

$$\exists P \in \Pi_i, \text{ ώστε } \forall x : x \cdot a_{|x|} \in S \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} \text{ ώστε } x \cdot a_{|x|} \cdot u \in P \quad \textbf{(2)}$$

Όπου $p^*(|x \cdot a_{|x|}|) = p^*(|x| + |a_{|x|}|) \leq p^*(|x| + poly(|x|)) = p(|x|)$ πολυώνυμο ως προς $|x|$.

(3): αφού $\Pi_i \subseteq \Sigma_i/poly$, θα έχουμε $P \in \Sigma_i/poly$, δηλαδή:

$$\exists S' \in \Sigma_i, \text{ ακολουθία } a' \text{ με } |a'_n| \leq poly(n), \text{ ώστε } \forall y : y \in P \Leftrightarrow y \cdot a'_{|y|} \in S'$$

Θέτοντας $y = x \cdot a_{|x|} \cdot u$ παίρνουμε ότι:

$$\exists S' \in \Sigma_i, \text{ ακολουθία } a' \text{ με } |a'_n| \leq poly(n), \text{ ώστε } \forall x, u : x \cdot a_{|x|} \cdot u \in P \Leftrightarrow \\ x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \in S' \quad \textbf{(3)}$$

(4): Λόγω του ότι $S' \in \Sigma_i$, με ανάλογη επιχειρηματολογία όπως στο (2) έχουμε:

$$\exists P' \in \Pi_{i-1} \text{ ώστε } \forall y : y \in S' \Leftrightarrow \exists b \in \{0,1\}^{q^*(|y|)} \text{ ώστε } y \cdot b \in P'$$

Θέτοντας $y = x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|}$ παίρνουμε ότι:

$$\exists P' \in \Pi_{i-1} \text{ ώστε } \forall x, u \text{ με } u \in \{0,1\}^{p(|x|)} : x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \in S' \Leftrightarrow \\ \exists b \in \{0,1\}^{q(|x|)} \text{ ώστε } x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \cdot b \in P' \quad \textbf{(4)}.$$

Όπου q το πολυώνυμο που προκύπτει από τη σύνθεση του q^* με το πολυώνυμο που αντιστοιχεί στο μήκους του $y = x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|}$.

(5): Συνδυάζοντας τις ισοδυναμίες των (1),(2) παίρνουμε:

$$\exists P \in \Pi_i, \text{ ακολουθία } a \text{ με } |a_n| \leq poly(n), \text{ ώστε } \forall x : x \in L \Leftrightarrow \\ \exists u \in \{0,1\}^{p(|x|)} \text{ ώστε } x \cdot a_{|x|} \cdot u \in P \quad \textbf{(5)}$$

(6): Συνδυάζοντας τις ισοδυναμίες των (5),(3) παίρνουμε:

$$\exists S' \in \Sigma_i, \text{ ακολουθίες } a, a' \text{ με } |a_n| \leq poly(n),\ |a'_n| \leq poly(n) \text{ ώστε } \forall x : x \in L \Leftrightarrow \\ \exists u \in \{0,1\}^{p(|x|)} \text{ ώστε } x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \in S' \quad \textbf{(6)}$$

(7): Συνδυάζοντας τις ισοδυναμίες των (6),(4) παίρνουμε:

$$\exists P' \in \Pi_{i-1}, \text{ ακολουθίες } a, a' \text{ με } |a_n| \leq poly(n),\ |a'_n| \leq poly(n) \text{ ώστε } \forall x : x \in L \Leftrightarrow \\ \exists u \in \{0,1\}^{p(|x|)},\ \exists b \in \{0,1\}^{q(|x|)} \text{ ώστε } x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \cdot b \in P' \quad \textbf{(7)}$$

Θυμίζουμε σκοπός μας είναι να δείξουμε ότι $L \in \Sigma_i/poly$. Θα μετασχηματίσουμε λοιπόν την (7) ώστε να ικανοποιεί τον εξής ορισμό:

$$\exists S^* \in \Sigma_i, \text{ ακολουθία } a^* \text{ με } |a^*_n| \leq poly(n), \text{ ώστε } \forall x : x \in L \Leftrightarrow x \cdot a^*_{|x|} \in S^*$$

Έστω $x \in L$, θέτουμε $k = p(|x|)$, δηλαδή το k αντιστοιχεί στο μήκος του u για το συγκεκριμένο x στην ισοδυναμία (7).

Τώρα ορίζουμε την a^* ως εξής:

$$a^*_{|x|} = a_{|x|} \cdot 0^k \cdot z_0 \cdot z_1 \cdot ... \cdot z_k, \text{ όπου } z_i = a'_{|x \cdot a_{|x|} \cdot 0^i|} = a'_{|x|+|a_{|x|}|+i}$$

Παρατηρήστε ότι η a^* εξαρτάται μόνο από το $|x|$. Επίσης παρατηρήστε ότι $|a^*_{|x|}| \leq poly(|x|)$. Για αυτό παρατηρήστε ότι $|a^*_{|x|}| = |a_{|x|}| + k + |z_0| + |z_1| + ... + |z_k|$ και ότι για οποιαδήποτε $i \in [k]$:

$$|z_i| = |a'_{|x \cdot a_{|x|} \cdot 0^i|} \leq poly(|x \cdot a_{|x|} \cdot 0^i|) = poly(|x| + |a_{|x|}| + i) \leq poly(|x| + poly(|x|) + p(|x|)),$$

το οποίο είναι ένα πολυώνυμο ως προς $|x|$ προφανώς. Άρα το $|a^*_{|x|}|$ είναι φραγμένο από άθροισμα πολυωνυμικού πλήθους πολυωνύμων ως προς $|x|$, συνεπώς είναι φραγμένο από ένα πολυώνυμο στο $|x|$, και άρα πράγματι $|a^*_{|x|}| \leq poly(|x|)$. Δηλαδή η a^*, όπως την ορίσαμε, είναι μια έγκυρη ακολουθία πολυωνυμικών συμβολοσειρών συμβουλής.

Ορίζουμε τώρα την γλώσσα P^* ως εξής:

$$P^* := \{x \cdot v \cdot 0^k \cdot z_0 \cdot z_1 \cdot ... \cdot z_k \cdot c : \exists u \text{ με } x \cdot v \cdot u \cdot z_{|u|} \cdot b \in P' \text{ και } c = u \cdot b\}$$

Η $P^* \in \Pi_{i-1}$ αφού ορίζεται μέσω της $P' \in \Pi_{i-1}$ και υπάρχουν πολυωνυμικά πολλοί συνδυασμοί u, b να δοκιμαστούν, για δεδομένο c στην είσοδο. Επίσης θα ισχύει το εξής:

$$x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot u|} \cdot b \in P' \Leftrightarrow \\ x \cdot a_{|x|} \cdot u \cdot a'_{|x|+|a_{|x|}|+|u|} \cdot b \in P' \Leftrightarrow \\ x \cdot a_{|x|} \cdot u \cdot a'_{|x|+|a_{|x|}|+|0^{|u|}|} \cdot b \in P' \Leftrightarrow \\ x \cdot a_{|x|} \cdot u \cdot a'_{|x \cdot a_{|x|} \cdot 0^{|u|}|} \cdot b \in P' \Leftrightarrow \\ x \cdot a_{|x|} \cdot u \cdot z_{|u|} \cdot b \in P' \Leftrightarrow \\ x \cdot a_{|x|} \cdot 0^k \cdot z_0 \cdot z_1 \cdot ... \cdot z_k \cdot c \in P^* \Leftrightarrow \\ x \cdot a^*_{|x|} \cdot c \in P^* \quad \textbf{(8)}, \text{ εξ ορισμού της } P^*$$

