ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

# Εφαρμογές της Λογικής σε Αλγορίθμους Μέτρησης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σωτήριος Γ. Κανελλόπουλος

**Επιβλέπων :** Αριστείδης Παγουρτζής
Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2022

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

# Εφαρμογές της Λογικής σε Αλγορίθμους Μέτρησης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σωτήριος Γ. Κανελλόπουλος

**Επιβλέπων :** Αριστείδης Παγουρτζής

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την $18^{η}$ Ιουλίου 2022.

| ............................ | ............................ | ............................ |
|---|---|---|
| Αριστείδης Παγουρτζής | Δημήτριος Φωτάκης | Γεώργιος Στάμου |
| Καθηγητής Ε.Μ.Π. | Αν. Καθηγητής Ε.Μ.Π. | Καθηγητής Ε.Μ.Π. |

Αθήνα, Ιούλιος 2022

...................................

Σωτήριος Γ. Κανελλόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

**ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ**

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

..................................

Σωτήριος Γ. Κανελλόπουλος

# **Περίληψη**

Σκοπός της παρούσας εργασίας είναι να μελετήσουμε χρήσιμες εφαρμογές της λογικής στη θεωρία αλγορίθμων και υπολογιστικής πολυπλοκότητας. Θα επικεντρωθούμε κυρίως στο πεδίο της περιγραφικής πολυπλοκότητας, ξεκινώντας από λογικές περιγραφές για κλάσεις προβλημάτων απόφασης (π.χ. τις P και NP) και στη συνέχεια επεκτείνοντας αυτές και για κλάσεις προβλημάτων μέτρησης. Όπως θα δούμε, οι λογικές περιγραφές αυτές χρησιμεύουν για την ταξινόμηση προβλημάτων σε κλάσεις, καθώς και τη μελέτη ιδιοτήτων των κλάσεων πολυπλοκότητας. Μάλιστα, σε ορισμένες περιπτώσεις μάς παρέχουν και εγγυήσεις για την ιεραρχία κάποιων κλάσεων. Παρουσιάζει ενδιαφέρον το γεγονός ότι με τη χρήση τέτοιων λογικών περιγραφών μπορεί ένα πρόβλημα να καταταγεί σε κλάσεις υπολογιστικής δυσκολίας μόνο από την εκφραστικότητα που χρειάζεται για να περιγραφεί η εκφώνησή του, χωρίς να μελετηθούν αλγόριθμοι για το αντίστοιχο πρόβλημα. Για μετρητικά προβλήματα, θα δούμε ότι η ύπαρξη αποδοτικών αλγορίθμων είναι σπάνια και για αυτό συνήθως στρεφόμαστε προς προσεγγιστικούς αλγορίθμους. Με βάση τις λογικές περιγραφές που έχουν δοθεί για την κλάση #P, μπορούν να δοθούν κάποιες εγγυήσεις για το ποια προβλήματα μέτρησης διαθέτουν προσεγγιστικό αλγόριθμο FPRAS. Κατ’ αναλογία με τις ήδη γνωστές λογικές περιγραφές που υπάρχουν για τις κλάσεις NP και #P, θα δώσουμε παρόμοιες περιγραφές για κάποιες λιγότερο μελετημένες κλάσεις που είναι συναφείς με μετρητικά προβλήματα. Αυτές οι περιγραφές μπορούν να φανούν χρήσιμες για την ιεράρχηση αυτών των κλάσεων, καθώς και για εναλλακτικές αποδείξεις ιδιοτήτων τους (π.χ. για το αν μια κλάση είναι κλειστή ως προς τομή).



Λέξεις Κλειδιά:

Λογική, Περιγραφική Πολυπλοκότητα, Προσεγγιστικοί Αλγόριθμοι, Κλάσεις Πολυπλοκότητας, Προβλήματα Μέτρησης

## Abstract

The purpose of this paper is to study useful applications of logic in the theory of algorithms and computational complexity. We will focus mainly on the field of descriptive complexity, starting with logical descriptions for classes of decision problems (e.g., P and NP) and then extending these for classes of counting problems. As we will see, these logical descriptions serve to classify problems into classes, as well as to study properties of complexity classes. In fact, in certain cases they also provide us with guarantees for the hierarchy of some classes. It is interesting that with the use of such logical descriptions, a problem can be classified into classes of computational difficulty only by the expressiveness needed to describe it, without studying algorithms for the corresponding problem. For counting problems, we will see that the existence of efficient algorithms is rare, and so we usually turn to approximate algorithms. Based on the logical descriptions given for the #P class, some guarantees can be given about which counting problems have an FPRAS. By analogy with the already known logical descriptions that exist for the classes NP and #P, we will give similar descriptions for some less studied classes that are relevant to counting problems. These descriptions can be useful for studying the hierarchy of such classes, as well as for alternative proofs of their properties (e.g., whether a class is closed under intersection).



Keywords:

Logic, Descriptive Complexity, Approximation Algorithms, Complexity Classes, Counting Problems

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα κ. Αριστείδη Παγουρτζή, καθηγητή Ε.Μ.Π., και την υποψήφια διδάκτορα Αγγελική Χαλκή, για την πολύτιμη βοήθεια που μου προσέφεραν στην παροχή σχετικής βιβλιογραφίας και στην κατανόηση εννοιών επί του θέματος, καθώς και για τις χρήσιμες παρατηρήσεις τους προς βελτίωση της μορφής και του περιεχομένου της εργασίας.

Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους διδάσκοντες της σχολής, χάριν στους οποίους έφτασα στο σημείο που βρίσκομαι τώρα. Ευχαριστώ ειδικά τον κ. Πέτρο Ποτίκα, Ε.ΔΙ.Π. Ε.Μ.Π., με τον οποίο συνεργάστηκα για τη συγγραφή μίας προηγούμενης προπτυχιακής εργασίας, στο μάθημα «Εφαρμογές της Λογικής στην Πληροφορική».

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου και τους φίλους μου για την πολύτιμη και διαρκή υποστήριξη που μου παρείχαν όλα αυτά τα χρόνια.

Αθήνα, Ιούλιος 2022

*Σωτήρης Κανελλόπουλος*

# Περιεχόμενα

# 1. Εισαγωγή

Όταν εξετάζουμε την πολυπλοκότητα ενός αλγόριθμου, συνήθως ενδιαφερόμαστε για το χώρο και το χρόνο που απαιτεί η εκτέλεσή του. Με βάση αυτά τα κριτήρια συνηθίζουμε να ταξινομούμε προβλήματα σε κλάσεις πολυπλοκότητας, όπως οι $P$ και $NP$. Θα υπενθυμίσουμε τους αυστηρούς ορισμούς αυτών των κλάσεων:

Ορισμός (Κλάση $P$)

Η κλάση πολυπλοκότητας $P$ ορίζεται ως το σύνολο προβλημάτων απόφασης που επιλύονται σε πολυωνυμικό χρόνο από ντετερμινιστική μηχανή Turing.

Ορισμός (Κλάση $NP$)

Η κλάση πολυπλοκότητας $NP$ ορίζεται ως το σύνολο προβλημάτων απόφασης των οποίων μια λύση μπορεί να *επιβεβαιωθεί* σε πολυωνυμικό χρόνο από ντετερμινιστική μηχανή Turing.

Ισοδύναμα, μπορούμε να ορίσουμε την κλάση $NP$ και ως το σύνολο προβλημάτων απόφασης που επιλύονται σε πολυωνυμικό χρόνο από *μη ντετερμινιστική* μηχανή Turing.

Ενδιαφέρον παρουσιάζει το γεγονός ότι τέτοιου είδους κλάσεις φαίνεται να μην διαμορφώνονται αποκλειστικά από τις απαιτήσεις των προβλημάτων τους σε χρόνο και χώρο. Όπως έχει αποδειχτεί από τον Ronald Fagin, η κλάση πολυπλοκότητας $NP$ περιέχει ακριβώς τα προβλήματα που μπορούν να περιγραφούν σε *υπαρξιακή λογική δεύτερης τάξης* (*existential second-order logic*). Το θεώρημα του Fagin δίνει μια πολύ σημαντική σύνδεση ανάμεσα σε λογική και πολυπλοκότητα. Ουσιαστικά μας οδηγεί στη διαπίστωση ότι η υπολογιστική δυσκολία ενός προβλήματος σχετίζεται με την *εκφραστικότητα* της γλώσσας που χρειαζόμαστε για να το περιγράψουμε.

Γύρω από αυτό το σκεπτικό γεννήθηκε το πεδίο της *περιγραφικής πολυπλοκότητας* (*descriptive complexity*), στο οποίο γίνεται προσπάθεια ταξινόμησης κλάσεων πολυπλοκότητας σύμφωνα με το είδος της λογικής που απαιτείται για την περιγραφή των γλωσσών τους. Μια τέτοιου είδους μελέτη ενδεχομένως να φανεί χρήσιμη στην απάντηση ερωτημάτων σχετικά με κλάσεις πολυπλοκότητας (π.χ. το περίφημο πρόβλημα για το αν οι κλάσεις $P$ και $NP$ ταυτίζονται) από μια πιο μαθηματική σκοπιά. Επιπλέον, η περιγραφική πολυπλοκότητα έχει εφαρμογές στη θεωρία βάσεων δεδομένων (database theory), καθώς τα queries που χρησιμοποιούνται σε βάσεις δεδομένων συνήθως εκφράζονται σε γλώσσες που μοιάζουν με λογική πρώτης τάξης.

Στα πλαίσια αυτής της εργασίας θα μελετήσουμε αποτελέσματα που έχουν προκύψει με χρήση περιγραφικής πολυπλοκότητας για *προβλήματα απόφασης* (decisional problems) και στη συνέχεια θα επεκταθούμε και σε *προβλήματα μέτρησης* (counting problems), στα οποία μας ενδιαφέρει να προσδιορίζουμε το πλήθος των δυνατών λύσεων ενός προβλήματος. Για αυτό το σκοπό θα ασχοληθούμε και με κλάσεις πολυπλοκότητας προβλημάτων μέτρησης (κυρίως την $\#P$). Θα μελετήσουμε μερικές σημαντικές έννοιες για αυτές τις κλάσεις, όπως την πληρότητα, και θα προσπαθήσουμε να κατανοήσουμε την υπολογιστική δυσκολία των αντίστοιχων προβλημάτων. Σε πολλές περιπτώσεις θα αντιμετωπίσουμε μετρητικά προβλήματα που αποτελούν επεκτάσεις γνωστών μας προβλημάτων από τις κλάσεις $P$ και $NP$. Επιπλέον, θα ασχοληθούμε και με προσεγγίσεις (approximation schemes) για μετρητικά προβλήματα που σχετίζονται με λογική.

Στο κεφάλαιο 7 θα γίνει μια προσπάθεια να οριστούν λογικές περιγραφές για κάποιες λιγότερο μελετημένες κλάσεις πολυπλοκότητας. Οι περιγραφές αυτές ορίζονται κατ’ αναλογία με τη λογική περιγραφή της κλάσης $NP$ από το θεώρημα του Fagin, καθώς και τις περιγραφές μετρητικών κλάσεων, όπως η $\#P$.

Σημειώνουμε ότι έχει γίνει σημαντική προσπάθεια να εξηγηθούν με προσιτό τρόπο όσα προαπαιτούμενα χρειάζεται ένας αναγνώστης για να κατανοήσει την ουσία της εργασίας. Παρόλα αυτά, σε αρκετές ενότητες το υλικό που χρειάστηκε να καλυφθεί ήταν μεγάλο σε όγκο, με αποτέλεσμα να αναφέρονται στην εργασία μόνο τα απολύτως αναγκαία. Για αυτό το λόγο, σε όσα σημεία αναφέρεται ότι έχουν παραλειφθεί λεπτομέρειες συνιστάται να ανατρέχει ο αναγνώστης στην αντίστοιχη βιβλιογραφία που υποδεικνύεται από τις παραπομπές, σε περίπτωση που ενδιαφέρεται να διαβάσει περισσότερα.

# 2. Προεκτάσεις της Λογικής Πρώτης Τάξης

Σε αυτή την ενότητα θα μελετήσουμε ορισμένες λογικές οι οποίες διαθέτουν μεγαλύτερη εκφραστικότητα από τη λογική πρώτης τάξης και θα μας χρησιμεύσουν παρακάτω στην περιγραφή κλάσεων πολυπλοκότητας με λογική. Συγκεκριμένα, θα ασχοληθούμε συνοπτικά με fixed point logics, καθώς και λογικές δεύτερης τάξης.

## 2.1. Λογική Σταθερού Σημείου (Fixed Point Logic)

Η ιδέα πίσω από τις λογικές σταθερού σημείου είναι η ανάγκη έκφρασης σχέσεων που ορίζονται αναδρομικά. Ένα παράδειγμα τέτοιας σχέσης είναι η μεταβατική κλειστότητα για γραφήματα [Imm99], την οποία άτυπα θα εκφράζαμε κάπως έτσι:

$$E^*(x,y) \equiv x = y \vee \exists z\big(E(x,z) \wedge E^*(z,y)\big)$$

Στο παραπάνω υποθέτουμε ότι οι $x, y, z$ είναι κόμβοι ενός γραφήματος και $E(x,z)$ ένα κατηγόρημα που εκφράζει ότι υπάρχει ακμή ανάμεσα στους δύο κόμβους $x$ και $z$. Στα πλαίσια της εργασίας αυτής, γενικά αυτοί οι συμβολισμοί θα έχουν την ίδια σημασία, όταν αναφερόμαστε σε γραφήματα.

Προφανώς αυτός ο ορισμός δεν είναι κάτι που επιτρέπεται στη λογική πρώτης τάξης. Η παραπάνω σχέση έχει σκοπό μόνο να μας δείξει πώς θα ορίζαμε κάτι τέτοιο διαισθητικά.

Ένα άλλο παρόμοιο παράδειγμα στο οποίο χρησιμεύουν οι λογικές σταθερού σημείου είναι η διατύπωση κλάσεων όπως αυτή των συνεκτικών γραφημάτων [EF99], η οποία πάλι απαιτεί αναδρομή στον ορισμό της. Κάτι τέτοιο δεν μπορεί να διατυπωθεί σε λογική πρώτης τάξης.

Σε αυτό το σημείο θα επικεντρωθούμε στην *least fixed point* λογική που προτείνει ο Immerman, η οποία συμβολίζεται ως $\boldsymbol{FO(LFP)}$. Σημειώνεται ότι υπάρχουν και άλλες λογικές σταθερού σημείου, όπως η *inflationary fixed point* λογική ($FO(IFP)$), η οποία έχει ακριβώς την ίδια εκφραστικότητα με την $FO(LFP)$ [EF99]. Ανεξαρτήτως των διαφορών τους, η γενική ιδέα πίσω από τέτοιου είδους λογικές είναι η έκφραση αναδρομικών σχέσεων.

Για να αυστηροποιήσουμε την περιγραφή της παραπάνω έκφρασης για τη μεταβατική κλειστότητα γραφήματος, ο Immerman προτείνει την εξής φόρμουλα:

$$\varphi(R,x,y) \equiv x = y \vee \exists z\big(E(x,z) \wedge R(z,y)\big)$$

Η φόρμουλα αυτή δημιουργεί μια αντιστοίχιση ("map") από το σύνολο των δυαδικών σχέσεων στο σύμπαν της δομής $A$ προς τον εαυτό του:

$$\varphi^A(R) = \{(a,b) \mid A \vDash \varphi(R,a,b)\}$$

Μια τέτοια αντιστοίχιση καλείται *μονότονη* εάν ισχύει το εξής:

$$R \subseteq R' \rightarrow \varphi^A(R) \subseteq \varphi^A(R')$$

Μπορούμε εύκολα να διαπιστώσουμε ότι στη λογική πρώτης τάξης αυτό ισχύει εάν η σχέση $R$ εμφανίζεται με άρτιο πλήθος αρνήσεων.

*Ελάχιστο σταθερό σημείο* (least fixed point) της $\varphi^A$ καλείται η ελάχιστη σχέση $T$ τέτοια ώστε να ισχύει $\varphi^A(T) = T$. Αποδεικνύεται με γενικό τρόπο ότι το least fixed point μιας τέτοιας αντιστοίχισης είναι το $(\varphi^A)^r(\emptyset)$, με $r$ τον ελάχιστο αριθμό για τον οποίο ισχύει $(\varphi^A)^r(\emptyset) = (\varphi^A)^{r+1}(\emptyset)$. Η απόδειξη βασίζεται σε τετριμμένες παρατηρήσεις και παραλείπεται επειδή δεν παρουσιάζει ιδιαίτερο ενδιαφέρον. Διευκρινίζουμε ότι στους παραπάνω συμβολισμούς ο εκθέτης $r$ υποδεικνύει εφαρμογή σύνθεσης $r$ φορές.

Για την $\varphi^A$ που εξετάσαμε παραπάνω μπορούμε εύκολα να δούμε ότι το least fixed point της είναι το $(\varphi^A)^{\|A\|}(\emptyset)$. Αυτό στην ουσία εκφράζει ακριβώς την έννοια της μεταβατικής κλειστότητας.

Η $FO(LFP)$ αποτελεί προέκταση της λογικής πρώτης τάξης με έναν τελεστή least fixed point. Ο τελεστής αυτός λειτουργεί ως εξής. Για κάθε φόρμουλα $\varphi$ της μορφής $\varphi\left(R^k, x_1, \dots, x_k\right)$, στην οποία η σχέση $R^k$ εμφανίζεται με άρτιο πλήθος αρνήσεων, το σύμβολο $LFP_{R^k, x_1, \dots, x_k}\varphi$ μπορεί να χρησιμοποιηθεί ως σχέση $k$ θέσεων που έχει το νόημα του least fixed point της $\varphi$.

Όπως θα δούμε στη συνέχεια, οι λογικές σταθερού σημείου έχουν μια πολύ σημαντική εφαρμογή στη θεωρία περιγραφικής πολυπλοκότητας, καθώς τα προβλήματα που μπορούν να περιγραφούν με αυτές είναι ακριβώς τα προβλήματα της κλάσης $P$.

## 2.2. Λογική Δεύτερης Τάξης (Second Order Logic)

Στη λογική πρώτης τάξης χρησιμοποιούνται ποσοδείκτες για αντικείμενα, αλλά όχι για σχέσεις. Αυτό σημαίνει ότι προτάσεις της μορφής «για κάθε σχέση ισχύει» ή «υπάρχει σχέση τέτοια ώστε» δεν μπορούν να εκφραστούν σε λογική πρώτης τάξης. Για αυτούς τους σκοπούς χρησιμοποιείται λογική δεύτερης τάξης, στην οποία μπορούμε να χρησιμοποιήσουμε ποσοδείκτες για σχέσεις, σύνολα ή συναρτήσεις [GSS08].

Για παράδειγμα, η παρακάτω πρόταση σε λογική δεύτερης τάξης σημαίνει ότι το αντικείμενο $a$ έχει κάποιο χρώμα:

$$\exists Color^1\big(Color(a)\big)$$

Σε λογική δεύτερης τάξης μπορούμε να εκφράσουμε και προτάσεις σαν την παρακάτω, η οποία εκφράζει μια ιδιότητα που ισχύει για κάθε σχέση $R^1$.

$$\forall R^1 \forall x\big(R(x) \vee \neg R(x)\big)$$

Η λογική δεύτερης τάξης είναι χρήσιμη για να εκφράσουμε διάφορα είδη προτάσεων, όπως ιδιότητες προσβασιμότητας (reachability) σε γραφήματα [Pap94]. Για παράδειγμα, η ιδιότητα μη προσβασιμότητας (*unreachability*) μπορεί να εκφραστεί ως εξής:

$$\varphi(x,y) = \exists P^2 \left(\forall u,v,w \left(P(u,u) \wedge \big(E(u,v) \rightarrow P(u,v)\big) \wedge \Big(\big(P(u,v) \wedge P(v,w)\big) \rightarrow P(u,w)\Big) \wedge \neg P(x,y)\right)\right)$$

Το παραπάνω μεταφράζεται ως εξής: ο κόμβος $y$ είναι απροσπέλαστος από τον $x$, εάν υπάρχει σχέση δύο θέσεων τέτοια ώστε να ισχύει $\neg P(x,y)$, και αυτή η σχέση εκφράζει την έννοια της προσβασιμότητας κόμβων, δηλαδή:

- Κάθε κόμβος είναι προσπελάσιμος από τον εαυτό του.
- Κάθε κόμβος $v$ είναι προσπελάσιμος από κόμβους $u$ για τους οποίους υπάρχει ακμή $u - v$.
- Για κάθε τριάδα κόμβων $u, v, w$, για τους οποίους ο $v$ είναι προσπελάσιμος από τον $u$ και ο $w$ από τον $v$, ισχύει και ότι ο $w$ είναι προσπελάσιμος από τον $u$.

Σημειώνουμε ότι κάθε πρόταση δεύτερης τάξης μπορεί να μετατραπεί σε μια ισοδύναμη που θα έχει όλους τους ποσοδείκτες δεύτερης τάξης στην αρχή [Imm99]. Εάν όλοι αυτοί οι ποσοδείκτες είναι υπαρξιακοί, τότε μιλάμε για *υπαρξιακή λογική δεύτερης τάξης*.

Όπως θα δούμε στη συνέχεια, χρησιμοποιώντας υπαρξιακή λογική δεύτερης τάξης μπορούμε να εκφράσουμε όλα τα προβλήματα στο $NP$. Μπορούμε να δούμε ένα παράδειγμα για την ύπαρξη 3-χρωματισμού σε γραφήματα:

$$\exists R^1, G^1, B^1 \left(\forall x \left(\big(R(x) \vee G(x) \vee B(x)\big) \wedge \forall y \left(E(x,y) \rightarrow \neg\big(R(x) \wedge R(y)\big) \wedge \neg\big(G(x) \wedge G(y)\big) \wedge \neg\big(B(x) \wedge B(y)\big)\right)\right)\right)$$

Σημειώνουμε ότι τα προβλήματα που μπορούν να εκφραστούν με υπαρξιακή λογική δεύτερης τάξης αποτελούν υπερσύνολο αυτών που μπορούν να εκφραστούν με τις fixed point logics που είδαμε προηγουμένως, χωρίς όμως να έχει βρεθεί εάν αυτό είναι γνήσιο υπερσύνολο. Η πρόταση αυτή θα προκύψει σαν πόρισμα στη συνέχεια.

# 3. Περιγραφική Πολυπλοκότητα για Προβλήματα Απόφασης

Σε αυτό το σημείο θα κάνουμε μια σύντομη αναφορά σε κάποια από τα σημαντικότερα αποτελέσματα που έχουν προκύψει από το πεδίο της περιγραφικής πολυπλοκότητας για κλάσεις προβλημάτων απόφασης.

Σημειώνουμε ότι σε αυτό το κεφάλαιο γενικά αναφερόμαστε σε *πεπερασμένες* και *διατεταγμένες* δομές. Με τον όρο διατεταγμένες εννοούμε ότι διαθέτουμε έναν τελεστή '≤', ο οποίος λειτουργεί ως δυαδική σχέση που καθορίζει μια ολική διάταξη στα στοιχεία του σύμπαντος.

## 3.1. Κλάση L – First Order Queries

Όπως θα δούμε στη συνέχεια, η εκφραστικότητα που μας προσφέρει η λογική πρώτης τάξης για προβλήματα είναι πολύ μικρή. Για αυτό το σκοπό θα παρουσιάσουμε αρχικά τους ορισμούς των κλάσεων πολυπλοκότητας $L$ και $NL$ [Sip97]:

Ορισμός (Κλάση $L$)

Η κλάση πολυπλοκότητας $L$ (εναλλακτική ονομασία: DLOGSPACE) περιέχει τα προβλήματα απόφασης τα οποία μπορούν να επιλυθούν από ντετερμινιστική μηχανή Turing χρησιμοποιώντας λογαριθμικό χώρο μνήμης.

Ορισμός (Κλάση $NL$)

Η κλάση πολυπλοκότητας $NL$ περιέχει τα προβλήματα απόφασης τα οποία μπορούν να επιλυθούν από μη ντετερμινιστική μηχανή Turing χρησιμοποιώντας λογαριθμικό χώρο μνήμης.

Όπως φαίνεται από τους ορισμούς, οι κλάσεις $L$ και $NL$ σχετίζονται μεταξύ τους όπως οι $P$ και $NP$. Αναφέρουμε ότι έχει αποδειχθεί η παρακάτω ιεραρχία κλάσεων [Sip97]:

$$L \subseteq NL \subseteq P$$

Εξακολουθεί να είναι ανοιχτό πρόβλημα εάν οι παραπάνω κλάσεις ταυτίζονται μεταξύ τους [GJ79].

Παρακάτω θα παρουσιάσουμε εν συντομία το θεώρημα που μας δίνει απάντηση σχετικά με την εκφραστικότητα της λογικής πρώτης τάξης, μαζί με την αντίστοιχη απόδειξη [Imm99].

Θεώρημα ($FO \subseteq L$)

Το σύνολο των boolean queries που μπορούν να περιγραφούν σε λογική πρώτης τάξης μπορεί να υπολογιστεί ντετερμινιστικά σε λογαριθμικό χώρο. Με σύμβολα αυτό γράφεται ως $FO \subseteq L$. Διευκρινίζουμε ότι ένα boolean query που μπορεί να περιγραφεί σε λογική πρώτης τάξης ουσιαστικά καθορίζεται από μια πρωτοβάθμια πρόταση $\varphi$.

Απόδειξη ($FO \subseteq L$)

Σκοπός μας είναι να κατασκευάσουμε μια μηχανή Turing $M$ λογαριθμικού χώρου τέτοια ώστε για κάθε δομή $A$ να είναι $A \vDash \varphi$ αν και μόνο αν η $M$ αποδέχεται τη δυαδική αναπαράσταση της $A$. Υποθέτουμε ότι η πρόταση $\varphi$ βρίσκεται στην παρακάτω μορφή:

$$\varphi \equiv (\exists x_1)(\forall x_2) \dots (Q_k x_k) a(x_1, x_2, \dots x_k)$$

Διευκρινίζουμε ότι τα $Q_i$ είναι ποσοδείκτες και το $a$ δεν περιέχει ποσοδείκτες.

Έστω τώρα ότι το σύμπαν $|A|$ περιέχει $n$ στοιχεία. Η δυαδική αναπαράσταση της $A$ θα αποτελείται από παράθεση των δυαδικών αναπαραστάσεων των κατηγορημάτων και των σταθερών της. Δεδομένου ότι ένα κατηγόρημα $a_i$ θέσεων είναι υποσύνολο του $|A|^{a_i}$, επιλέγουμε να αναπαραστήσουμε τα κατηγορήματα ως δυαδικές ακολουθίες μήκους $n^{a_i}$, όπου μια θέση είναι '1' εάν το κατηγόρημα είναι αληθές για το αντίστοιχο tuple. Για τις σταθερές επιλέγουμε αναπαράσταση μήκους $\lceil \log n \rceil$, η οποία αντιστοιχεί στην τιμή τους. Συνεπώς, αν το πλήθος των κατηγορημάτων είναι $r$ και το πλήθος των σταθερών είναι $s$, η $M$ θα δέχεται είσοδο μήκους:

$$f(n) = \sum_{i=1}^{r} n^{a_i} + s\lceil \log n \rceil$$

Παραλείποντας κάποιες λεπτομέρειες της λειτουργίας της μηχανής Turing, αναφέρουμε ότι από το παραπάνω μήκος εισόδου είναι εφικτό να υπολογίσει η μηχανή τα $n$ και $\lceil \log n \rceil$. Γνωρίζοντας αυτά, η μηχανή γνωρίζει ποια bits αντιστοιχούν σε κάθε σταθερά/κατηγόρημα και επομένως μπορεί απλά κοιτώντας κάποια bits να βρει την τιμή στην οποία έχει αντιστοιχηθεί μια σταθερά ή το αν ένα κατηγόρημα είναι αληθές για κάποιο συγκεκριμένο tuple.

Η κατασκευή της $M$ θα γίνει με επαγωγή στο $k$, δηλαδή το πλήθος των ποσοδεικτών της $\varphi$.

- Επαγωγική βάση: Για $k = 0$ η $\varphi$ δεν περιέχει ποσοδείκτες, δηλαδή αποτελείται από ατομικούς τύπους συνδυασμένους μεταξύ τους με λογικούς τελεστές. Σύμφωνα με τα παραπάνω, ο έλεγχος για το αν είναι αληθής ένας ατομικός τύπος μπορεί να γίνει από τη μηχανή με απλή επισκόπηση κάποιων τιμών και συγκρίσεις. Στη συνέχεια, οι λογικές πράξεις ανάμεσα στους ατομικούς τύπους είναι τετριμμένες και εύκολα μπορούμε να δούμε ότι μια μηχανή λογαριθμικού χώρου μπορεί να τις εκτελέσει. Με αυτό τον τρόπο μπορεί η $M$ να ελέγξει εάν ισχύει $A \vDash \varphi$.