(9): Συνδυάζοντας τις ισοδυναμίες των (7),(8) παίρνουμε:

$$\exists P^* \in \Pi_{i-1},\ \text{ακολουθία } a^* \text{ με } |a_n^*| \leq poly(n),\ \text{ώστε } \forall x :$$
$$x \in L \Leftrightarrow \exists c \in \{0,1\}^{p(|x|)+q(|x|)} \text{ ώστε } x \cdot a^*_{|x|} \cdot c \in P^*$$

Θέτουμε για ευκολία $t_1(n) = p(n) + q(n)$. Έστω M_{P^*} μηχανή Turing, t_2 πολυώνυμο ώστε:

$$x' \in P^* \Leftrightarrow \forall u_1 \in \{0,1\}^{t_2(|x'|)}\ \exists u_2 \in \{0,1\}^{t_2(|x'|)}\ ...\ Q_{i-1}u_{i-1} \in \{0,1\}^{t_2(|x'|)}$$
$$M_{P^*}(x', u_1, u_2, ..., u_{i-1}) = 1$$

(10): Ορίζουμε τώρα την S^* ως εξής: $y \in S^* \Leftrightarrow \exists c \in \{0,1\}^{t_1(|y|)}$ ώστε $y \cdot c \in P^*$

Ισοδύναμα έχουμε:

$\exists c \in \{0,1\}^{t_1(|y|)}\ \forall u_1 \in \{0,1\}^{t_2(|y|+t_1(|y|))}\ ...\ Q_{i-1}u_{i-1} \in \{0,1\}^{t_2(|y|+t_1(|y|))}$ με
$M_{P^*}(y \cdot c, u_1, u_2, ..., u_{i-1}) = 1 \Leftrightarrow \exists c \in \{0,1\}^{r(|y|)}\ \forall u_1 \in \{0,1\}^{r(|y|)}\ ...\ Q_{i-1}u_{i-1} \in \{0,1\}^{r(|y|)}$
με $M^*_{P^*}(y, c, u_1, u_2, ..., u_{i-1}) = 1$ **(11)**

όπου $r(n) = t_1(n) + t_2(n + t_1(n))$ πολυώνυμο και $M^*_{P^*}$ μηχανή Turing ίδια με την M_{P^*}, μόνο που το πρώτο όρισμα της M_{P^*} έχει σπάσει στα δύο πρώτα ορίσματα στην $M^*_{P^*}$ και η $M^*_{P^*}$ αγνοεί τα τελευταία $r(n) - t_1(n)$ bits του δεύτερου ορίσματός της, και τα τελευταία $r(n) - t_2(n + t_1(n))$ bits των υπολοίπων ορισμάτων της από το 3ο και μετά, όπου n το μήκος του εκάστοτε ορίσματος.

Όπως δείξαμε στην **(11)** θα είναι $S^* \in \Sigma_i$ και συνδυάζοντας τις ισοδυναμίες των **(9),(10)** και θέτοντας $y = x \cdot a^*_{|x|}$, παίρνουμε ότι $\exists S^* \in \Sigma_i$, ακολουθία a^*, με $|a_n^*| \leq poly(n)$, ώστε $\forall x$: $x \in L \Leftrightarrow x \cdot a^*_{|x|} \in S^*$, που είναι ακριβώς αυτό που θέλαμε, αφού εξ ορισμού παίρνουμε ότι $L \in \Sigma_i/poly$, και συνεπώς παίρνουμε το ζητούμενο.

■

Απόδειξη Λήμματος 6:

Η απόδειξη είναι από το [11].

Απόδειξη. Έστω ότι για κάποιο $i > 0$ έχουμε $\Sigma_i/poly = \Pi_i/poly$. Αφού προφανώς ισχύει $\Pi_i \subseteq \Pi_i/poly$, θα είναι λοιπόν $\Pi_i \subseteq \Sigma_i/poly$. Από το λήμμα 4 παίρνουμε ότι $\Sigma_i/poly = \Sigma_{i+1}/poly$. Συνεπώς όπως είχαμε αναφέρει η κυκλωματική ιεραρχία καταρρέει, θα είναι: $\Sigma_i/poly = \bigcup_{j>i}(\Sigma_j/poly) = (\bigcup_{j>i}\Sigma_j)/poly = PH/poly$. ■

Ορισμοί/Έννοιες για την απόδειξη του Λήμματος 7:

Αρχίζουμε με κάποιες έννοιες.

Έστω $L \subseteq \{0,1\}^*$. **Χαρακτηριστική συνάρτηση** της L είναι η συνάρτηση $C_L : \{0,1\}^* \to \{0,1\}$, όπου $\forall x \in \{0,1\}^*,\ C_L(x) = 1 \Leftrightarrow x \in L$.

Αυστηρή (strict) μέρικη διάταξη ενός συνόλου S είναι μία δυαδική σχέση $\prec$ ορισμένη πάνω στο S με τις εξής ιδιότητες:

1. Μη ανακλαστική (irreflexivity): $\forall a \in S$: $\neg(a \prec a)$
2. Ασυμμετρική (asymmetrical): $\forall a, b \in S$, με $a \prec b$ τότε $\neg(b \prec a)$
3. Μεταβατική (transitive): $\forall a, b, c \in S$, με $a \prec b$ και $b \prec c$, τότε και $a \prec c$

Επιπλέον, **ελαχιστικό στοιχείο** μιας αυστηρής μερικής διάταξης $(S, \prec)$, είναι ένα στοιχείο $s \in S$ για το οποίο: $\forall s' \in S : \neg(s' \prec s)$.

Καλά Θεμελιωμένη (Well Founded) ονομάζεται μια μερική διάταξη $(S, \prec)$ για την οποία κάθε μη κενό υποσύνολό του S έχει ελαχιστικό ως προς την $\prec$ στοιχείο. Δηλαδή ισχύει: $(\forall X \subseteq S)\ [X \neq \emptyset \Rightarrow \exists s \in X$ ώστε $\forall s' \in X : \neg(s' \prec s)]$.

Οι ορισμοί και η ανάλυση που ακολουθούν προέρχονται από τα [8], [11].

Για μια γλώσσα $L \subseteq \{0,1\}^*$, **Αναδρομική Δομή (Recursive Structure)** της L ονομάζουμε μια πλειάδα συναρτήσεων $(B, F_1, ..., F_r, G_1, ..., G_S)$ όπου $F_j : \{0,1\}^* \to \{0,1\},\ j \in [r]$, $G_k : \{0,1\}^* \to \{0,1\}^*,\ k \in [s]$, $B : \{0,1\}^{r+s} \to \{0,1\}$, με τις εξής ιδιότητες:

(1) $\forall x \in \{0,1\}^* : C_L(x) = B(F_1(x), ..., F_r(x), C_L(G_1(x)), ..., C_L(G_s(x)))$

(2) Υπάρχει μια καλά θεμελιωμένη, αυστηρή μερική διάταξη $(\{0,1\}, \prec)$ ώστε:

- (α□) $\forall x \in \{0,1\}^*$, $\forall k \in [s]$: είτε $G_k(x) \prec x$ είτε $G_k(x) = x$
- (β□) Ένα $x \in \{0,1\}^*$ είναι ελαχιστικό ως προς την $\prec$ αν και μόνο αν $\forall k \in [s]$ ισχύει ότι $G_k(x) = x$

(3) Εάν x ελαχιστικό ως προς την $\prec$ στοιχείο, τότε θα ισχύει:

$$B(F_1(x), ..., F_r(x), y_1, ..., y_s) = B(F_1(x), ..., F_r(x), y'_1, ..., y'_s),\ \forall y_k, y'_k \in \{0,1\},\ \text{με } k \in [s]$$

Επίσης αν οι F_j, G_k, B είναι και υπολογίσιμες σε πολυωνυμικό χρόνο, τότε λέμε ότι η L έχει πολυωνυμική αναδρομική δομή (polynomial recursive structure).

Για κάθε $i > 0$, ορίζουμε το πρόβλημα $\Pi_i SAT$ στο οποίο ανήκουν όλες οι ικανοποιήσιμες προτάσεις της μορφής: $\forall u_1 \exists u_2 ... Q_i u_i\ \phi(u_1, u_2, ..., u_i)$ όπου η ϕ είναι μια boolean φόρμουλα, ένα κατηγόρημα, ελεύθερο από ποσοδείκτες, της οποίας οι μεταβλητές εμπεριέχονται στα u_i, το Q_i είναι $\exists$ ή $\forall$ ανάλογα με το αν i άρτιος ή περιττός αντίστοιχα και κάθε u_i είναι ένα διάνυσμα boolean μεταβλητών.

Το $\Pi_i SAT$ είναι ως γνωστόν πλήρες πρόβλημα για την κλάση Π_i^p, για $i > 0$.

Επίσης το $\Pi_i SAT$ έχει πολυωνυμική αναδρομική δομή, όπως περιγράφεται στα [8], [11]. Συγκεκριμένα την (B, F_1, F_2, G_1, G_2) όπου:

- $F_1 : F_1(x) = 1 \Leftrightarrow$ το x είναι ένα έγκυρο στιγμιότυπο του $\Pi_i SAT$ και στο οποίο η ϕ δεν είναι σταθερή, δηλαδή, δεν δίνει μόνο 0 ή μόνο 1 ανεξάρτητα από τα ορίσματα της, κοινώς δεν είναι ούτε αντίφαση ούτε ταυτολογία.
- $F_2 : F_2(x) = 1 \Leftrightarrow$ το x είναι ένα έγκυρο στιγμιότυπο του $\Pi_i SAT$ και στο οποίο είτε η ϕ αποτιμάται πάντα σε 1 (κοινώς είναι ταυτολογία, πάντα αληθής), είτε η αριστερότερη μεταβλητή από τις $(u_1, u_2, .., u_i)$ που εμφανίζεται στην ϕ έχει υπαρξιακό ποσοδείκτη.

- $G_1 : G_1(x) = x$, εάν $F_1(x) = 0$, διαφορετικά εάν $F_1(x) = 1$, έχουμε $G_1(x) = y$, όπου y η πρόταση που προκύπτει αν αντικαταστήσουμε όλες τις εμφανίσεις της αριστερότερης μεταβλητής από τις $(u_1, u_2, ..., u_i)$ που εμφανίζεται στην ϕ, με το $0 \equiv$ Ψευδές.
- $G_2 : G_2(x) = x$, εάν $F_1(x) = 0$, διαφορετικά εάν $F_1(x) = 1$, έχουμε $G_2(x) = y$, όπου y η πρόταση που προκύπτει αν αντικαταστήσουμε όλες τις εμφανίσεις της αριστερότερης μεταβλητής από τις $(u_1, u_2, ..., u_i)$ που εμφανίζεται στην ϕ, με το $1 \equiv$ Αληθές.
- $B : B(x_1, x_2, y_1, y_2) = z$:
  - Αν $x_1 = 0$, $z = x_2$
  - Αν $x_1 = 1 \wedge x_2 = 1$, $z = y_1 \vee y_2$
  - Αν $x_1 = 1 \wedge x_2 = 0$, $z = y_1 \wedge y_2$

Οι G_k όπως είναι προφανές, με κατάλληλη κωδικοποίηση, μπορούν να διατηρούν το μήκος των ορισμάτων τους, δηλαδή να ισχύει $|G_k(x)| = |x|,\ \forall k \in \{1, 2\}$.

Εύκολα βλέπουμε ότι η συγκεκριμένη (B, F_1, F_2, G_1, G_2) πράγματι αποτελεί αναδρομική δομή για την $\Pi_i SAT$ αφού ικανοποιούνται οι ιδιότητες (1) , (2) , (3) του ορισμού παραπάνω. Συγκεκριμένα η (1) εύκολα προκύπτει ότι ισχύει, εκ κατασκευής των συναρτήσεων B, F_1, F_2, G_1, G_2 που ορίσαμε παραπάνω, παίρνοντας περιπτώσεις. Σε κάθε περίπτωση δείχνεται λοιπόν παρακάτω ότι ισχύει:

$$C_L(x) = B(F_1(x), ..., F_r(x), C_L(G_1(x)), ..., C_L(G_s(x))) = z$$

.

- **Περίπτωση 1:** Το x δεν είναι έγκυρο στιγμιότυπο του $\Pi_i SAT$.
  Τότε $C_L(x) = 0, F_1(x) = F_2(x) = 0$ και άρα θα είναι $z = F_2(x) = 0 = C_L(x)$.
- **Περίπτωση 2:** το x είναι έγκυρο στιγμιότυπο του $\Pi_i SAT$.
  - **Υποπερίπτωση 2.1:** Η ϕ είναι σταθερή, δηλαδή $F_1(x) = 0$.
    - **Υποπερίπτωση 2.1.1:** $\phi \equiv 1$, δηλαδή ϕ ταυτολογία.
      Τότε $C_L(x) = 1$, $F_2(x) = 1$ και θα είναι $z = F_2(x) = 1 = C_L(x)$.
    - **Υποπερίπτωση 2.1.2:** $\phi \equiv 0$, δηλαδή ϕ αντίφαση.
      Τότε $C_L(x) = 0$, και μπορούμε να υποθέσουμε ότι η αριστερότερη μεταβλητή που εμφανίζεται στην ϕ είναι καθολικά ποσοδεικτούμενη, αφού ούτως ή άλλως η ϕ είναι αντίφαση. Άρα παίρνουμε $F_2(x) = 0$ και θα είναι $z = F_2(x) = 0 = C_L(x)$.
  - **Υποπερίπτωση 2.2:** Η ϕ δεν είναι σταθερή, δηλαδή $F_1(x) = 1$.
    - **Υποπερίπτωση 2.2.1:** Η αριστερότερη μεταβλητή που εμφανίζεται στην ϕ έχει $\exists$ σαν ποσοδείκτη.
      Τότε $F_1(x) = 1$ και $F_2(x) = 1$ και άρα $z = C_L(G_1(x)) \vee C_L(G_2(x))$. Όπου $G_1(x), G_2(x)$ οι προτάσεις που προκύπτουν αν αντικαταστήσουμε όλες τις εμφανίσεις της αριστερότερης μεταβλητής με 0 ή 1 αντίστοιχα. Και επειδή η αριστερότερη μεταβλητή έχει υπαρξιακό ποσοδείκτη, η x θα είναι ικανοποιήσιμη αν και μόνο αν τουλάχιστον μία εκ των $G_1(x),\ G_2(x)$ είναι ικανοποιήσιμη δηλαδή πράγματι $C_L(x) = z$.