- Επαγωγική υπόθεση: Έστω ότι έχει κατασκευαστεί μηχανή Turing λογαριθμικού χώρου για κάθε πρόταση $\varphi$ με $k-1$ ποσοδείκτες.
- Επαγωγικό βήμα: Θέτουμε $\psi(x_1) \equiv (\forall x_2) \dots (Q_k x_k) a(x_1, x_2, \dots x_k)$ και έτσι έχουμε:
$$\varphi \equiv (\exists x_1)\big(\psi(x_1)\big)$$
Κατασκευάζουμε μια μηχανή $M$ η οποία εκτελεί την εξής διαδικασία. Για κάθε πιθανή τιμή της $x_1$ παίρνει την πρόταση $\psi(c)$ βάζοντας στη σταθερά $c$ την αντίστοιχη τιμή. Σημειώνουμε ότι η $\psi(c)$ είναι πρόταση λογικής πρώτης τάξης και περιέχει ακριβώς $k-1$ ποσοδείκτες, επομένως από επαγωγική υπόθεση υπάρχει αντίστοιχη μηχανή $M'$ για την $\psi(c)$. Άρα αρκεί να τρέξουμε την $M'$ για καθεμία από τις τιμές που θα πάρει η σταθερά $c$. Εάν η $M'$ αποδεχτεί την αντίστοιχη είσοδο τουλάχιστον μια φορά, τότε και η $M$ θα αποδεχτεί, αφού θα υπάρχει $x_1$ τέτοιο ώστε να ισχύει η $\psi(x_1)$. Παρατηρούμε ότι ο επιπλέον χώρος που χρειάζεται η $M$ συγκριτικά με την $M'$ είναι $\log n$ bits για την αποθήκευση των τιμών της $x_1$, επομένως ο χώρος που χρησιμοποιείται παραμένει λογαριθμικός. ■

Με τα παραπάνω έχουμε αποδείξει ότι $FO \subseteq L$. Υποθέσαμε ότι η $\varphi$ ξεκινάει με υπαρξιακό ποσοδείκτη, ωστόσο η διαδικασία θα ήταν παρόμοια και για καθολικό ποσοδείκτη. Ουσιαστικά η μόνη διαφορά θα ήταν ότι στο τελευταίο βήμα η $M$ θα έπρεπε να αποδεχτεί αν και μόνο αν η $M'$ αποδέχτηκε όλες τις εισόδους που της δόθηκαν (δηλαδή όλες τις δυνατές τιμές της $x_1$).

Με βάση την παραπάνω απόδειξη και την ιεραρχία των κλάσεων $N, NL, P$ που παρουσιάσαμε πρωτύτερα, γνωρίζουμε ότι **για να εκφράσουμε προβλήματα των κλάσεων $P$ και $NP$ με λογική, θα χρειαστούμε μεγαλύτερη εκφραστικότητα από αυτήν που προσφέρει η λογική πρώτης τάξης**.

Σημειώνουμε ότι **έχουν βρεθεί και προεκτάσεις της λογικής πρώτης τάξης που περιέχουν ακριβώς τα προβλήματα των κλάσεων $L$ και $NL$**. Αυτές οι λογικές ανήκουν στην κατηγορία των *transitive closure logics* και δίνουν δυνατότητα έκφρασης της μεταβατικής κλειστότητας σχέσεων, το οποίο κανονικά δεν είναι εφικτό στη λογική πρώτης τάξης. Συγκεκριμένα, έχει αποδειχθεί ότι ισχύει $FO(DTC) = L$ (*deterministic transitive closure logic*) και $FO(TC) = NL$ (*transitive closure logic*) [EF99]. Στα πλαίσια αυτής της εργασίας δεν κρίνεται σκόπιμο να μελετήσουμε και αυτές τις λογικές σε βάθος, ωστόσο αναφέρουμε ότι αυτές αποτελούν υποσύνολα των fixed point logics που μελετήσαμε σε προηγούμενη ενότητα.

## 3.2. Κλάση P – Λογικές Σταθερού Σημείου

Σε αυτό το σημείο έχουμε δει ότι δεν μας αρκεί η λογική πρώτης τάξης για να εκφράσουμε προβλήματα της κλάσης $P$. Ωστόσο, δεν είναι αναγκαίο να χρησιμοποιηθεί λογική ανώτερης τάξης για την κλάση $P$. Έχει αποδειχθεί ότι η κλάση $P$ περιέχει ακριβώς τα προβλήματα που μπορούν να εκφραστούν σε λογικές σταθερού σημείου (*fixed point logics*) [Imm99] [EF99], τις οποίες μελετήσαμε περιληπτικά σε προηγούμενη ενότητα.

Θα ασχοληθούμε με την απόδειξη $P = FO(LFP)$ κατά Immerman [Imm99], όμως τονίζουμε ότι αυτή δεν είναι η μοναδική λογική τέτοιου είδους που περιγράφει ακριβώς τα προβλήματα της κλάσης $P$. Παρομοίως έχει αποδειχτεί ότι $P = FO(IFP)$ [EF99].

Για την απόδειξη ότι $P = FO(LFP)$ κατά Immerman θα χρειαστούμε να ορίσουμε το πρόβλημα *προσβασιμότητας με εναλλασσόμενα μονοπάτια* (alternating path reachability) για γραφήματα, το οποίο συμβολίζουμε ως $\boldsymbol{REACH_a}$.

<u>Ορισμός (Πρόβλημα $REACH_a$)</u>

Έχουμε ένα <u>κατευθυνόμενο</u> γράφημα στο οποίο μας ενδιαφέρει να βρούμε εάν υπάρχει μονοπάτι ανάμεσα σε δύο συγκεκριμένους κόμβους $s, t$. Η ιδιαιτερότητα του προβλήματος είναι ότι οι κόμβοι του γραφήματος χωρίζονται σε δύο κατηγορίες:

1. "Υπαρξιακούς" (existential) κόμβους, για τους οποίους αρκεί να υπάρχει μία εξερχόμενη ακμή τους η οποία να οδηγεί σε μονοπάτι προς τον στόχο $t$.

2. "Καθολικούς" (universal) κόμβους, για τους οποίους πρέπει όλες οι εξερχόμενες ακμές τους να οδηγούν σε κάποιο μονοπάτι προς τον στόχο $t$. Επιπλέον, πρέπει να έχουν τουλάχιστον μία εξερχόμενη ακμή.

Σημειώνουμε ότι η παραπάνω περιγραφή του προβλήματος αποτελεί προσπάθεια απλούστευσης και δεν περιέχει τους αυστηρούς ορισμούς που προτείνει ο Immerman.

Αρχικά παρατηρούμε ότι το παραπάνω πρόβλημα **μπορεί να περιγραφεί με least fixed point logic** ως εξής:

$$\varphi(P, x, y) \equiv x = y \vee \Big[\exists z\big(E(x,z) \wedge P(z,y)\big) \wedge \Big(A(x) \rightarrow (\forall z)\big(E(x,z) \rightarrow P(z,y)\big)\Big)\Big]$$

Διευκρινίζουμε ότι στην παραπάνω φόρμουλα το κατηγόρημα $E$ εκφράζει την ύπαρξη ακμής ανάμεσα σε δύο κόμβους, το κατηγόρημα $A$ σημαίνει ότι ο αντίστοιχος κόμβος είναι καθολικός (universal) και το κατηγόρημα $P$ θα χρησιμοποιηθεί για την έκφραση της ύπαρξης εναλλασσόμενου μονοπατιού ανάμεσα σε δύο κόμβους. Η παραπάνω φόρμουλα μπορεί άτυπα να μεταφραστεί ως «οι κόμβοι $x, y$ συνδέονται με εναλλασσόμενο μονοπάτι αν και μόνο αν ταυτίζονται ή υπάρχει ακμή $x - z$ και εναλλασσόμενο μονοπάτι $z - y$ και, αν ο $x$ είναι καθολικός, τότε για κάθε κόμβο $z$ με τον οποίο συνδέεται, υπάρχει εναλλασσόμενο μονοπάτι $z - y$». Το ελάχιστο σταθερό σημείο (least fixed point) της $\varphi$, κατ' αναλογία με την παρόμοια αλλά απλούστερη περίπτωση της μεταβατικής κλειστότητας που μελετήσαμε σε προηγούμενη ενότητα, θα έχει το νόημα της ύπαρξης εναλλασσόμενου μονοπατιού ανάμεσα σε δύο κόμβους.

Με βάση τα παραπάνω, έχουμε:

$$REACH_a = \left(LFP_{P,x,y}\varphi\right)(s,t)$$

Σε αυτό το σημείο είμαστε έτοιμοι να παρουσιάσουμε περιληπτικά το βασικό θεώρημα αυτής της ενότητας, μαζί με την απόδειξή του.

<u>Θεώρημα ($P = FO(LFP)$)</u>

Για δομές που είναι πεπερασμένες και διατεταγμένες ισχύει $P = FO(LFP)$, δηλαδή η λογική $FO(LFP)$ εκφράζει ακριβώς το σύνολο των boolean queries που μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο από ντετερμινιστική μηχανή Turing.

<u>Απόδειξη ($P = FO(LFP)$)</u>

- <u>$P \subseteq FO(LFP)$:</u> Όπως είδαμε, το πρόβλημα $REACH_a$ μπορεί να εκφραστεί με $FO(LFP)$. Επειδή το $REACH_a$ είναι P-πλήρες με αναγωγές πρώτης τάξης και η $FO(LFP)$ είναι κλειστή ως προς αναγωγές πρώτης τάξης [Imm99], καταλήγουμε ότι όλα τα προβλήματα της κλάσης $P$ μπορούν να εκφραστούν με $FO(LFP)$. Οι αποδείξεις για αυτές τις προτάσεις παραλείπονται χάριν συντομίας.
- <u>$FO(LFP) \subseteq P$:</u> Όπως είχαμε δει στην ενότητα των fixed point λογικών, το ελάχιστο σταθερό σημείο μιας αντιστοίχισης $\varphi^A$ είναι το $(\varphi^A)^r(\emptyset)$, με $r$ τον ελάχιστο αριθμό για τον οποίο ισχύει:
$$(\varphi^A)^r(\emptyset) = (\varphi^A)^{r+1}(\emptyset)$$
Υποθέτοντας ότι το σύμβολο κατηγορήματος που περιέχει η φόρμουλα $\varphi$ είναι $k$ θέσεων, υπάρχουν συνολικά $\|A\|^k$ $k$-άδες που μπορεί να ανήκουν ή να μην ανήκουν στο κατηγόρημα. Επειδή η $\varphi^A$ είναι μονότονη και $r$ είναι ο ελάχιστος αριθμός για τον οποίο ισχύει η παραπάνω ισότητα, συμπεραίνουμε ότι για $i < r$ πρέπει να υπάρχει τουλάχιστον μία $k$-άδα κατά την οποία να διαφέρουν δύο διαδοχικά $(\varphi^A)^{i-1}(\emptyset)$ και $(\varphi^A)^i(\emptyset)$. Εύκολα βλέπουμε ότι αυτό συνεπάγεται ότι $\boldsymbol{r \leq \|A\|^k}$. Επομένως, για τον υπολογισμό του ελάχιστου σταθερού σημείου χρειάζονται το πολύ $\|A\|^k$ υπολογισμοί first order boolean queries. Επειδή είναι $FO \subseteq L \subseteq P$, ένας τέτοιος υπολογισμός γίνεται σε πολυωνυμικό χρόνο. Σημειώνουμε ότι το $k$ είναι σταθερά, επομένως δεν μιλάμε για εκθετική πολυπλοκότητα. ■

Έτσι έχουμε ένα ενδιαφέρον αποτέλεσμα που ουσιαστικά μας λέει ότι τα προβλήματα που λύνονται σε πολυωνυμικό χρόνο μπορούν να εκφραστούν ακριβώς από λογική πρώτης τάξης με τη δυνατότητα αναδρομικών ορισμών για σχέσεις.

Σημειώνουμε σαν ενδιαφέρουσα πληροφορία ότι η γλώσσα λογικού προγραμματισμού Datalog έχει ακριβώς την εκφραστικότητα της least fixed point logic, το οποίο σύμφωνα με τα παραπάνω συνεπάγεται ότι στην Datalog μπορούν να εκφραστούν ακριβώς τα queries που είναι υπολογίσιμα σε πολυωνυμικό χρόνο [EF99].

## 3.3. Κλάση NP – Το Θεώρημα του Fagin

Όπως αναφέρθηκε και στην εισαγωγή, το θεώρημα του Fagin [Fag74] ουσιαστικά «γέννησε» το πεδίο της περιγραφικής πολυπλοκότητας. Το θεώρημα αυτό αποδείχτηκε από τον Ronald Fagin το 1973.

Η αξία του θεωρήματος έγκειται στο ότι φανέρωσε ότι οι κλάσεις πολυπλοκότητας δεν χαρακτηρίζονται μόνο από την υπολογιστική δυσκολία των αντίστοιχων προβλημάτων, αλλά μπορούν να καθοριστούν και από την εκφραστικότητα που απαιτείται για τη διατύπωση των προβλημάτων τους με λογική. Ένα τέτοιο αποτέλεσμα ουσιαστικά ανεξαρτητοποιεί τις κλάσεις πολυπλοκότητας από τα υπολογιστικά μας εργαλεία και μας δείχνει ότι θα μπορούσαμε να ορίσουμε αυτές τις κλάσεις χωρίς καν να αναφερθούμε σε έννοιες όπως χώρο, χρόνο, μηχανές Turing και άλλες. Παρακάτω θα παρουσιάσουμε εν συντομία το θεώρημα και την αντίστοιχη απόδειξη που προτείνει ο Immerman [Imm99].

Θεώρημα (Fagin)

Η κλάση πολυπλοκότητας $NP$ περιέχει ακριβώς τα προβλήματα που μπορούν να περιγραφούν σε υπαρξιακή λογική δεύτερης τάξης. Με σύμβολα αυτό γράφεται ως:

$$NP = SO\exists$$

Απόδειξη (Fagin)

1. $SO\exists \subseteq NP$:

Η ιδέα για την απόδειξη αυτή μοιάζει με την απόδειξη $FO \subseteq L$ που είδαμε πρωτύτερα.

Σκοπός μας είναι να κατασκευάσουμε μια μη ντετερμινιστική πολυωνυμική μηχανή Turing $N$ τέτοια ώστε για κάθε δομή $A$ να είναι $A \vDash \Phi$ ($\Phi$: πρόταση $SO\exists$) αν και μόνο αν η $N$ αποδέχεται τη δυαδική αναπαράσταση της $A$. Η πρόταση $\Phi$ βρίσκεται στην παρακάτω μορφή:

$$\Phi \equiv \exists R_1^{r_1} \dots \exists R_k^{r_k} \psi$$

Διευκρινίζουμε ότι η $\psi$ είναι φόρμουλα πρώτης τάξης. Υπενθυμίζουμε ότι κάθε πρόταση $SO\exists$ μπορεί να γραφεί στην παραπάνω μορφή, επειδή οι ποσοδείκτες δεύτερης τάξης μπορούν να μεταφερθούν στην αρχή της πρότασης.