* **Υποπερίπτωση 2.2.2:** Η αριστερότερη μεταβλητή που εμφανίζεται στην ϕ έχει $\forall$ σαν ποσοδείκτη.
Τώρα $F_1(x) = 1$ και $F_2(x) = 0$ και άρα $z = C_L(G_1(x)) \wedge C_L(G_2(x))$. Τώρα όμως επειδή η αριστερότερη μεταβλητή έχει καθολικό ποσοδείκτη, η x θα είναι ικανοποιήσιμη αν και μόνο αν και οι δύο εκ των $G_1(x),\ G_2(x)$ είναι ικανοποιήσιμες, δηλαδή πράγματι $C_L(x) = z$.

Για την ιδιότητα (2), ορίζουμε: $\forall x \in \{0,1\}^*$ ως $free(x) \coloneqq$ το πλήθος των ελεύθερων (δηλαδή που δεν έχουν πάρει ακόμα τιμή) μεταβλητών από τις $u_1, ..., u_i$, από τα αριστερά προς τα δεξιά, που πρέπει να πάρουν τιμή ώστε η προκύπτουσα πρόταση να έχει σταθερό κατηγόρημα ϕ. Δηλαδή ώστε η προκύπτουσα ϕ να είναι σταθερή, είτε ταυτολογία είτε αντίφαση.

Για να είναι η $free : \{0,1\}^* \to \mathbb{N}$ καλά ορισμένη, θέτουμε $free(x) = 0$ για τα x τα οποία δεν είναι στιγμιότυπα του $\Pi_i SAT$. Παρατηρήστε ότι μια τέτοια μερική διάταξη που ικανοποιεί την ιδιότητα (2) θα μπορούσε να ήταν η εξής: $a \prec b \Leftrightarrow free(a) < free(b)$. Εύκολα βλέπουμε ότι η προκύπτουσα μερική διάταξη είναι αυστηρή, αφού ο τελεστής < προφανώς ικανοποιεί την μη-ανακλαστικότητα, μη συμμετρικότητα και μεταβατικότητα. Επίσης είναι και καλά δομημένη, αφού για οποιοδήποτε μη κενό υποσύνολο S του $\{0,1\}^*$, η εικόνα του μέσω της $free$ θα είναι ένα μη κενό υποσύνολο των φυσικών, άρα από αρχή ελαχίστου, θα υπάρχει ελάχιστο στοιχείο, του οποίου η αντίστροφη εικόνα θα είναι ελαχιστικό στοιχείο του S ως προς την $\prec$.

Πάμε για τις ιδιότητες (α), (β) τώρα.

Η (α) προκύπτει άμεσα ότι ισχύει από τον ορισμό των G_k και της $free$.

Για την (β), παρατηρήστε ότι από τους ορισμούς που δώσαμε για τα $F_j,\ G_k$ ισχύει ότι: $G_k(x) = x,\ \forall k \in [s] \Leftrightarrow F_1(x) = 0$. Άρα:

$(\Leftarrow)$: Έστω x ώστε $G_k(x) = x,\ \forall k \in [s]$. Τότε $F_1(x) = 0$, άρα είτε x όχι έγκυρο στιγμιότυπο του $\Pi_i SAT$ είτε η x έχει σταθερό κατηγόρημα, συνεπώς $free(x) = 0$, και άρα x ελαχιστικό στοιχείο ως προς την $\prec$.

$(\Rightarrow)$: Έστω x ελαχιστικό ως προς την $\prec$ στοιχείο. Τότε δεν υπάρχει y με $y \prec x$, άρα $F_1(x) = 0$ (διαφορετικά αν $F_1(x) = 1$ θα ήταν $G_k(x) \prec x$, άτοπο), συνεπώς $G_k(x) = x,\ \forall k \in [s]$.

Παρατηρήστε ότι σαν πόρισμα για την συγκεκριμένη μερική διάταξη παίρνουμε ότι x ελαχιστικό $\Leftrightarrow F_1(x) = 0$.

Τέλος, για την ιδιότητα (3) παρατηρήστε ότι αν x ελαχιστικό ως προς την $\prec$ στοιχείο, τότε από το παραπάνω πόρισμα, $F_1(x) = 0$, άρα θα ισχύει $B(F_1(x),\ F_2(x),\ \cdot\ ,\ \cdot) = F_2(x)$, ανεξάρτητο των δύο τελευταίων ορισμάτων, άρα $\forall y_k, y'_k \in \{0,1\}$, ισχύει αυτό που ζητάει η ιδιότητα (3).

Επίσης οι F_1, F_2, G_1, G_2, B είναι πολυωνυμικά υπολογίσιμες, άρα η παραπάνω αποτελεί πολυωνυμική αναδρομική δομή για την $\Pi_i SAT$.

Απόδειξη Λήμματος 7:

Η απόδειξη είναι από το [11].

Απόδειξη. Έστω ότι για κάποιο $i > 0$ ισχύει $\Sigma_i/poly = \Pi_i/poly$. Αρκεί να δείξουμε ότι $\Pi_{i+2}SAT \in \Sigma_{i+2}$. Και αυτό διότι ήδη ξέρουμε ότι $\Pi_{i+2}SAT$ πλήρες για την Π_{i+2}, δηλαδή $\forall L \in \Pi_{i+2},\ L \leq_m^p \Pi_{i+2}SAT$. Αν έχουμε και $\Pi_{i+2}SAT \in \Sigma_{i+2}$, τότε συνδυάζοντας αυτά τα δύο παίρνουμε ότι $\forall L \in \Pi_{i+2},\ L \in \Sigma_{i+2}$, δηλαδή $\Pi_{i+2} \subseteq \Sigma_{i+2}$. Και άρα παίρνουμε ότι τελικά πράγματι $\Sigma_{i+2} = \Pi_{i+2}$, αφού για οποιαδήποτε κλάση πολυπλοκότητας K ισχύει $K \subseteq co\text{-}K \Leftrightarrow K = co\text{-}K$.

Προς αυτήν την κατεύθυνση λοιπόν έχουμε:

$$\Pi_{i+2}SAT \in \Pi_{i+2} \subseteq \Pi_{i+2}/poly \subseteq PH/poly = \Pi_i/poly \text{ από λήμμα 6.}$$

Δηλαδή $\Pi_{i+2}SAT \in \Pi_i/poly$, από ορισμό:

$$\exists P \in \Pi_i, \text{ ακολουθία } a \text{ με } |a_n| \leq poly(n), \text{ ώστε } x \in \Pi_{i+2}SAT \Leftrightarrow x \cdot a_{|x|} \in P$$

Έστω επίσης (B, F_1, F_2, G_1, G_2) η πολυωνυμική αναδρομική δομή για την $\Pi_{i+2}SAT$, όπως την παρουσιάσαμε παραπάνω. Ορίζουμε το κατηγόρημα $W(x, w)$ ως εξής:

$$\forall y : |y| = |x| \Rightarrow C_P(y \cdot w) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot w), C_P(G_2(y) \cdot w))$$

Παρατηρήστε ότι ο έλεγχος του κατηγορήματος $W(x, w)$ ανήκει στο Π_{i+1}, αφού για να ελέγξουμε την συνεπαγωγή θέλουμε αποτιμήσεις των B, F_1, F_2, G_1, G_2 που είναι πολυωνυμικές, και σταθερό πλήθος αποτιμήσεων της χαρακτηριστικής συνάρτησης της P, που ανήκει στο Π_i. Ολόκληρος αυτός ο έλεγχος, έστω C, δηλαδή $W(x, w) = \forall y : C$, ανήκει στο Π_i και μαζί με τον καθολικό ποσοδείκτη y στην αρχή, παίρνουμε, συνενώνοντας το y με τον πρώτο ποσοδείκτη του C σε έναν ενιαίο πρώτο καθολικό ποσοδείκτη, ότι το $W(x, w)$ θα ανήκει στο Π_i και άρα και στο Π_{i+1}.

Επίσης παρατηρήστε ότι για οποιαδήποτε x, το $W(x, a_{|x|})$ αληθεύει. Πράγματι, από ιδιότητα (1) της πολυωνυμικής αναδρομικής δομής έχουμε:

$$C_{\Pi_{i+2}SAT}(x) = B(F_1(x), F_2(x), C_{\Pi_{i+2}SAT}(G_1(x)), C_{\Pi_{i+2}SAT}(G_2(x))) \quad (1^*)$$

Επίσης παρατηρήστε ότι:

$$C_{\Pi_{i+2}SAT}(x) = 1 \Leftrightarrow x \in \Pi_{i+2}SAT \Leftrightarrow x \cdot a_{|x|} \in P \Leftrightarrow C_P(x \cdot a_{|x|}) = 1$$

Δηλαδή θα είναι:

$$C_{\Pi_{i+2}SAT}(x) = C_P(x \cdot a_{|x|}) \quad (2^*)$$

Αντικαθιστώντας στην (1^*) την (2^*) και εφαρμόζοντας για τυχαίο y με $|y| = |x|$ παίρνουμε:

$$C_P(y \cdot a_{|y|}) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot a_{|G_1(y)|}), C_P(G_2(y) \cdot a_{|G_2(y)|}))$$

Επειδή οι G_k όπως είδαμε με κατάλληλη κωδικοποίηση διατηρούν το μήκος των ορισμάτων τους, δηλαδή $|G_k(y)| = |y|,\ \forall k \in \{1, 2\}$, ισοδύναμα έχουμε:

$C_P(y \cdot a_{|y|}) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot a_{|y|}), C_P(G_2(y) \cdot a_{|y|})) \Rightarrow$
$C_P(y \cdot a_{|x|}) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot a_{|x|}), C_P(G_2(y) \cdot a_{|x|})) \Rightarrow$
$C_P(y \cdot w) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot w), C_P(G_2(y) \cdot w))$ για $w = a_{|x|} \Rightarrow$
$W(x, a_{|x|})$ πράγματι αληθές.

Ισχυρισμός: $x \in \Pi_{i+2}SAT \Leftrightarrow \exists w \in \{0,1\}^{poly(|x|)}\ [x \cdot w \in P \wedge W(x,w)]$

Ο παραπάνω ισχυρισμός μας δίνει έναν χαρακτηρισμό για την $\Pi_{i+2}SAT$ μέσω μιας ισοδυναμίας, της οποίας το δεύτερο μέλος έχει έναν υπαρξιακό ποσοδείκτη, ακολουθούμενο από ένα κατηγόρημα το οποίο ανήκει στο Π_{i+1}, αφού $P \in \Pi_i \subseteq \Pi_{i+1}$ και όπως είδαμε και ο έλεγχος του $W(x,w)$ επίσης ανήκει στο Π_{i+1}. Συνεπώς παίρνουμε ότι ο έλεγχος του δεύτερου μέλους της ισοδυναμίας ανήκει στο Σ_{i+2}, συνεπώς και ο έλεγχος του πρώτου μέλους της ισοδυναμίας ανήκει στο Σ_{i+2}, δηλαδή παίρνουμε $\Pi_{i+2}SAT \in \Sigma_{i+2}$, που είναι αυτό που θέλουμε.

Απόδειξη Ισχυρισμού:

$(\Rightarrow)$: Έστω $x \in \Pi_{i+2}SAT$. Τότε από ορισμό θα είναι $x \cdot a_{|x|} \in P$ και όπως είδαμε το $W(x \cdot a_{|x|})$ είναι αληθές, και προφανώς $|a_{|x|}| \leq poly(|x|)$, άρα πολύ απλά θέτοντας $w = a_{|x|}$ έχουμε το ζητούμενο.

$(\Leftarrow)$: Έστω $x \in \{0,1\}^*$ και έστω $w \in \{0,1\}^{poly(|x|)}$ ώστε να ισχύει $x \cdot w \in P$ και $W(x \cdot w)$. Θα δείξουμε με επαγωγή ως προς την $\prec$ της αναδρομικής δομής, ότι:

$$\forall y,\ \text{με } |y| = |x| \text{ ισχύει } y \cdot w \in P \Leftrightarrow y \in \Pi_{i+2}SAT \quad (**)$$

Έχοντας την (**), για $y = x$, παίρνουμε ότι $x \in \Pi_{i+2}SAT$, το οποίο είναι αυτό που θέλουμε.

Βάση: Στην βάση της επαγωγής βρίσκονται τα ελαχιστικά ως προς την $\prec$ στοιχεία που έχουν ίδιο μήκος με το x. Αφού τα G_k διατηρούν το μήκος των ορισμάτων τους, θα υπάρχει σίγουρα ένα τέτοιο ελαχιστικό y, με $|y| = |x|$. Αρκεί να ακολουθήσουμε την πορεία του x προς τα πίσω, δηλαδή την ακολουθία $y_n \succ y_{n-1} \succ ... \succ y_1$, όπου $y_n = x$ και $y_{i-1} = G_k(y_i)$ για $k \in \{1,2\}$. Επειδή η $\prec$ είναι καλά δομημένη και εξ ορισμού των G_k, η παραπάνω ακολουθία-αλυσίδα, αφενός θα είναι πεπερασμένη, αφετέρου θα καταλήξει εν τέλει σε κάποιο ελαχιστικό στοιχείο της $\prec$, έστω το $y = y_1$, και επειδή θα ισχύει $|y_{i-1}| = |y_i|$, θα είναι $|y| = |x|$.