Εφόσον αναφερόμαστε σε μη ντετερμινιστική μηχανή Turing, μπορούμε να ακολουθήσουμε την εξής διαδικασία. Η μηχανή θα καταγράψει μη ντετερμινιστικά τη δυαδική αναπαράσταση καθεμίας σχέσης $R_i$ (χρησιμοποιώντας $\|A\|^{r_i}$ bits, όπως έχει εξηγηθεί και στην απόδειξη $FO \subseteq L$), δηλαδή θα εξετάσει όλους τους διαφορετικούς συνδυασμούς τιμών των σχέσεων $R_i$. Υπενθυμίζουμε ότι τα $r_i$ είναι σταθερές και επομένως το παραπάνω γίνεται σε πολυωνυμικό χρόνο (μη ντετερμινιστικά). Στη συνέχεια η μηχανή θα ελέγξει εάν ισχύει:

$$(A, R_1, \dots, R_k) \vDash \psi$$

Αν το παραπάνω ισχύει, η μηχανή θα αποδεχτεί, αλλιώς όχι. Σημειώνουμε ότι εφόσον μιλάμε για μη ντετερμινιστικό έλεγχο, η μηχανή θα αποδεχτεί αν και μόνο αν *υπάρχουν* σχέσεις $R_i$ τέτοιες ώστε να ισχύει το παραπάνω, δηλαδή αν και μόνο αν $A \vDash \Phi$.

Επειδή είναι $FO \subseteq L \subseteq P$, ο παραπάνω έλεγχος επίσης γίνεται σε πολυωνυμικό χρόνο. Επομένως, κατασκευάσαμε τη ζητούμενη μηχανή $N$, άρα ισχύει $SO\exists \subseteq NP$.

2. $NP \subseteq SO\exists$:

Σκοπός μας είναι να βρούμε πρόταση $SO\exists$ $\Phi$, τέτοια ώστε για μια μη ντετερμινιστική πολυωνυμική μηχανή Turing $N$ να ισχύει $A \vDash \Phi$ αν και μόνο αν η $N$ αποδέχεται τη δυαδική αναπαράσταση της δομής $A$. Θέτουμε $n = \|A\|$ και θεωρούμε ακέραιο αριθμό $k$ τέτοιο ώστε η $N$ να χρησιμοποιεί χρόνο $n^k - 1$ (το πολύ) και χώρο $n^k$ (το πολύ) όταν δέχεται ως είσοδο δομή $A$.

Ορίζουμε τα παρακάτω σύμβολα που θα χρησιμοποιηθούν στην απόδειξη:

- $\vec{s}$: Η αρίθμηση των $n^k$ κελιών της μηχανής $N$. Χρησιμοποιούμε $k$-tuples $\vec{s} = (s_1, \dots, s_k)$, όπου κάθε στοιχείο $s_i$ παίρνει τιμές στο σύμπαν $|A|$, δηλαδή τιμές $0, \dots, n-1$. Με αυτό τον τρόπο η $\vec{s}$ λαμβάνει τιμές $0, \dots, n^k - 1$.
- $\vec{t}$: Η αρίθμηση των $n^k$ χρονικών στιγμών κατά τον υπολογισμό που εκτελεί η μηχανή $N$. Εντελώς όμοια με το $\vec{s}$, το $\vec{t}$ λαμβάνει τιμές $0, \dots, n^k - 1$ χρησιμοποιώντας $k$-tuples.
- $\Sigma$: Το σύνολο των δυνατών συμβόλων $\sigma$ που μπορεί να έχει ένα κελί της $N$ σε κάποια χρονική στιγμή.
- $Q$: Το σύνολο των δυνατών καταστάσεων $q$ της μηχανής $N$.
- $\Gamma = \{\gamma_0, \dots, \gamma_g\} = (Q \times \Sigma) \cup \Sigma$: Το σύνολο των δυνατών περιεχομένων ενός κελιού της $N$ σε κάποια χρονική στιγμή, θεωρώντας ότι κρατάμε το σύμβολο $\sigma$ όταν *δεν* βρίσκεται η κεφαλή της $N$ σε εκείνη τη θέση, ενώ αλλιώς κρατάμε το διατεταγμένο ζεύγος $(q, \sigma)$.

Θεωρούμε την παρακάτω μορφή για την πρόταση $\Phi$, όπου η $\varphi$ είναι πρόταση πρώτης τάξης:

$$\Phi \equiv \left(\exists C_1^{2k} \dots C_g^{2k} \Delta^k\right)\varphi$$

Τα κατηγορήματα $C_i(\vec{s}, \vec{t})$ έχουν την εξής σημασία: το κελί $\vec{s}$ τη χρονική στιγμή $\vec{t}$ έχει περιεχόμενο $\gamma_i \in \Gamma$.

Σημειώνουμε ότι μπορούμε να θεωρήσουμε ότι η μηχανή $N$ κάθε χρονική στιγμή λαμβάνει (μη ντετερμινιστικά) μία από δύο αποφάσεις. Στην πραγματικότητα, λαμβάνει μία από *πολλές* αποφάσεις, αλλά αναγκάζοντάς την να αποφασίζει ανάμεσα σε δύο ενδεχόμενα ανά βήμα την καθυστερούμε κατά ένα σταθερό παράγοντα, το οποίο είναι επιτρεπτό (και η μηχανή παραμένει πολυωνυμική).

Με αυτή τη λογική θεωρούμε ότι το κατηγόρημα $\Delta(\vec{t})$ διαθέτει τη σημασία: τη χρονική στιγμή $\vec{t}$ η μηχανή $N$ λαμβάνει την απόφαση '1' (αλλιώς λαμβάνει την απόφαση '0').

Μένει να διευκρινίσουμε τι θα είναι η πρόταση πρώτης τάξης $\varphi(\vec{C}, \Delta)$. Ο Immerman προτείνει να σπάσουμε αυτή την πρόταση σε τέσσερα κομμάτια:

$$\varphi \equiv \alpha \wedge \beta \wedge \eta \wedge \zeta$$

Αυτά θα έχουν την παρακάτω σημασία:

- $\alpha$: Για $\vec{t} = 0$ πρέπει το περιεχόμενο των κελιών να περιέχει τη δυαδική αναπαράσταση της δομής $A$.
- $\beta$: Δεν ισχύει $C_i(\vec{s}, \vec{t}) \wedge C_j(\vec{s}, \vec{t})$ για $i \neq j$.
- $\eta$: Το περιεχόμενο των κελιών τη στιγμή $\vec{t} + 1$ καθορίζεται από το περιεχόμενό τους τη στιγμή $\vec{t}$, με βάση την απόφαση $\Delta(\vec{t})$.
- $\zeta$: Για $\vec{t} = n^k - 1$ η μηχανή περιέχει την κατάσταση αποδοχής.

Σε αυτό το σημείο αναφέρουμε πως θεωρούμε ότι μπορούμε στις διατυπώσεις των προτάσεων να χρησιμοποιούμε τα σύμβολα 0 και $max$, τα οποία αντιστοιχούν στο ελάχιστο και το μέγιστο στοιχείο της διατεταγμένης δομής μας. Με $\vec{0}$ και $\overrightarrow{max}$ θα συμβολίζουμε τα $k$-tuples των οποίων όλα τα $k$ στοιχεία είναι 0 ή $max$ αντίστοιχα.

Για τη διατύπωση της **πρότασης $\boldsymbol{\zeta}$** θεωρούμε ότι η μηχανή όταν αποδέχεται καθαρίζει την ταινία της και μετακινεί την κεφαλή της στη θέση 0, μπαίνοντας σε μία κατάσταση $q_f$. Αν $\gamma_f = (q_f, 0) \in \Gamma$, τότε η $\zeta$ διατυπώνεται ως εξής:

$$\zeta \equiv C_f(\vec{0}, \overrightarrow{max})$$

Η **πρόταση $\boldsymbol{\alpha}$** θα διατυπωθεί χρησιμοποιώντας τη μορφή δυαδικής αναπαράστασης δομών που εξηγήσαμε στην απόδειξη $FO \subseteq L$ της ενότητας 3.1. Ουσιαστικά θα αποτελείται από υπο-προτάσεις που θα έχουν το νόημα ότι «αν το κατηγόρημα εισόδου $R_i^j$ ισχύει για ένα συγκεκριμένο $j$-tuple, τότε το αντίστοιχο κελί θα περιέχει 1 για χρόνο 0». Παραλείπουμε τη διατύπωσή της επειδή είναι πολύ τεχνική και δε θεωρούμε ότι προσφέρει κάτι στην ουσία της απόδειξης.

Η **πρόταση $\boldsymbol{\beta}$** διατυπώνεται με αρκετά προφανή τρόπο. Αποτελεί τη σύζευξη όλων των προτάσεων της παρακάτω μορφής, για τα διάφορα $i, j$ με $i \neq j$.

$$\beta_{ij} \equiv (\forall \vec{s}, \vec{t}) \neg \left( C_i(\vec{s}, \vec{t}) \wedge C_j(\vec{s}, \vec{t}) \right)$$

Τέλος, θα ασχοληθούμε με τη διατύπωση της **πρότασης $\boldsymbol{\eta}$**, που είναι μάλλον η πιο περίπλοκη. Αρχικά, για να διευκολύνουμε τη διατύπωση της πρότασης, θα χρησιμοποιήσουμε τον παρακάτω συμβολισμό, ο οποίος θα σημαίνει ότι η τριάδα περιεχομένων κελιών $a_{-1}, a_0, a_1$ οδηγεί σε κελί $b$ μέσω κίνησης $\delta \in \{0,1\}$ της μηχανής $N$:

$$(a_{-1}, a_0, a_1, \delta) \overset{N}{\rightarrow} b$$

Θεωρούμε την παρακάτω πρόταση:

$$\eta_1 \equiv (\forall \vec{s}, \vec{t}) \left( (\vec{t} \neq \overrightarrow{max} \wedge \vec{0} < \vec{s} < \overrightarrow{max}) \right.$$
$$\rightarrow \bigwedge_{(a_{-1}, a_0, a_1, \delta) \overset{N}{\rightarrow} b} \Big( \Big( \delta = 1$$
$$\rightarrow \Big( \Big( \Delta(\vec{t}) \wedge C_{a_{-1}}(\vec{s} - 1, \vec{t}) \wedge C_{a_0}(\vec{s}, \vec{t}) \wedge C_{a_1}(\vec{s} + 1, \vec{t}) \Big) \rightarrow C_b(\vec{s}, \vec{t} + 1) \Big) \Big)$$
$$\wedge \Big( \delta = 0$$
$$\left. \rightarrow \Big( \Big( \neg \Delta(\vec{t}) \wedge C_{a_{-1}}(\vec{s} - 1, \vec{t}) \wedge C_{a_0}(\vec{s}, \vec{t}) \wedge C_{a_1}(\vec{s} + 1, \vec{t}) \Big) \rightarrow C_b(\vec{s}, \vec{t} + 1) \Big) \Big) \Big) \right)$$

Παρά την περιπλοκότητά της, η παραπάνω πρόταση διατυπώνει κάτι απλό: για κάθε tuple στοιχείων $(a_{-1}, a_0, a_1, \delta) \overset{N}{\rightarrow} b$, αν $\delta = 1$ τότε οι συνθήκες $\Delta(\vec{t}) \wedge C_{a_{-1}}(\vec{s} - 1, \vec{t}) \wedge C_{a_0}(\vec{s}, \vec{t}) \wedge C_{a_1}(\vec{s} + 1, \vec{t})$ οδηγούν το κελί $\vec{s}$ να έχει περιεχόμενο $b$ την επόμενη χρονική στιγμή (το ίδιο για $\delta = 0$, αλλά με $\neg\Delta(\vec{t})$). Επιπλέον, υποθέσαμε ότι το κελί $\vec{s}$ δεν είναι κάποιο εκ των δύο ακραίων και ο χρόνος $\vec{t}$ δεν αντιστοιχεί στην τελευταία χρονική στιγμή.

Με αντίστοιχο (απλούστερο) τρόπο μπορούμε να διατυπώσουμε δύο προτάσεις $\eta_0, \eta_2$ που να έχουν το ίδιο νόημα, αλλά για $\vec{s} = \vec{0}$ και $\vec{s} = \overrightarrow{max}$ αντίστοιχα. Τελικά θέτουμε:

$$\eta \equiv \eta_0 \wedge \eta_1 \wedge \eta_2$$

Έτσι, ολοκληρώσαμε την απόδειξη. ■

Ας παρατηρήσουμε ότι η πρόταση πρώτης τάξης $\varphi$ που χρησιμοποιείται στην απόδειξη περιέχει μόνο καθολικούς ποσοδείκτες. Αυτό θα έχει σημασία στο κεφάλαιο 6, όπου θα ασχοληθούμε με τη λογική περιγραφή της κλάσης $\#P$. Ωστόσο, ήδη αυτό αποτελεί ενδιαφέρουσα παρατήρηση, καθώς σημαίνει ότι για περιγραφή προβλημάτων της κλάσης $NP$ **μάς αρκεί καθολικός ποσοδείκτης για το πρωτοβάθμιο σκέλος**. Αντιθέτως, στο δευτεροβάθμιο σκέλος χρειαζόμαστε υπαρξιακό ποσοδείκτη, όπως έχουμε δει.

Υπενθυμίζεται ότι για αυτή τη διατύπωση της πρότασης $\varphi$ χρησιμοποιήσαμε έτοιμους τους όρους $\vec{0}$ και $\overrightarrow{max}$. Εάν δεν μας ήταν διαθέσιμοι αυτοί οι όροι, θα χρειαζόμασταν και **υπαρξιακό ποσοδείκτη για τη διατύπωση ύπαρξης ελάχιστου και μέγιστου στοιχείου**. Αυτό επίσης θα έχει σημασία για το κεφάλαιο 6.

Ένα σημαντικό πόρισμα του θεωρήματος, σε συνδυασμό με την αντίστοιχη μελέτη που κάναμε παραπάνω για την κλάση $P$, είναι ότι οι κλάσεις $P$ και $NP$ ταυτίζονται αν και μόνο αν οι αντίστοιχες λογικές τους έχουν την ίδια εκφραστικότητα. Πιο συγκεκριμένα, **είναι $\boldsymbol{P} = \boldsymbol{NP}$ αν και μόνο αν είναι $\boldsymbol{FO}(\boldsymbol{LFP}) = \boldsymbol{SO}\exists$ για πεπερασμένες και διατεταγμένες δομές**.

Βλέπουμε λοιπόν ότι η περιγραφική πολυπλοκότητα προσφέρει μια εναλλακτική οπτική στο περίφημο ανοιχτό πρόβλημα για την ισότητα των κλάσεων $P$ και $NP$, ανάγοντας το πρόβλημα σε σύγκριση εκφραστικότητας δύο λογικών.

# 4. Προβλήματα Μέτρησης (Counting Problems) – #P

## 4.1. Κλάσεις #P και FP

### 4.1.1. Ορισμοί

Με τον όρο *προβλήματα μέτρησης* ή *μετρητικά προβλήματα* (counting problems) αναφερόμαστε σε προβλήματα στα οποία μας ενδιαφέρει να βρούμε το πλήθος των λύσεων, δηλαδή το πλήθος των δυνατών τρόπων να επιτευχθεί κάποιος στόχος. Η κλάση $\#P$ άτυπα αποτελεί το σύνολο των προβλημάτων μέτρησης που προκύπτουν από ένα αντίστοιχο πρόβλημα της κλάσης $NP$.