Έστω λοιπόν τώρα ένα στοιχείο y, ελαχιστικό ως προς την $\prec$, που να έχει ίδιο μήκος με το x. Θα ισχύει προφανώς όπως είδαμε:

$$C_P(y \cdot a_{|y|}) = C_{\Pi_{i+2}SAT}(y) = B(F_1(y), F_2(y), C_{\Pi_{i+2}SAT}(G_1(y)), C_{\Pi_{i+2}SAT}(G_2(y)))$$

Επίσης αφού ισχύει το $W(x,w)$ και $|y| = |x|$ από την συνεπαγωγή της $W(x,w)$ παίρνουμε:

$$C_P(y \cdot w) = B(F_1(y), F_2(y), C_P(G_1(y) \cdot w), C_P(G_2(y) \cdot w))$$

Επειδή όμως y ελαχιστικό, από ιδιότητα (3) του ορισμού της αναδρομικής δομής, θυμηθείτε ότι τα ορίσματα πέραν των F_j δεν επηρεάζουν την τιμή της B, συνεπώς οι δύο παραπάνω ποσότητες είναι ίσες, δηλαδή $C_P(y \cdot a_{|y|}) = C_P(y \cdot w)$. Τότε θα είναι:

$$y \in \Pi_{i+2}SAT \Leftrightarrow C_{\Pi_{i+2}SAT}(y) = 1 \Leftrightarrow C_P(y \cdot a_{|y|}) = 1 \Leftrightarrow C_P(y \cdot w) = 1 \Leftrightarrow y \cdot w \in P$$

Δηλαδή πράγματι ισχύει η (**).

Επαγωγική Υπόθεση: Έστω ότι ισχύει η (**) για όλα τα στοιχεία y που απέχουν $i \geq 0$ ως προς την $\prec$, από ελαχιστικό στοιχείο της $\prec$, και $|y| = |x|$.

Επαγωγικό Βήμα: Έστω y' που απέχει $i+1$ ως προς την $\prec$ από κάποιο ελαχιστικό στοιχείο της $\prec$ και είναι $|y'| = |x|$. Θα δείξουμε ότι ισχύει η (**) και για το y'. Αφού y' όχι ελαχιστικό, $F_1(y') = 1$, άρα υπάρχουν y_1, y_2 με $y_1 = G_1(y')$ και $y_2 = G_2(y')$ και προφανώς θα είναι $y_1 \prec y'$ και $y_2 \prec y'$, άρα από επαγωγική υπόθεση θα ισχύουν:

$$y_1 \in \Pi_{i+2}SAT \Leftrightarrow C_P(y_1 \cdot w) = 1 \text{ και } y_2 \in \Pi_{i+2}SAT \Leftrightarrow C_P(y_2 \cdot w) = 1$$

Επειδή ισχύει το $W(x, w)$ και $|y'| = |x|$ από την συνεπαγωγή της $W(x, w)$ παίρνουμε:

$$C_P(y' \cdot w) = B(F_1(y'), F_2(y'), C_P(G_1(y') \cdot w), C_P(G_2(y') \cdot w)) =$$
$$B(F_1(y'), F_2(y'), C_P(y_1 \cdot w), C_P(y_2 \cdot w))$$

Περίπτωση 1: $F_2(y') = 1$, δηλαδή ο αριστερότερος ποσοδείκτης στην y' είναι $\exists$.

Τότε από ορισμό της B αφού $F_1(y') = F_2(y') = 1$, θα είναι:

$B(F_1(y'), F_2(y'), C_P(y_1 \cdot w), C_P(y_2 \cdot w)) = C_P(y_1 \cdot w) \vee C_P(y_2 \cdot w)$ επομένως έχουμε:

$$y' \cdot w \in P \Leftrightarrow C_P(y' \cdot w) = 1 \Leftrightarrow B(F_1(y'), F_2(y'), C_P(y_1 \cdot w), C_P(y_2 \cdot w)) = 1 \Leftrightarrow$$
$$C_P(y_1 \cdot w) \vee C_P(y_2 \cdot w) = 1 \Leftrightarrow C_P(y_1 \cdot w) = 1 \ \vee \ C_P(y_2 \cdot w) = 1 \Leftrightarrow^{\text{EY}}$$
$$y_1 \in \Pi_{i+2}SAT \ \vee \ y_2 \in \Pi_{i+2}SAT \Leftrightarrow y' \in \Pi_{i+2}SAT$$

αφού οι y_1, y_2 θυμίζουμε προκύπτουν αντικαθιστώντας όλες τις εμφανίσεις της αριστερότερης μεταβλητής στην y' με 0,1 αντίστοιχα και η αριστερότερη μεταβλητή στην y' είναι από υποθεση υπαρξιακά ποσοδεικτούμενη. Άρα ισχύει η (**).

Περίπτωση 2: $F_2(y') = 0$, δηλαδή ο αριστερότερος ποσοδείκτης στην y' είναι $\forall$.

Τότε, εντελώς συμμετρικά με την πρώτη περίπτωση, από ορισμό της B αφού $F_1(y') = 1, F_2(y') = 0$, θα είναι:

$B(F_1(y'), F_2(y'), C_P(y_1 \cdot w), C_P(y_2 \cdot w)) = C_P(y_1 \cdot w) \wedge C_P(y_2 \cdot w)$ επομένως έχουμε:

$$y' \cdot w \in P \Leftrightarrow C_P(y' \cdot w) = 1 \Leftrightarrow B(F_1(y'), F_2(y'), C_P(y_1 \cdot w), C_P(y_2 \cdot w)) = 1 \Leftrightarrow$$
$$C_P(y_1 \cdot w) \wedge C_P(y_2 \cdot w) = 1 \Leftrightarrow C_P(y_1 \cdot w) = 1 \ \wedge \ C_P(y_2 \cdot w) = 1 \Leftrightarrow^{\text{EY}}$$
$$y_1 \in \Pi_{i+2}SAT \ \wedge \ y_2 \in \Pi_{i+2}SAT \Leftrightarrow y' \in \Pi_{i+2}SAT$$

αφού τώρα η αριστερότερη μεταβλητή της y' είναι καθολικά ποσοδεικτούμενη από υπόθεση. Άρα πάλι ισχύει η (**).

Συνεπώς από επαγωγή, πράγματι ισχύει η (**) για όλα τα y με ίδιο μήκος με το x, άρα και για το ίδιο το x. Άρα απεδείχθη ο ισχυρισμός και κατ'επέκταση όπως επιχειρηματολογήσαμε το ζητούμενο. ■

Β. ΠΑΡΑΡΤΗΜΑ ΙΙ

Απόδειξη Λήμματος Ισοδυναμίας

Η απόδειξη είναι από το [4].

Απόδειξη. $(\Leftarrow)$: Αφού L πυρηνοποιήσιμη, υπάρχει πολυωνυμική αναγωγή και υπολογίσιμη συνάρτηση h, ώστε από το (x,k) στιγμιότυπο της L να παίρνουμε ένα ισοδύναμο στιγμιότυπο της L, το οποίο θα έχει μέγεθος το πολύ $h(k)$. Επειδή L αποφασίσιμη, θα υπάρχει υπολογίσιμη συνάρτηση g, η οποία θα επιλύει το ανηγμένο στιγμιότυπο. Έτσι για να αποφασιστεί εάν $(x,k) \in L$, παίρνουμε έναν αλγόριθμο χρόνου $O(g(h(k)) + poly(|(x,k)|))$, με $g \circ h$ υπολογίσιμη συνάρτηση που εξαρτάται μόνο από το k. Και επειδή προφανώς ισχύει $O(g(h(k)) + poly(|(x,k)|)) \subseteq O(f(k) \cdot poly(|(x,k)|))$, παίρνουμε ότι $L \in FPT$.