Για να διασαφηνίσουμε τι σημαίνει αυτό, ας πάρουμε για παράδειγμα κάποια προβλήματα της κλάσης $NP$. Στο πρόβλημα $CNF$ μάς ενδιαφέρει εάν είναι ικανοποιήσιμη μία πρόταση λογικής εκφρασμένη σε κανονική συζευκτική μορφή. Στο αντίστοιχο πρόβλημα μέτρησης μάς ενδιαφέρει *πόσες* αναθέσεις μεταβλητών ικανοποιούν την αντίστοιχη πρόταση. Παρομοίως, στο μετρητικό πρόβλημα για 3-χρωματισμούς γραφημάτων μάς ενδιαφέρει πόσοι έγκυροι 3-χρωματισμοί υπάρχουν για κάποιο γράφημα.

Θα παρουσιάσουμε τον αυστηρό ορισμό της κλάσης $\#P$, όπως διατυπώθηκε για πρώτη φορά από τον Leslie Valiant το 1979 [Val79]. Για αυτό το σκοπό θα ορίσουμε πρώτα την έννοια των *μετρητικών μηχανών Turing*.

Ορισμός (Μετρητική Μηχανή Turing)

Μια μετρητική μηχανή Turing (counting Turing machine) ορίζεται ως μια κλασική μη ντετερμινιστική μηχανή Turing, η οποία επιπλέον διαθέτει τη δυνατότητα να γράφει σε μια ξεχωριστή ταινία τη δυαδική αναπαράσταση του πλήθους των μονοπατιών που καταλήγουν σε αποδοχή. Αυτή η διαδικασία εκτελείται στιγμιαία, χωρίς να αυξάνει την υπολογιστική πολυπλοκότητα.

Ορισμός (Κλάση $\#P$)

Η κλάση $\#P$ ορίζεται ως το σύνολο των συναρτήσεων $f\colon\{0,1\}^* \to \{0,1\}^*$ που είναι υπολογίσιμες από μετρητική μηχανή Turing πολυωνυμικού χρόνου.

Είναι αρκετά προφανές ότι ένα πρόβλημα της κλάσης $\#P$ είναι οπωσδήποτε δυσκολότερο από το αντίστοιχο της κλάσης $NP$, αφού λύνοντας το πρώτο προκύπτει η απάντηση και για το δεύτερο, ελέγχοντας αν το πλήθος των λύσεων είναι μεγαλύτερο του μηδενός.

Παρακάτω ορίζουμε την κλάση $FP$, η οποία ουσιαστικά είναι το ανάλογο της $P$ για μετρητικά προβλήματα, δηλαδή περιέχει τα μετρητικά προβλήματα που επιλύονται σε πολυωνυμικό χρόνο.

<u>Ορισμός (Κλάση FP)</u>

Η κλάση FP ορίζεται ως το σύνολο των συναρτήσεων $f: \{0,1\}^* \to \{0,1\}^*$ που είναι υπολογίσιμες από ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου.

Σημειώνουμε ότι αποτελεί ανοιχτό πρόβλημα εάν ισχύει $\#P = FP$ [AB09]. Μάλιστα, εάν αυτή η ισότητα ισχύει, τότε θα είναι και $P = NP$, καθώς όπως ήδη αναφέραμε τα προβλήματα της $\#P$ είναι δυσκολότερα από τα αντίστοιχα της $NP$.

Παρακάτω θα μελετήσουμε μερικά προβλήματα της κλάσης $\#P$ και θα δούμε ότι ίσως να είναι δυσκολότερα από ό,τι θα αναμέναμε.

## 4.1.2. Πρόβλημα #CYCLE

Ας πάρουμε για παράδειγμα το πρόβλημα $\#CYCLE$ της κλάσης #P (μέτρηση απλών κύκλων κατευθυνόμενου γραφήματος). Υπενθυμίζουμε ότι το αντίστοιχο πρόβλημα απόφασης (εύρεση ενός κύκλου σε κατευθυνόμενο γράφημα) λύνεται αρκετά εύκολα σε γραμμικό χρόνο με διάσχιση κατά βάθος, αναζητώντας μια «πίσω ακμή» (back edge).

Πιθανόν να αναμέναμε ότι ένα τέτοιο πρόβλημα δεν θα είναι ιδιαίτερα δύσκολο, ωστόσο έχει αποδειχθεί ότι αν είναι $\#CYCLE \in FP$ τότε είναι $P = NP$ [AB09]. Αυτό φυσικά σημαίνει ότι *πιθανότατα* δεν ισχύει $\#CYCLE \in FP$. Η απόδειξη για αυτή την πρόταση στηρίζεται στο γεγονός ότι μπορούμε να ανάγουμε το πρόβλημα εύρεσης κύκλου Hamilton, το οποίο ως γνωστόν είναι $NP$-complete, στο $\#CYCLE$.

Η αναγωγή πραγματοποιείται αντικαθιστώντας κάθε ακμή ενός κατευθυνόμενου γραφήματος με ένα συγκεκριμένο μη κατευθυνόμενο γράφημα, καταλήγοντας σε ένα γράφημα στο οποίο η ύπαρξη κύκλου Hamilton καθορίζεται από το πλήθος απλών κύκλων που περιείχε το αρχικό γράφημα. Αυτό συνεπάγεται ότι το πρόβλημα Hamilton λύνεται σε πολυωνυμικό χρόνο, εάν ισχύει $\#CYCLE \in FP$. Αν αυτό ίσχυε, θα ήταν $P = NP$, επειδή το πρόβλημα Hamilton είναι $NP$-complete.

Παρατηρούμε λοιπόν ότι η δυσκολία των μετρητικών προβλημάτων δεν είναι ακριβώς ανάλογη της δυσκολίας των αντίστοιχων προβλημάτων απόφασης. Αυτό θα επιβεβαιωθεί και στις επόμενες ενότητες, στις οποίες θα δούμε και ότι κάποια $\#P$-πλήρη προβλήματα μπορεί να μας έδιναν την εντύπωση ότι είναι πιο εύκολα από ό,τι είναι στην πραγματικότητα.

Μάλιστα, όπως θα δούμε στη συνέχεια, αυτό μας οδηγεί στο να ασχοληθούμε με *προσεγγιστικούς αλγόριθμους*, καθώς τα περισσότερα προβλήματα της κλάσης $\#P$ δεν φαίνεται να μπορούν να λυθούν αποδοτικά με αλγόριθμους που προσδιορίζουν ακριβώς το πλήθος των ζητούμενων λύσεων.

### 4.1.3. Πρόβλημα #MATCHING

Ας πάρουμε τώρα για παράδειγμα το πρόβλημα $MATCHING$, που αφορά την ύπαρξη τέλειου ταιριάσματος σε διμερή γραφήματα. Το πρόβλημα αυτό επιλύεται σε πολυωνυμικό χρόνο και επομένως ανήκει στην κλάση $P$ [Pap94]. Μάλιστα, το πρόβλημα αυτό μπορεί να αναχθεί σε υπολογισμό της ορίζουσας του πίνακα γειτνίασης του γραφήματος (τοποθετώντας το ένα μέρος του γραφήματος στις γραμμές και το άλλο στις στήλες).

Για να δούμε τη σύνδεση αυτού του προβλήματος με την έννοια της ορίζουσας, πρέπει να το σκεφτούμε ως εξής. Έχουμε δύο ομάδες $n$ αριθμημένων κόμβων (από 1 έως $n$) και θέλουμε να δημιουργήσουμε ζεύγη κόμβων ανάμεσα στις δυο ομάδες, με τρόπο τέτοιο ώστε να υπάρχει ακμή ανάμεσα σε κάθε ζεύγος. Μπορούμε να σκεφτούμε ότι κρατάμε την πρώτη αριθμημένη ομάδα σταθερή και εφαρμόζουμε μεταθέσεις στη δεύτερη. Αν με κάποια μετάθεση κάθε ζεύγος κόμβων με ίδιο αριθμό έχει ακμή μεταξύ του, τότε υπάρχει τέλειο ταίριασμα στο γράφημα.

Αν όμως υπάρχει τέτοια μετάθεση, μπορούμε αρκετά εύκολα να δούμε ότι η ορίζουσα του πίνακα γειτνίασης θα έχει τουλάχιστον έναν μη μηδενικό όρο στο άθροισμά της. Αυτό προκύπτει από τον ορισμό της ορίζουσας, ο οποίος μάλιστα χρησιμοποιεί μέσα του την έννοια της μετάθεσης. Επομένως, για να μην υπάρχει τέλειο ταίριασμα θα πρέπει όλοι οι όροι της ορίζουσας να είναι $0$.

Αν αντικαταστήσουμε κάθε ‘1’ του πίνακα γειτνίασης με μια μεταβλητή $x_{ij}$ (διαφορετική για κάθε θέση), τότε αρκεί να υπολογίσουμε την ορίζουσα και να ελέγξουμε εάν ισούται ταυτοτικά με $0$, το οποίο μπορεί να γίνει σε πολυωνυμικό χρόνο.

Φαίνεται ότι το αντίστοιχο μετρητικό πρόβλημα $\#MATCHING$ ίσως να μπορούσε να υπολογιστεί με κάποιο παρόμοιο τρόπο, μετρώντας τους μη μηδενικούς όρους της ορίζουσας. Για να αυστηροποιήσουμε αυτή την ιδέα θα χρειαστούμε την έννοια του “permanent” ενός πίνακα, το οποίο θα δούμε σε επόμενη ενότητα.

Όπως θα δούμε, τελικά αυτή η ιδέα για το $\#MATCHING$ είναι μάλλον αποτυχημένη για την επίλυση του προβλήματος, ωστόσο μας οδηγεί στη διαπίστωση ότι πολλές φορές δεν μπορούμε να λύσουμε τα προβλήματα της κλάσης $\#P$ με τρόπο που μας θυμίζει την αντιμετώπισή μας προς το αντίστοιχο πρόβλημα απόφασης. Σύμφωνα με όσα θα δούμε στη συνέχεια, το φαινομενικά απλό πρόβλημα $\#MATCHING$ όχι μόνο είναι $\#P$-πλήρες, αλλά φαίνεται να είναι δύσκολο και για ολόκληρη την πολυωνυμική ιεραρχία.

## 4.2. #P-Πληρότητα (#P-Completeness)

### 4.2.1. Ορισμοί

Όπως θα αναμέναμε, ως $\#P$-complete χαρακτηρίζονται τα «δυσκολότερα» προβλήματα της κλάσης $\#P$, δηλαδή εκείνα για τα οποία αν βρεθεί πολυωνυμικός αλγόριθμος, τότε θα ισχύει $\#P = FP$. Για τον τυπικό ορισμό της έννοιας $\#P$-completeness χρησιμοποιούνται *oracle Turing machines*. Ουσιαστικά αυτό σημαίνει ότι έχουμε μηχανές Turing οι οποίες μπορούν σε ένα υπολογιστικό βήμα να κάνουν ερώτηση σε ένα μαντείο και να λάβουν απάντηση για την τιμή μιας συνάρτησης. Για παράδειγμα, για συνάρτηση $f$, το σύνολο $FP^f$ ορίζεται ως το σύνολο των συναρτήσεων που είναι υπολογίσιμες σε πολυωνυμικό χρόνο από ντετερμινιστική μηχανή Turing, η οποία έχει πρόσβαση σε μαντείο για τη συνάρτηση $f$.

Με βάση αυτό τον ορισμό, μπορούμε να αυστηροποιήσουμε την έννοια της $\#P$ πληρότητας ως εξής [AB09]:

Ορισμός ($\#P$-πληρότητα)

Μια συνάρτηση $f$ είναι $\#P$-πλήρης εάν ισχύει $f \in \#P$ και για κάθε $g \in \#P$ είναι $g \in FP^f$.

Ουσιαστικά αυτό σημαίνει ότι κάθε συνάρτηση $g \in \#P$ θα μπορούσε να υπολογιστεί σε πολυωνυμικό χρόνο, εάν μπορούσαμε να υπολογίσουμε την $f$ στιγμιαία.

Όπως πιθανόν θα αναμέναμε, πολλά $NP$-complete προβλήματα δίνουν $\#P$-complete προβλήματα, εάν τα μετατρέψουμε σε προβλήματα μέτρησης με τον τρόπο που παρουσιάσαμε πρωτύτερα. Ένα τέτοιο πρόβλημα είναι το $\#SAT$ ή $\#3SAT$ [Pap94] [AB09], στο οποίο μας ενδιαφέρει να μετρήσουμε πόσοι συνδυασμοί αληθοτιμών ικανοποιούν μία πρόταση. Ωστόσο, παρουσιάζει ενδιαφέρον ότι **υπάρχουν και προβλήματα που ανήκουν στην κλάση $P$, των οποίων τα αντίστοιχα μετρητικά προβλήματα είναι $\#P$-complete**.

### 4.2.2. Πρόβλημα Permanent – Το Θεώρημα του Valiant

Στη γραμμική άλγεβρα, το *permanent* ενός $n \times n$ πίνακα ορίζεται παρόμοια με την ορίζουσα, όπως φαίνεται παρακάτω.

Ορισμός (Permanent πίνακα)

"Permanent" ενός $n \times n$ πίνακα $a_{ij}$ καλείται η παρακάτω ποσότητα:

$$perm(a_{ij}) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Διευκρινίζουμε ότι με $S_n$ συμβολίζεται η ομάδα μεταθέσεων των αριθμών $1, \ldots, n$. Ουσιαστικά η μοναδική διαφορά από την ορίζουσα είναι ότι απουσιάζει η εναλλαγή προσήμου στους όρους του αθροίσματος. Για παράδειγμα σε πίνακα $2 \times 2$ έχουμε:

$$perm\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad + bc$$

Όπως είδαμε και πρωτύτερα, ο υπολογισμός του permanent ενός πίνακα σχετίζεται στενά με το πρόβλημα $\#MATCHING$.

Συγκεκριμένα, για να έχουμε ισοδυναμία ανάμεσα στα δύο προβλήματα θα πρέπει να περιορίσουμε τους πίνακές μας σε πίνακες με στοιχεία 0 και 1. Έτσι, θα μιλάμε για το πρόβλημα *01-permanent*. Σύμφωνα με όσα αναφέρθηκαν πρωτύτερα για το πρόβλημα $\#MATCHING$ είναι φανερό ότι τα δύο προβλήματα είναι ισοδύναμα, δηλαδή εάν θέλουμε να υπολογίσουμε το πλήθος ταιριασμάτων ενός διμερούς γραφήματος αρκεί να υπολογίσουμε το permanent του πίνακα γειτνίασης, ενώ για το αντίστροφο μπορούμε να κατασκευάσουμε το γράφημα από τον πίνακα.

Σε αυτό το σημείο θα παρουσιάσουμε το θεώρημα του Valiant, που αποδείχθηκε από τον Leslie Valiant το 1979 στην ίδια δημοσίευση στην οποία ορίστηκε η κλάση $\#P$ [Val79].

Θεώρημα (Valiant)

Το πρόβλημα 01-permanent είναι $\#P$-πλήρες.