$(\Rightarrow)$: Έστω $L \in FPT$, αλγόριθμος χρόνου $O(f(k) \cdot poly(|(x,k)|))$, που να αποφασίζει εάν $(x,k) \in L$, και έστω $poly(|(x,k)|) = |(x,k)|^c$. Προφανώς L αποφασίσιμη, μένει να δείξουμε ότι είναι και πυρηνοποιήσιμη. Αν $L = \emptyset$ ή $L = \{0,1\}^*$, τότε η L είναι τετριμμένα πυρηνοποιήσιμη. Διαφορετικά, υπάρχουν στιγμιότυπα I_0, I_1 τέτοια ώστε $I_0 \notin L$ και $I_1 \in L$. Θεωρούμε την εξής αναγωγή τ για την παραγωγή του πυρήνα: Με είσοδο (x,k) στιγμιότυπο της L, τρέξε τον $O(f(k) \cdot poly(|(x,k)|))$ αλγόριθμο για $|(x,k)|^{c+1}$ βήματα. Αν τερματίσει εντός των $|(x,k)|^{c+1}$ βημάτων σε κατάσταση αποδοχής, θέσε $\tau((x,k)) = I_1$. Αν τερματίσει εντός των $|(x,k)|^{c+1}$ βημάτων σε κατάσταση απόρριψης, θέσε $\tau((x,k)) = I_0$. Αν δεν τερματίσει εντός των $|(x,k)|^{c+1}$ βημάτων, θέσε $\tau((x,k)) = (x,k)$.

Προφανώς η τ τρέχει σε πολυωνυμικό χρόνο ως προς το μέγεθος της εισόδου $|(x,k)|$. Επίσης προφανώς σε κάθε περίπτωση ισχύει $(x,k) \in L \Leftrightarrow \tau((x,k)) \in L$.

Τώρα πρέπει και $|\tau((x,k))| \leq h(k)$, για κάποια υπολογίσιμη συνάρτηση h.

Αρκεί $h(k) = max\{|I_0|, |I_1|, f(k)\}$. Η συγκεκριμένη h είναι υπολογίσιμη αφού I_0, I_1 είναι δεδομένα και f υπολογίσιμη από υπόθεση. Επίσης σε κάθε περίπτωση θα ισχύει ότι $|\tau((x,k))| \leq h(k)$, αφού είτε $|\tau((x,k))| = |I_0| \leq h(k)$, είτε $|\tau((x,k))| = |I_1| \leq h(k)$, είτε $|\tau((x,k))| = |(x,k)|$ με $f(k) \cdot |(x,k)|^c \geq |(x,k)|^{c+1}$ αφού δεν τερματίζει εντός $|(x,k)|^{c+1}$ βημάτων, και συνεπώς πάλι $|\tau((x,k))| = |(x,k)| \leq f(k) \leq h(k)$. Τέλος η ύπαρξη συνάρτησης g η οποία επιλύει το στιγμιότυπο του πυρήνα (δηλαδή το I_0, I_1 ή (x,k)) προκύπτει από το ότι $L \in FPT$. Δείξαμε λοιπόν ότι L πυρηνοποιήσιμη. ■

Πυρηνοποίηση για το 2-VERTEX-COVER

Παρουσιάζουμε εδώ την πυρηνοποίηση του προβλήματος του καλύμματος κορυφών για τα κλασικά γραφήματα, παραμετροποιημένο ως προς το μέγεθος του καλύμματος κορυφών. Η πυρηνοποίηση που παρουσιάζεται είναι αυτή που προτάθηκε από τον J.F.Buss [2]. Η βασική ιδέα είναι ότι δεδομένου ενός στιγμιότυπου (G,k) του προβλήματος, αφαιρούμε διαδοχικά κορυφές από το γράφημα βαθμού μεγαλύτερου του k, διότι αυτές οι κορυφές σίγουρα θα ανήκουν σε οποιοδήποτε κάλυμμα κορυφών μεγέθους το πολύ k. Το προκύπτον στιγμιότυπο, θα έχει μέγεθος που εξαρτάται μόνο από την παράμετρο k.

Παρακάτω παρουσιάζεται ο αλγόριθμος της πυρηνοποίησης και σκιαγραφείται η απόδειξη ορθότητας του, ακολουθώντας το [6]:

Algorithm 1 Buss(G,k) : Vertex Cover Kernelization of Buss

Require: G,k ▷ Γράφημα G και μέγεθος του vertex cover k

$I(G) \leftarrow$ απομονωμένες κορυφές του G

if $k=0$ και $I(G)=V(G)$ **then** return I_1 ▷ (1)

end if

if $k=0$ και $I(G)\neq V(G)$ **then** return I_0 ▷ (2)

end if

if $\exists v \in V(G)$ με $deg_G(v) > k$ **then** return Buss$(G-v,k-1)$ ▷ (3)

end if

if $|V(G)-I(G)| > k\cdot(k+1)$ **then** return I_0 ▷ (4)

end if

if $|E(G)| > k^2$ **then** return I_0 ▷ (5)

end if

if G έχει $> k$ μη τετριμμένες συνεκτικές συνιστώσες **then** return I_0 ▷ (6)

end if

return $(G[V(G)-I(G)],k)$ ▷ (7)

Σχήμα Β□.1: Αλγόριθμος πυρηνοποίησης του Buss για το Vertex Cover

Τα I_0, I_1, αντιστοιχούν σε αρνητικά και καταφατικά στιγμιότυπα του προβλήματος του Vertex Cover αντίστοιχα. Θυμηθείτε ότι ο αλγόριθμος της πυρηνοποίησης ουσιαστικά έχει σαν έξοδο ένα στιγμιότυπο του ίδιου προβλήματος, ισοδύναμου με αυτό στην είσοδο.

Για την ορθότητα αρκεί λοιπόν να δείξουμε ότι σε κάθε περίπτωση : (G,k) καταφατικό στιμιότυπο του Vertex Cover $\Leftrightarrow Buss(G,k)$ καταφατικό στιγμιότυπο του Vertex Cover. Για την ορθότητα λοιπόν παρατηρήστε τα εξής:

1. Στην πρώτη περίπτωση έχουμε ότι $k=0$ και ότι $I(G)=V(G)$ δηλαδή όλες οι κορυφές του G είναι απομονωμένες. Σε αυτήν την περίπτωση πράγματι το G έχει κάλυμμα κορυφών μεγέθους μηδέν, και άρα επιστρέφεται ένα ισοδύναμο καταφατικό στιγμιότυπο I_1.

2. Στην δεύτερη περίπτωση έχουμε ότι $k=0$ και ότι $I(G)\neq V(G)$ δηλαδή δεν είναι όλες οι κορυφές του G απομονωμένες, υπάρχει δηλαδή ακμή στο G και άρα το G δεν έχει κάλυμμα κορυφών μεγέθους μηδέν, και άρα επιστρέφεται ένα ισοδύναμο αρνητικό στιγμιότυπο I_0.

3. Στην τρίτη περίπτωση έχουμε $k>0$ και ότι υπάρχει κορυφή v στο G βαθμού αυστηρά μεγαλύτερου του k. Παρατηρήστε ότι η v, θα ανήκει υποχρεωτικά σε οποιοδήποτε κάλυμμα κορυφών S μεγέθους το πολύ k του G. Διαφορετικά, οι γείτονες αυτής της κορυφής θα έπρεπε να ανήκουν στο κάλυμα κορυφών, δηλαδή θα ήταν $N(v)\subseteq S$, άτοπο αφού $|N(v)| > k \geq |S|$. Επίσης, από αυτήν την παρατήρηση προκύπτει ότι το G έχει κάλυμμα κορυφών μεγέθους $k \Leftrightarrow$ το $G-v$, το γράφημα που προκύπτει από την αφαίρεση της v και των ακμών προσκείμενων στην v, έχει κάλυμμα κορυφών μεγέθους $k-1$. Άρα ορθά επιστρέφεται το ισοδύναμο στιγμιότυπο $Buss(G-v,k-1)$.

4. Στην τέταρτη περίπτωση έχουμε $k>0$ και ότι δεν υπάρχει κορυφή βαθμού αυστηρά μεγαλύτερου του k στο G. Δηλαδή είναι $\Delta(G)\leq k$, όπου με $\Delta(G)$ συμβολίζεται ο μέγιστος βαθμός του G. Παρατηρήστε ότι αν το G είχε και κάλυμμα κορυφών S μεγέθους το πολύ k, επειδή οποιαδήποτε μη απομονωμένη κορυφή του G είτε θα ανήκει στο S είτε θα συνδέεται με ακμή με κάποιον κόμβο του S, θα είναι $S\cup N(S)\supseteq V(G)-I(G)$, και δηλαδή: $|V(G)-I(G)|\leq |S\cup N(S)|\leq |S|+|N(S)|\leq |S|+|S|\cdot\Delta(G)\leq k+k\cdot k=$

$k + k^2 = k(k + 1)$. Συνεπώς αν είναι $|V(G) - I(G)| > k(k + 1)$, δεν γίνεται να υπάρχει στο G κάλυμμα κορυφών μεγέθους το πολύ k και άρα ορθά επιστρέφεται ένα ισοδύναμο αρνητικό στιγμιότυπο I_0.

5. Στην πέμπτη περίπτωση, έχουμε $k > 0$ και ότι πάλι $\Delta(G) \leq k$. Παρατηρήστε ότι αν το G είχε κάλυμμα κορυφών S μεγέθους το πολύ k, τότε επειδή οι $|S|$ κόμβοι του καλύμματος κορυφών καλύπτουν το πολύ $|S| \cdot \Delta(G) \leq k^2$ ακμές, αν ήταν $|E(G)| > k^2$, τότε δεν γίνεται να υπάρχει τέτοιο S, άρα ορθά επιστρέφεται ισόδυναμο αρνητικό στιγμιότυπο I_0.

6. Στην έκτη περίπτωση, αν το G έχει αυστηρά περισσότερες από k μη τετριμμένες (με τουλάχιστον 2 κόμβους) συνεκτικές συνιστώσες, θα έπρεπε τουλάχιστον ένας κόμβος από κάθε συνεκτική συνιστώσα να άνηκε σε οποιοδήποτε κάλυμμα κορυφών, άρα δεν νοείται κάλυμμα κορυφών του G μεγέθους το πολύ k και άρα ορθά επιστρέφεται ένα ισοδύναμο αρνητικό στιγμιότυπο I_0.

7. Απλά αφαιρούνται οι απομονώμενες κορύφες, που προφανώς δεν επηρεάζουν την ύπαρξη ούτε το μέγεθος ενός καλύμματος κορυφών.

Ως προς τον χρόνο εκτέλεσης του αλγορίθμου της πυρηνοποίησης, ο χρόνος $T(G, k)$ για την $Buss(G, k)$ είναι $O(|V(G)|)$ για τα βήματα πλην του 3, συν ενδεχομένως τον χρόνο $T(G-v, k-1)$ της αναδρομικής κλήσης $Buss(G-v, k-1)$. Άρα στην χειρότερη περίπτωση θα είναι $T(G, k) = T(G - v, k - 1) + O(|V(G)|)$, το οποίο δίνει $T(G, k) = O(k \cdot |V(G)|) = O(|V(G)|^2)$, πολυωνυμικός ως προς την είσοδο όπως θέλουμε.

Ως προς το μέγεθος του προκύπτοντος στιγμιότυπου, παρατηρήστε ότι ο αλγόριθμος πυρηνοποίησης επιστρέφει είτε I_0 είτε I_1 είτε ένα στιγμιότυπο (G', k') όπου $\Delta(G') \leq k$ και $|V(G')| \leq k(k + 1)$ και $|E(G')| \leq k^2$, άρα $|V(G')| = O(k^2)$ και $|E(G')| = O(k^2)$, δηλαδή το προκύπτον στιγμιότυπο σε κάθε περίπτωση έχει μέγεθος φραγμένο από μια υπολογίσιμη συνάρτηση εξαρτώμενη μόνο από την παράμετρο k, αφού θα είναι $|(G', k')| = O(k^2)$. Όπως είδαμε αυτό το μέγεθος του πυρήνα είναι το μικρότερο δυνατό που μπορούμε να πετύχουμε δεδομένου ότι η πολυωνυμική ιεραρχία δεν καταρρέει.

Έπειτα το προκύπτον στιγμιότυπο μπορεί να λυθεί εξαντλητικά, διατρέχοντας όλα τα υποσύνολα κορυφών του πυρήνα και ελέγχοντας αν αυτά αποτελούν κάλυμμα κορυφών. Υπάρχουν $2^{|V(G')|} = 2^{O(k^2)}$ τέτοια υποσύνολα και καθένα χρειάζεται χρόνο $O(|E(G')|) = O(k^2)$ για να ελεγχθεί αν είναι κάλυμμα κορυφών, άρα συνολικά ο πυρήνας επιλύεται σε χρόνο της τάξης του $k^2 \cdot 2^{O(k^2)}$, δίνοντας στο πρόβλημα του καλύμματος κορυφών έναν χρόνο εκτέλεσης της μορφής: $O(|V(G)|^2) + k^2 \cdot 2^{O(k^2)}$ για να αποφασιστεί ένα στιγμιότυπο (G, k).

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[2] Jonathan F Buss and Judy Goldsmith. Nondeterminism within p^. *SIAM Journal on Computing*, 22(3):560--572, 1993.

[3] H Christos. Papadimitriou: Computational complexity. *Addison-Wesley*, 2(3):4, 1994.

[4] Marek Cygan, Fedor V Fomin, Łukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michał Pilipczuk, and Saket Saurabh. *Parameterized algorithms*, volume 5. Springer, 2015.

[5] Holger Dell and Dieter Van Melkebeek. Satisfiability allows no nontrivial sparsification unless the polynomial-time hierarchy collapses. *Journal of the ACM (JACM)*, 61(4):1--27, 2014.

[6] Josep Díaz, Jordi Petit, and Dimitrios M Thilikos. Kernels for the vertex cover problem on the preferred attachment model. In *International Workshop on Experimental and Efficient Algorithms*, pages 231--240. Springer, 2006.

[7] Fedor V Fomin, Daniel Lokshtanov, Saket Saurabh, and Meirav Zehavi. *Kernelization: theory of parameterized preprocessing*. Cambridge University Press, 2019.

[8] Richard M Karp and Richard J Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the twelfth annual ACM symposium on Theory of computing*, pages 302--309, 1980.

[9] Raphaël Salem and Donald C Spencer. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 28(12):561--563, 1942.

[10] Michael Sipser. Introduction to the theory of computation. 2021.

[11] Chee K Yap. Some consequences of non-uniform conditions on uniform classes. *Theoretical computer science*, 26(3):287--300, 1983.