Αναφέρουμε ότι η απόδειξη του θεωρήματος μπορεί να γίνει με αναγωγή του $\#SAT$ (ή του $\#3SAT$) στο 01-permanent [Pap94] [AB09], ωστόσο την παραλείπουμε για συντομία. Σημειώνουμε ότι τα $\#SAT$ και $\#3SAT$ είναι $\#P$-complete.

Το παραπάνω θεώρημα θα λέγαμε ότι είναι μη αναμενόμενο από διάφορες απόψεις. Πρώτον, μας διασφαλίζει τη δυσκολία του προβλήματος $\#MATCHING$ και μας δείχνει με χειροπιαστό τρόπο ότι για κάποια counting problems δεν έχει νόημα να προσπαθήσουμε να σκεφτούμε τεχνάσματα που θα χρησιμοποιούσαμε στα αντίστοιχα προβλήματα απόφασης.

Δεύτερον, το θεώρημα αυτό μας δείχνει ότι *πιθανότατα* ο υπολογισμός permanent είναι πολύ δυσκολότερος από τον υπολογισμό οριζουσών (εκτός αν ισχύει $P = NP$). Αυτό από μόνο του είναι ένα αρκετά αξιοπερίεργο πόρισμα, καθώς ο ορισμός του permanent μοιάζει με τον ορισμό της ορίζουσας και μάλιστα είναι απλούστερος, παραλείποντας την εναλλαγή προσήμου αναλόγως με το αν η μετάθεση είναι άρτια ή περιττή. Φυσικά, μπορούμε εύκολα να διαπιστώσουμε ότι αυτή η διαφορά δυσκολίας υπολογισμού οφείλεται στις γνωστές ιδιότητες της ορίζουσας, οι οποίες μας δίνουν τη δυνατότητα να την υπολογίσουμε απαλείφοντας γραμμές και στήλες για να καταλήξουμε σε τριγωνικό πίνακα.

## 4.3. Το Θεώρημα του Toda

Μέχρι τώρα έχουμε δει ότι η κλάση $\#P$ περιέχει προβλήματα πολύ δυσκολότερα από την κλάση $NP$. Έτσι, προκύπτει φυσικά το ερώτημα του πώς συγκρίνεται η δυσκολία της $\#P$ με άλλες υπερκλάσεις της $NP$.

Ο Seinosuke Toda στη δημοσίευσή του το 1991 [Tod91] απέδειξε το θεώρημα που θα παρουσιάσουμε, το οποίο απαντά σε αυτό το ερώτημα. Σε αυτή τη δημοσίευση μελετώνται οι κλάσεις $PP$ (probabilistic polynomial time) και $\oplus P$ ("parity P") και συγκρίνονται ως προς τη δυσκολία τους με την πολυωνυμική ιεραρχία $PH$ [Sto77].

Σε αυτό το σημείο δεν κρίνεται σκόπιμο να παρουσιάσουμε τους αυστηρούς ορισμούς αυτών των κλάσεων και να τις μελετήσουμε σε βάθος, ωστόσο θα αναφέρουμε ότι οι $PP$ και $\oplus P$ ισοδυναμούν με τον υπολογισμό του περισσότερο και λιγότερο σημαντικού bit συναρτήσεων της κλάσης $\#P$ [AB09]. Για τον αυστηρό ορισμό της κλάσης $PP$ χρησιμοποιούνται "randomized Turing machines" [Jan98]. Μπορούμε άτυπα να πούμε ότι η $PP$ περιέχει τα προβλήματα απόφασης που λύνονται σε πολυωνυμικό χρόνο από τυχαίο αλγόριθμο που απαντά ορθά με πιθανότητα μεγαλύτερη από $1/2$ σε όλες τις περιπτώσεις.

Σημειώνουμε ότι στο θεώρημα θα χρησιμοποιήσουμε το συμβολισμό με τις κλήσεις σε μαντείο, ο οποίος χρησιμοποιήθηκε ήδη στον ορισμό της $\#P$-πληρότητας.

<u>Θεώρημα (Toda)</u>

(1) Η πολυωνυμική ιεραρχία μπορεί να λυθεί σε πολυωνυμικό χρόνο, έχοντας πρόσβαση σε μαντείο για την κλάση $PP$, δηλαδή:

$$PH \subseteq P^{PP}$$

(2) Η πολυωνυμική ιεραρχία μπορεί να λυθεί σε πολυωνυμικό χρόνο, με μία μόνο κλήση σε μαντείο για την κλάση $\#P$, δηλαδή:

$$PH \subseteq P^{\#P[1]}$$

Το παραπάνω είναι ένα αρκετά ισχυρό θεώρημα που μας παρέχει μια «σύγκριση» για την ισχύ διαφόρων δύσκολων κλάσεων. Παραλείπουμε την απόδειξη, ωστόσο θα αναφέρουμε ότι οι δύο παραπάνω προτάσεις σχετίζονται μεταξύ τους.

## 5. Προσεγγιστικοί Αλγόριθμοι για Μετρητικά Προβλήματα

Στις προηγούμενες ενότητες είδαμε με παραδείγματα ότι αν δεν ισχύει $P = NP$, τότε τα προβλήματα της κλάσης $\#P$ είναι εν γένει πολύ δύσκολα, σε αρκετές περιπτώσεις μάλιστα δυσκολότερα από όσο θα περιμέναμε. Εφόσον τα μετρητικά προβλήματα ουσιαστικά αποτελούν υπολογισμό συναρτήσεων, προκύπτει με φυσικό τρόπο το ερώτημα αν αυτά γίνεται να λυθούν προσεγγιστικά. Σε περίπτωση που αυτό γίνεται, θα μας ενδιέφερε πόσο γρηγορότερη είναι μια προσεγγιστική λύση σε σύγκριση με την αντίστοιχη κλασική, καθώς και πόσο ισχυρές εγγυήσεις έχει για την ακρίβειά της.

### 5.1. Ορισμοί

Σε αυτή την ενότητα θα παρουσιάσουμε ορισμένα είδη προσεγγιστικών αλγορίθμων που θα μας χρησιμεύσουν στη συνέχεια.

Ορισμός (PRAS)

Ένας αλγόριθμος $A$ με τυχαιότητα καλείται *polynomial-time randomized approximation scheme* (PRAS) εάν για κάθε $0 < \varepsilon < 1$ προσεγγίζει μια συνάρτηση $f(x)$ εντός ενός παράγοντα $1 \pm \varepsilon$ με μεγάλη πιθανότητα (συμβατικά, συνήθως απαιτούμε πιθανότητα $\geq 3/4$) και χρόνο πολυωνυμικό ως προς το μέγεθος της εισόδου $x$. Δηλαδή:

$$\Pr[(1-\varepsilon)f(x) \leq A(x) \leq (1+\varepsilon)f(x)] \geq \frac{3}{4}, \qquad A \sim poly(|x|)$$

Ένα πρόβλημα με αυτό τον ορισμό είναι ότι δεν λαμβάνει υπόψη του ότι η χρονική πολυπλοκότητα του αλγορίθμου μπορεί να εξαρτάται από την ακρίβεια προσέγγισης (και μάλιστα σε μερικές περιπτώσεις να είναι απαγορευτικό να έχουμε μεγάλη ακρίβεια). Για αυτό το λόγο συνήθως είναι χρησιμότερος ο παρακάτω ορισμός:

Ορισμός (FPRAS)

Ένας αλγόριθμος $A$ με τυχαιότητα καλείται *fully polynomial-time randomized approximation scheme* (FPRAS) εάν για κάθε $0 < \varepsilon, \delta < 1$ προσεγγίζει μια συνάρτηση $f(x)$ εντός ενός παράγοντα $1 \pm \varepsilon$, με πιθανότητα σφάλματος το πολύ $\delta$ και χρόνο πολυωνυμικό ως προς το μέγεθος της εισόδου $x$, αλλά και τα $\log 1/\delta$, $1/\varepsilon$. Δηλαδή:

$$\Pr[(1-\varepsilon)f(x) \leq A(x) \leq (1+\varepsilon)f(x)] \geq 1-\delta, \qquad A \sim poly\left(|x|, \log\frac{1}{\delta}, \frac{1}{\varepsilon}\right)$$

Στον παραπάνω ορισμό απαιτήσαμε ο αλγόριθμος να είναι πολυωνυμικός και ως προς την πιθανότητα σφάλματος και ως προς την ακρίβεια του υπολογισμού [AB09].

Σημειώνουμε ότι η έννοια FPRAS δεν ορίζεται πάντα ακριβώς έτσι. Στη βιβλιογραφία εμφανίζονται αρκετές μικρές διαφοροποιήσεις, π.χ. μερικές φορές απουσιάζουν οι λογάριθμοι από την πολυωνυμική εξάρτηση ή **παραλείπεται τελείως η απαίτηση για πολυωνυμική εξάρτηση από την πιθανότητα σφάλματος $\delta$** [Vaz04] [ACJR21]. Επίσης, ορισμένες φορές μπορεί η ίδια έννοια να αναφέρεται ως 'FPTRAS' [SST95]. Επιλέξαμε να παρουσιάσουμε αυτό τον ορισμό επειδή είναι πληρέστερος, ωστόσο στη συνέχεια μπορεί να μην τον ακολουθούμε κατά γράμμα.

Παρουσιάζει ενδιαφέρον το γεγονός ότι αν ισχύει $P = NP$, τότε όλα τα προβλήματα της $\#P$ επιδέχονται FPRAS, αλλά και FPTAS (ντετερμινιστικό *fully polynomial-time approximation scheme*) [AB09].

## 5.2. FPRAS για Μετρητικά Προβλήματα

Ένα ενδιαφέρον ερώτημα είναι ποια προβλήματα της $\#P$ μπορούν να λυθούν προσεγγιστικά σε πολυωνυμικό χρόνο. Σε αυτή την ενότητα θα δούμε ότι το πρόβλημα $\#DNF$ διαθέτει FPRAS [KLM89], παρόλο που είναι $\#P$-πλήρες. Ωστόσο, αυτό δεν σημαίνει ότι κάθε $\#P$-πλήρες πρόβλημα διαθέτει FPRAS.

Στο επόμενο κεφάλαιο, όπου θα ασχοληθούμε με περιγραφική πολυπλοκότητα για μετρητικά προβλήματα, θα δούμε με περισσότερη λεπτομέρεια κάποια συμπεράσματα για το ποια προβλήματα της κλάσης $\#P$ διαθέτουν FPRAS.

### 5.2.1. Προβλήματα #DNF και #CNF – Πληρότητα

Υπενθυμίζουμε ότι το πρόβλημα απόφασης $DNF$ (ικανοποιησιμότητα για προτάσεις σε κανονική διαζευκτική μορφή) επιλύεται σε πολυωνυμικό χρόνο. Μάλιστα η λύση του είναι πολύ απλή και προφανής: εάν κάποια από τις συζεύξεις δεν περιέχει αντίφαση (δηλαδή $a \wedge \neg a$), τότε εκείνη η σύζευξη είναι ικανοποιήσιμη και επομένως ολόκληρη η πρόταση είναι επίσης ικανοποιήσιμη.

Αντιθέτως, το πρόβλημα $CNF$ (ικανοποιησιμότητα για προτάσεις σε κανονική συζευκτική μορφή) είναι $NP$-πλήρες. Μπορούμε μάλιστα να προσέξουμε ότι το πρόβλημα αυτό είναι ισοδύναμο με το πρόβλημα “falsifiability” για προτάσεις κανονικής διαζευκτικής μορφής (δηλαδή εάν υπάρχει συνδυασμός αληθοτιμών που να καθιστά την πρόταση ψευδή). Αυτό συμβαίνει επειδή η άρνηση μιας πρότασης CNF μετατρέπεται με τον κανόνα De Morgan σε πρόταση DNF και αντιστρόφως. Επομένως, και αυτό το πρόβλημα είναι $NP$-complete.

Στα αντίστοιχα μετρητικά προβλήματα για ικανοποιησιμότητα προτάσεων μάς ενδιαφέρει να μετρήσουμε πόσοι συνδυασμοί αληθοτιμών ικανοποιούν μία πρόταση. Με βάση τα παραπάνω, θα αναμέναμε το πρόβλημα $\#DNF$ να είναι ευκολότερο από το $\#CNF$. Για αυτό μάλλον αποτελεί έκπληξη ότι και τα δύο είναι $\#P$-πλήρη. Παρόλα αυτά, μπορούμε εύκολα να αποδείξουμε ότι αυτά τα δυο προβλήματα είναι εξίσου δύσκολα, βασιζόμενοι στην ίδια περίπου ιδέα που χρησιμοποιήσαμε για το πρόβλημα DNF falsifiability.

Συγκεκριμένα, αν πάρουμε την άρνηση μιας πρότασης CNF με $n$ μεταβλητές, αυτή μετατρέπεται σε πρόταση DNF ίδιου μεγέθους με τον κανόνα De Morgan. Αν η δεύτερη πρόταση έχει $k$ συνδυασμούς αληθοτιμών που την ικανοποιούν, τότε η πρώτη θα έχει ακριβώς $2^n - k$ συνδυασμούς που την ικανοποιούν. Με αυτό τον τρόπο έχουμε αναγάγει το $\#CNF$ (ή $\#SAT$) στο $\#DNF$.

Βλέπουμε λοιπόν ότι τα $\#DNF$ και $\#CNF$ είναι ουσιαστικά ισοδύναμα, παρόλο που δε φαίνεται να ισχύει το ίδιο για τα αντίστοιχα προβλήματα απόφασης. Βέβαια, τα δύο αυτά προβλήματα δεν φαίνεται να έχουν την ίδια δυσκολία όταν αναφερόμαστε σε προσεγγιστικούς αλγορίθμους. Όπως θα δούμε στη συνέχεια, το πρόβλημα $\#DNF$ διαθέτει FPRAS, ενώ το $\#CNF$ *πιθανότατα* όχι, καθώς η ύπαρξη του δεύτερου θα συνεπαγόταν ότι ισχύει $RP = NP$ [SST95].

Για τον αυστηρό ορισμό της κλάσης $RP$ (randomized polynomial time) χρησιμοποιούνται “randomized Turing machines” [Jan98]. Ωστόσο, μπορούμε άτυπα να πούμε ότι περιέχει τα προβλήματα απόφασης που λύνονται σε πολυωνυμικό χρόνο από τυχαίο αλγόριθμο που απαντά ορθά με πιθανότητα μεγαλύτερη από $1/2$ σε περίπτωση που θα έπρεπε να απαντήσει θετικά, ενώ απαντά πάντοτε ορθά σε περίπτωση που θα έπρεπε να απαντήσει αρνητικά.

Σημειώνουμε ότι αυτή η διαφορά δυσκολίας ανάμεσα στα $\#DNF$ και $\#CNF$ δεν οφείλεται απαραίτητα στο ότι το $CNF$ είναι $NP$-πλήρες ενώ το $DNF$ όχι, καθώς υπάρχουν προβλήματα της κλάσης $P$ για τα οποία τα αντίστοιχα μετρητικά προβλήματα δεν φαίνεται να διαθέτουν FPRAS.

### 5.2.2. FPRAS για το Πρόβλημα #DNF

Μια πρώτη ιδέα για να προσεγγίσουμε το πλήθος λύσεων $DNF$ είναι να χρησιμοποιήσουμε *δειγματοληψία* (sampling), δηλαδή να επιλέξουμε ομοιόμορφα κάποιες αποτιμήσεις των λογικών μεταβλητών της πρότασης και, ύστερα από πολλές επαναλήψεις (έστω $t$ σε πλήθος), να υπολογίσουμε το ποσοστό των αποτιμήσεων που κατέστησαν την πρόταση αληθή. Πολλαπλασιάζοντας με το πλήθος όλων των δυνατών αποτιμήσεων (δηλαδή $2^n$, όπου $n$ το πλήθος των μεταβλητών), έχουμε μια εκτίμηση για το πλήθος των λύσεων.

Η εκτίμηση που λαμβάνουμε από αυτή τη διαδικασία έχει πράγματι τη ζητούμενη μέση τιμή, ωστόσο διαθέτει ένα σοβαρό πρόβλημα. Αρχικά, είναι προφανές ότι αυξάνοντας το πλήθος $t$ των επαναλήψεων βελτιώνεται η ακρίβεια. Ωστόσο, ο λόγος που επιδιώκουμε να προσεγγίσουμε ένα πρόβλημα σαν το $\#DNF$ είναι για να έχουμε μια λύση που θα είναι πιο αποδοτική χρονικά, συγκριτικά με αντίστοιχες μη-προσεγγιστικές λύσεις, οι οποίες μάλλον θα είχαν εκθετική πολυπλοκότητα. Επομένως είναι εύλογο να περιορίσουμε το εύρος τιμών που μπορεί να πάρει το $t$, ώστε να εξασφαλίσουμε πολυωνυμική πολυπλοκότητα.

Για αυτό το σκοπό ας θεωρήσουμε ότι το $t$ είναι πολυωνυμικό ως προς το $n$. Το πρόβλημα με αυτή την υπόθεση είναι ότι αυτό μπορεί να οδηγήσει σε πολύ ανακριβή προσέγγιση. Για παράδειγμα, αν το πλήθος συνδυασμών αληθοτιμών που ικανοποιούν την πρόταση είναι επίσης πολυωνυμικό ως προς το $n$, τότε με πολυωνυμικό πλήθος δειγμάτων είναι πολύ πιθανό να μην πετύχουμε καμία αποτίμηση που να ικανοποιεί την πρόταση, και επομένως να λάβουμε προσέγγιση ίση με 0.

Παρακάτω θα παρουσιάσουμε την ιδέα που προτείνει ο Vijay Vazirani [Vaz04] για τη διόρθωση αυτού του σφάλματος. Αρχικά, ορίζουμε τα εξής μεγέθη:

- $n$: το πλήθος των μεταβλητών της πρότασης DNF
- $x_1, \dots, x_n$: οι αντίστοιχες μεταβλητές
- $C_i$: το $i$-οστό “clause” της πρότασης, δηλαδή η $i$-οστή υπο-πρόταση από αυτές ανάμεσα στις οποίες εφαρμόζεται διάζευξη
- $S_i$: το σύνολο των αναθέσεων αληθοτιμών στις $x_1, \dots, x_n$ που ικανοποιούν το $C_i$
- $r_i$: το πλήθος των “literals” (δηλαδή ατόμων με ή χωρίς άρνηση, ανάμεσα στα οποία εφαρμόζεται σύζευξη) που περιέχει το $C_i$
- $c(\tau)$: το πλήθος των $C_i$ που ικανοποιεί η ανάθεση αληθοτιμών $\tau$
- $M$: η “multiset” ένωση των $S_i$, δηλαδή η ένωση των $S_i$ με τρόπο τέτοιο ώστε κάθε στοιχείο (ανάθεση) να εμφανίζεται στο $M$ τόσες φορές όσες στα $S_i$
- $\#f$: το πλήθος αναθέσεων αληθοτιμών της πρότασης DNF που ενδιαφερόμαστε να προσεγγίσουμε

Παρατηρούμε ότι, σύμφωνα με τους παραπάνω ορισμούς, ισχύουν τα εξής:

- Κάθε ανάθεση $\tau$ περιέχεται στο $M$ $c(\tau)$ φορές.
- Είναι $|S_i| = 2^{n-r_i}$.
- Είναι $|M| = \sum_i |S_i|$.

Παρατηρούμε επιπλέον ότι τα $|S_i|$ (και επομένως και το $|M|$) υπολογίζονται εύκολα.

Για την προσέγγιση της $\#f$ θα ακολουθήσουμε την παρακάτω διαδικασία:

- Επιλέγουμε ένα clause $C_i$ με πιθανότητα:
$$p(C_i) = \frac{|S_i|}{|M|}$$
Όπως εξηγήσαμε, τα $|S_i|, |M|$ υπολογίζονται εύκολα.
- Για το $C_i$ που επιλέξαμε, διαλέγουμε ομοιόμορφα μία από τις $|S_i|$ αναθέσεις αληθοτιμών που το ικανοποιούν.
- Με αυτό τον τρόπο, έχουμε επιλέξει μια ανάθεση αληθοτιμών $\tau$ με πιθανότητα:

$$p(\tau) = \sum_{i:\, \tau\ \iota\kappa\alpha\nu o\pi o\iota\varepsilon\acute{\iota}\ C_i} p(C_i) \cdot \frac{1}{|S_i|} = \sum_{i:\, \tau\ \iota\kappa\alpha\nu o\pi o\iota\varepsilon\acute{\iota}\ C_i} \frac{1}{|M|} = \frac{c(\tau)}{|M|}$$

Επαναλαμβάνοντας την παραπάνω διαδικασία, έχουμε μια αποδοτική προσέγγιση για την τιμή $p(\tau)$. Παρατηρούμε ότι η μέση τιμή της ποσότητας $X(\tau) = 1/p(\tau)$ είναι ίση με την $\#f$:

$$E[X] = \sum_{\tau} p(\tau)\, X(\tau) = \sum_{\tau\ \iota\kappa\alpha\nu o\pi o\iota\varepsilon\acute{\iota}\ \kappa\acute{\alpha}\pi o\iota o\ C_i} 1 = \#f$$

Σημειώνουμε ότι η ποσότητα $X(\tau)$ ορίστηκε θεωρώντας ότι έχουμε ήδη επιλέξει κάποια ανάθεση $\tau$ με πιθανότητα $p(\tau)$, επομένως δεν μας ενδιαφέρει να ορίσουμε το $X(\tau)$ για $p(\tau) = 0$, καθώς τέτοιες αναθέσεις δεν επιλέγονται ποτέ.

Η μέθοδος αυτή προσφέρει καλύτερη ακρίβεια από την «αφελή» μέθοδο προσέγγισης που παρουσιάσαμε προηγουμένως, διότι η μέση τιμή υπολογίζεται **λαμβάνοντας υπόψη μόνο τις αναθέσεις αληθοτιμών που ικανοποιούν την πρόταση DNF**. Έτσι, με αυτή τη μέθοδο προσέγγισης δεν εμφανίζεται το πρόβλημα που είδαμε προηγουμένως για μικρό πλήθος αναθέσεων που ικανοποιούν την πρόταση.

Εξηγήσαμε λοιπόν ότι αυτή η μέθοδος δίνει καλύτερη προσέγγιση συγκριτικά με την αρχική, ωστόσο αυτό δεν αρκεί για να αποδείξουμε αυστηρά ότι η μέθοδος αυτή είναι FPRAS. Για αυτό το σκοπό πρέπει να δείξουμε ότι ικανοποιείται η ανισότητα που δείξαμε στον ορισμό του FPRAS στην ενότητα 5.1 (ή μια ισοδύναμη παραλλαγή αυτής της ανισότητας). Για αυτό το σκοπό χρησιμεύει η **ανισότητα του Chebyshev**. Χάριν συντομίας, επιλέγουμε να μην παρουσιάσουμε αναλυτικά την απόδειξη, ωστόσο παραπέμπουμε στις σελ. 296-297 του βιβλίου του Vazirani [Vaz04] για περαιτέρω μελέτη.

# 6. Περιγραφική Πολυπλοκότητα για Προβλήματα Μέτρησης

Στο κεφάλαιο 3 είδαμε κάποια από τα κυριότερα συμπεράσματα που έχουν προκύψει από το πεδίο της περιγραφικής πολυπλοκότητας για προβλήματα απόφασης. Ωστόσο, για προβλήματα μέτρησης το πεδίο αυτό δεν είναι εξίσου μελετημένο και έτσι είναι αναμενόμενο σε μερικά χρόνια να προκύψουν νέα θεωρήματα και εξελίξεις.

Υπενθυμίζουμε ότι, όπως και στο κεφάλαιο 3, θα αναφερόμαστε σε πεπερασμένες και διατεταγμένες δομές. Δηλαδή διαθέτουμε έναν τελεστή '$\leq$' που καθορίζει μια ολική διάταξη στα στοιχεία του σύμπαντος.

## 6.1. Περιγραφή της #P με Λογική

### 6.1.1. Ορισμοί Λογικών Κλάσεων για Μετρητικά Προβλήματα

Όπως είδαμε στο κεφάλαιο 3 με το θεώρημα του Fagin, κάθε πρόβλημα στο $NP$ μπορεί να περιγραφεί με υπαρξιακή λογική δεύτερης τάξης. Εφόσον τα προβλήματα της κλάσης $\#P$ αποτελούν παραλλαγές των προβλημάτων της $NP$, ρωτώντας «πόσες λύσεις υπάρχουν;» αντί για «υπάρχει λύση;», φαίνεται λογικό ότι για την κλάση $\#P$ χρειαζόμαστε κάτι παρόμοιο με υπαρξιακή λογική δεύτερης τάξης, αλλά αντικαθιστώντας τον υπαρξιακό ποσοδείκτη δεύτερης τάξης με ερώτηση για το πόσες αντίστοιχες σχέσεις υπάρχουν. Έτσι, οδηγούμαστε στον παρακάτω ορισμό [SST95].

<u>Ορισμός (Κλάση $\#FO$)</u>

1. Έστω $\sigma$ ένα λεξιλόγιο που περιέχει τον τελεστή δυαδικής σχέσης '$\leq$'.

2. Έστω μια συνάρτηση μέτρησης $f$, η οποία δέχεται ως όρισμα πεπερασμένες και διατεταγμένες δομές $A$ με λεξιλόγιο $\sigma$.

3. Έστω ένα σύνολο $T$ συμβόλων κατηγορημάτων και ένα σύνολο $z$ ελεύθερων μεταβλητών πρώτης τάξης.

Η συνάρτηση $f$ ανήκει στην κλάση $\#FO$ αν υπάρχει φόρμουλα $\varphi$ λογικής πρώτης τάξης με σύμβολα κατηγορημάτων από το $T \cup \sigma$ και ελεύθερες μεταβλητές πρώτης τάξης από το $z$, τέτοια ώστε να ισχύει:

$$f(A) = |\{\langle T, z\rangle : A \vDash \varphi(T, z)\}|$$

Ο ορισμός αυτός, παρόλο που φαίνεται περίπλοκος, στην ουσία αποτελεί μια αρκετά προφανή τροποποίηση της υπαρξιακής λογικής δεύτερης τάξης, δεδομένου ότι τώρα ασχολούμαστε με πλήθος λύσεων.

Σε αυτό το σημείο θα χρειαστούμε να ορίσουμε τα σύνολα $\Sigma_i, \Pi_i$ για λογική πρώτης τάξης.

<u>Ορισμός (Κλάσεις $\Sigma_i, \Pi_i$)</u>

Σε αυτό τον ορισμό όπου εμφανίζεται το σύμβολο $\varphi$ θεωρούμε ότι συμβολίζει φόρμουλα **χωρίς ποσοδείκτες**.

1. Ορίζουμε ως $\Sigma_0 \equiv \Pi_0$ το σύνολο φόρμουλων λογικής πρώτης τάξης που δεν περιέχουν ποσοδείκτες.

2. Ορίζουμε ως $\Sigma_1$ το σύνολο φόρμουλων λογικής πρώτης τάξης που περιέχει οσουσδήποτε υπαρξιακούς ποσοδείκτες, αλλά όχι καθολικούς ποσοδείκτες. Μια τέτοια φόρμουλα γράφεται στην εξής μορφή:

$$\exists x_1 \exists x_2 \dots \exists x_n \varphi(x_1, x_2, \dots, x_n)$$

Για συντομία, θα γράφουμε:

$$\exists \vec{x} \varphi(\vec{x})$$

3. Αντίστοιχα, ορίζουμε ως $\Pi_1$ το σύνολο φόρμουλων της μορφής $\forall \vec{x} \varphi(\vec{x})$.

4. Οι κλάσεις $\Sigma_i, \Pi_i$ για $i > 1$ ορίζονται λαμβάνοντας υπόψη την εναλλαγή των ποσοδεικτών. Για παράδειγμα, οι φόρμουλες της κλάσης $\Sigma_2$ γράφονται ως:

$$\exists \vec{x} \forall \vec{y} \varphi(\vec{x}, \vec{y})$$

Ενώ οι φόρμουλες της κλάσης $\Pi_2$ γράφονται ως:

$$\forall \vec{x} \exists \vec{y} \varphi(\vec{x}, \vec{y})$$

Αυστηρότερα, μπορούμε να δώσουμε **αναδρομικό** ορισμό ως εξής. Η κλάση $\Sigma_{i+1}$ περιέχει φόρμουλες της μορφής $\exists \vec{x} \psi(\vec{x})$, όπου η $\psi$ είναι φόρμουλα της κλάσης $\Pi_i$. Αντίστοιχα, η κλάση $\Pi_{i+1}$ περιέχει φόρμουλες της μορφής $\forall \vec{x} \psi(\vec{x})$, όπου η $\psi$ είναι φόρμουλα της κλάσης $\Sigma_i$.

Θα επεκτείνουμε τον ορισμό των παραπάνω κλάσεων για συναρτήσεις μέτρησης, ώστε να έχουμε κλάσεις προσαρμοσμένες στις ανάγκες μας για περιγραφή μετρητικών προβλημάτων [SST95].

Ορισμός (Κλάσεις $\#\Sigma_i, \#\Pi_i$)

Έστω μια συνάρτηση $f \in \#FO$. Σύμφωνα με τον ορισμό που δώσαμε για την $\#FO$, θα υπάρχει φόρμουλα $\varphi$ λογικής πρώτης τάξης με σύμβολα κατηγορημάτων στο $T \cup \sigma$ και ελεύθερες μεταβλητές πρώτης τάξης στο $z$, τέτοια ώστε να ισχύει:

$$f(A) = |\{\langle T, z \rangle : A \vDash \varphi(T, z)\}|$$

Ορίζουμε ως $\#\Sigma_i$ το σύνολο των συναρτήσεων $f \in \#FO$ για τις οποίες για την αντίστοιχη φόρμουλα $\varphi$ ισχύει $\varphi \in \Sigma_i$.

Οι κλάσεις $\#\Pi_i$ ορίζονται κατ’ αναλογία.

Στην επόμενη ενότητα θα δούμε κάποια ενδιαφέροντα συμπεράσματα σχετικά με την ιεραρχία αυτών των κλάσεων και την εκφραστικότητα που χρειαζόμαστε για ορισμένα προβλήματα της $\#P$.

### 6.1.2. Ιεραρχία Λογικών Υποκλάσεων της #P

Σε αυτό το σημείο θα παρουσιάσουμε συνοπτικά μερικά από τα συμπεράσματα των **Saluja, Subrahmanyam και Thakur** [SST95], τα οποία ήταν από τα πρώτα σημαντικά συμπεράσματα που προέκυψαν σχετικά με περιγραφική πολυπλοκότητα προβλημάτων μέτρησης.

Οι αποδείξεις των αντίστοιχων θεωρημάτων δεν θα παρουσιαστούν όλες αναλυτικά, καθώς μπορεί ο αναγνώστης να τις βρει εύκολα στην αντίστοιχη δημοσίευση. Παρόλα αυτά, θα σχολιάσουμε ορισμένα σημεία που παρουσιάζουν ιδιαίτερο ενδιαφέρον.

<ins>Θεώρημα (SST1)</ins>

Οι κλάσεις $\#P$, $\#FO$ και $\#\Pi_2$ ταυτίζονται.

Εφόσον γνωρίζουμε από το **θεώρημα του Fagin** ότι $NP = SO\exists$ και κατασκευάσαμε για μετρητικά προβλήματα την $\#FO$ κατ' αναλογία με την $SO\exists$, είναι διαισθητικά προφανές ότι θα είναι $\#\boldsymbol{P} = \#\boldsymbol{FO}$, αν λάβουμε υπόψη μας ότι η $\#P$ περιέχει τις μετρητικές εκδοχές των προβλημάτων της $NP$. Για αυτό το λόγο μάλιστα η απόδειξη της παραπάνω πρότασης είναι ουσιαστικά μια παραλλαγή της απόδειξης του Fagin.

Το δεύτερο σκέλος του θεωρήματος, δηλαδή ότι $\#\boldsymbol{P} = \#\boldsymbol{\Pi_2}$, πάλι προκύπτει από την απόδειξη του Fagin. Συγκεκριμένα, από την απόδειξη που έχουμε παρουσιάσει στην ενότητα 3.3 προκύπτει ότι οι προτάσεις $SO\exists$ που χρησιμοποιούνται για τα προβλήματα της κλάσης $NP$ περιέχουν (στο πρωτοβάθμιο σκέλος τους) φόρμουλα που περιλαμβάνει μόνο καθολικούς ποσοδείκτες, δηλαδή φόρμουλα της κλάσης $\Pi_1$.

Όμως, σε εκείνη την απόδειξη υποθέσαμε ότι διαθέτουμε τα σύμβολα $0$ και $max$, χωρίς τα οποία θα χρειαζόμασταν υπαρξιακούς ποσοδείκτες για να εκφράσουμε την απαίτηση ύπαρξης ελάχιστου και μέγιστου στοιχείο στη διατεταγμένη δομή μας. Για αυτό το λόγο, θεωρώντας ότι διαθέτουμε μόνο τον τελεστή ολικής διάταξης '$\leq$', ένα πρόβλημα της $NP$ θα χρειαζόταν πρόταση $SO\exists$ που να περιέχει φόρμουλα της κλάσης $\Pi_2$ στο πρωτοβάθμιο σκέλος της. Κατ' αναλογία, οδηγούμαστε στο συμπέρασμα ότι για την περιγραφή προβλημάτων της $\#P$ μάς αρκεί η εκφραστικότητα της $\#\Pi_2$.

Σύμφωνα με τα παραπάνω, συμπεραίνουμε ότι ισχύει το εξής:

$$\#\Pi_2 = \#\Sigma_i = \#\Pi_i, \forall i > 2$$

Το επόμενο θεώρημα χρησιμεύει στο να καθοριστεί η ιεραρχία των υποκλάσεων της $\#\Pi_2$, το οποίο είναι σημαντικό για την κατάταξη των προβλημάτων της $\#P$ σε επίπεδα δυσκολίας.

Θεώρημα (SST2)

Η κλάση $\#\Sigma_1$ περιέχεται στην $\#\Pi_1$.

Απόδειξη (SST2)

Έστω ότι έχουμε μια συνάρτηση $f \in \#\Sigma_1$:

$$f(A) = |\{\langle T, z\rangle : A \vDash (\exists x)\varphi(x, T, z)\}|$$

Υπενθυμίζουμε ότι η $\varphi$ δεν θα περιέχει ποσοδείκτες. Θεωρούμε την παρακάτω συνάρτηση $g$:

$$g(A) = |\{\langle T, (z, x^*)\rangle : A \vDash \varphi(x^*, T, z) \wedge (\forall x)(\varphi(x, T, z) \rightarrow x^* \leq x)\}|$$

Σημειώνουμε ότι ο ποσοδείκτης $\forall$ μπορεί να μετακινηθεί στην αρχή της πρότασης και επομένως είναι $g \in \#\Pi_1$. Εύκολα μπορούμε να δούμε ότι είναι $f(A) = g(A)$. Ουσιαστικά η $g$ μετράει τα ζεύγη $\langle T, (z, x^*)\rangle$ για τα οποία ισχύει η $\varphi(x^*, T, z)$ και το $x^*$ είναι το ελάχιστο τέτοιο στοιχείο. Αυτό είναι ισοδύναμο με το να μετρήσουμε τα ζεύγη $\langle T, z\rangle$ για τα οποία υπάρχει $x$ τέτοιο ώστε $\varphi(x, T, z)$.

Επομένως είναι $f \in \#\Pi_1$, άρα $\#\Sigma_1 \subseteq \#\Pi_1$. ■

Με βάση το παραπάνω θεώρημα, καταλήγουμε στην εξής ιεραρχία κλάσεων:

$$\#\Sigma_0 = \#\Pi_0 \subseteq \#\Sigma_1 \subseteq \#\Pi_1 \subseteq \#\Sigma_2 \subseteq \#\Pi_2 = \#P$$

Μένει να ελέγξουμε τι ισχύει για τις ενδιάμεσες κλάσεις, δηλαδή αν είναι ίσες μεταξύ τους ή αν οι υπαγωγές είναι γνήσιες. Το επόμενο θεώρημα απαντά σε αυτή την ερώτηση.

Θεώρημα (SST3)

Για τα ακόλουθα μετρητικά προβλήματα ισχύουν τα εξής:

1. $\#3DNF \in \#\Sigma_1 \backslash \#\Sigma_0$

2. $\#3CNF \in \#\Pi_1 \backslash \#\Sigma_1$

3. $\#DNF \in \#\Sigma_2 \backslash \#\Pi_1$

4. $\#HamiltonCycle \in \#\Pi_2 \backslash \#\Sigma_2$

Θα παραλείψουμε τις αποδείξεις χάριν συντομίας. Οι αποδείξεις μη υπαγωγής προβλημάτων σε κλάσεις γίνονται με απαγωγή σε άτοπο, υποθέτοντας ότι το πρόβλημα ανήκει στην αντίστοιχη κλάση και επομένως διαθέτει λογική περιγραφή της αντίστοιχης μορφής.

Θα δείξουμε για παράδειγμα τη **λογική περιγραφή του προβλήματος** $\#\boldsymbol{DNF}$ **σε μορφή** $\#\boldsymbol{\Sigma_2}$. Θεωρούμε ότι το σύμπαν $A$ περιέχει τις boolean μεταβλητές της πρότασης και τις συζεύξεις της (δηλαδή τις υπο-προτάσεις μεταξύ των οποίων εφαρμόζεται διάζευξη). Επίσης θεωρούμε ότι διαθέτουμε τα παρακάτω κατηγορήματα:

- $P(d, v)$: Η μεταβλητή $v$ εμφανίζεται χωρίς άρνηση στη σύζευξη $d$.
- $N(d, v)$: Η μεταβλητή $v$ εμφανίζεται με άρνηση στη σύζευξη $d$.
- $D(d)$: Το στοιχείο $d$ είναι σύζευξη (και όχι λογική μεταβλητή).

Επιπλέον, θεωρούμε ότι η σχέση $T$ συμβολίζει το σύνολο των boolean μεταβλητών της πρότασης στις οποίες έχει ανατεθεί τιμή “True”.

Με βάση αυτά, μπορούμε να ορίσουμε την εξής συνάρτηση για το πρόβλημα $\#DNF$:

$$f_{\#DNF}(A) = \left|\left\{\langle T\rangle : A \vDash (\exists d)(\forall v)\Big(D(d) \wedge \big(P(d,v) \rightarrow T(v)\big) \wedge \big(N(d,v) \rightarrow \neg T(v)\big)\Big)\right\}\right|$$

Η παραπάνω πρόταση σημαίνει «υπάρχει σύζευξη στην οποία όλες οι μεταβλητές που εμφανίζονται χωρίς άρνηση είναι “True”, ενώ όλες που εμφανίζονται με άρνηση είναι “False”». Εύκολα διαπιστώνουμε ότι αυτή είναι ικανή και αναγκαία συνθήκη ώστε να ικανοποιείται μία πρόταση $DNF$ από μια ανάθεση αληθοτιμών $T$.

Σημειώνουμε ότι για το πρόβλημα απόφασης $DNF$ θα χρησιμοποιούσαμε την ίδια περιγραφή σε λογική $SO\exists$, βάζοντας μπροστά έναν ποσοδείκτη δεύτερης τάξης για τη σχέση $T$. Εν γένει, οι λογικές περιγραφές τέτοιων μετρητικών προβλημάτων προκύπτουν άμεσα από τις λογικές περιγραφές των αντίστοιχων προβλημάτων απόφασης.

Με αντίστοιχες σκέψεις προκύπτουν οι λογικές περιγραφές των $\#3DNF$ και $\#3CNF$. Η διαφορά είναι ότι αν έχουμε τρεις λογικές μεταβλητές (ή, γενικότερα, πεπερασμένο πλήθος), τότε είναι συγκεκριμένες οι συζεύξεις/διαζεύξεις που μπορούν να εμφανιστούν στην πρόταση και επομένως μπορούμε να δημιουργήσουμε ένα κατηγόρημα για την καθεμία, το οποίο θα υποδεικνύει εάν η αντίστοιχη σύζευξη/διάζευξη εμφανίζεται στην πρόταση. Με αυτό τον τρόπο γλιτώνουμε τη χρήση ποσοδείκτη για τις συζεύξεις/διαζεύξεις. Τελικά προκύπτει ότι για το $\#3DNF$ μάς αρκούν τρεις υπαρξιακοί ποσοδείκτες, ενώ για το $\#3CNF$ τρεις καθολικοί, άρα είναι $\#\boldsymbol{3DNF} \in \#\boldsymbol{\Sigma_1}$ και $\#\boldsymbol{3CNF} \in \#\boldsymbol{\Pi_1}$.

Για το πρόβλημα $\#HamiltonCycle$ δεν είναι εξίσου εύκολο να βρεθεί λογική περιγραφή, ωστόσο δεν είναι αναγκαίο για την απόδειξη $\#HamiltonCycle \in \#\Pi_2$, αφού έχουμε ότι $\#\Pi_2 = \#FO$.

Το ακόλουθο πόρισμα προκύπτει άμεσα από τα θεωρήματα που έχουμε παρουσιάσει μέχρι στιγμής σε αυτή την ενότητα.

Πόρισμα (SST4)

Ισχύει η εξής ιεραρχία κλάσεων:

$$\#\Sigma_0 = \#\Pi_0 \subset \#\Sigma_1 \subset \#\Pi_1 \subset \#\Sigma_2 \subset \#\Pi_2 = \#P$$

Όλες οι παραπάνω υπαγωγές είναι γνήσιες.

Παρουσιάζει ενδιαφέρον ότι η γνησιότητα αυτών των υπαγωγών είναι εγγυημένη και δεν εξαρτάται από υποθέσεις θεωρίας πολυπλοκότητας, όπως θα συνέβαινε συνήθως για ιεραρχίες κλάσεων.

### 6.1.3. Υπολογιστική Δυσκολία Λογικών Υποκλάσεων της #P

Έχοντας βρει την ιεραρχία λογικών κλάσεων που παρουσιάσαμε στην προηγούμενη ενότητα, προκύπτει φυσικά το ερώτημα για το τι ισχύει για την υπολογιστική δυσκολία καθεμίας από αυτές τις κλάσεις. Σημειώνουμε ότι έχουμε δει στην ενότητα 5.2.2 ότι υπάρχει FPRAS για το πρόβλημα $\#DNF$, το οποίο όπως είδαμε ανήκει στην κλάση $\#\Sigma_2$.

Από τη μέχρι τώρα μελέτη μας στο πεδίο της περιγραφικής πολυπλοκότητας έχουμε δει ότι, εν γένει, όταν ένα πρόβλημα χρειάζεται περίπλοκη λογική για να περιγραφεί, τότε είναι και υπολογιστικά δύσκολο. Επομένως, αναμένουμε ότι η ιεραρχία κλάσεων που είδαμε στην προηγούμενη ενότητα θα διαχωρίζει τα προβλήματα της $\#P$ σε επίπεδα δυσκολίας.

Πράγματι, το θεώρημα που θα παρουσιάσουμε παρακάτω [SST95] δείχνει ακριβώς αυτό.

<u>Θεώρημα (SST5)</u>

(1) Κάθε πρόβλημα μέτρησης της κλάσης $\#\Sigma_0$ λύνεται ντετερμινιστικά σε πολυωνυμικό χρόνο.

(2) Κάθε πρόβλημα μέτρησης της κλάσης $\#\Sigma_1$ έχει FPRAS.

Παρατηρούμε ότι είναι αναμενόμενο για προβλήματα της κλάσης $\#\Sigma_1$ να μη λύνονται ντετερμινιστικά σε πολυωνυμικό χρόνο, καθώς αυτή περιέχει το $\#3DNF$, το οποίο είναι $\#P$-complete.

Θα παραλείψουμε τις αποδείξεις των ανωτέρω χάριν συντομίας, ωστόσο θα αναφέρουμε ότι η απόδειξη του (2) γίνεται δείχνοντας ότι κάθε πρόβλημα της $\#\Sigma_1$ ανάγεται σε μια ειδική περίπτωση του προβλήματος $\#DNF$, με αναγωγή η οποία διατηρεί την ύπαρξη προσέγγισης.

Στη συνέχεια θα ορίσουμε μία υποκλάση της $\#\Sigma_2$, προκειμένου να δούμε τι ισχύει για τις δυσκολότερες κλάσεις.

<u>Ορισμός (Κλάση $\#R\Sigma_2$)</u>

1. Έστω $\sigma$ ένα λεξιλόγιο που περιέχει τον τελεστή δυαδικής σχέσης '$\leq$'.

2. Έστω μια συνάρτηση μέτρησης $f$, η οποία δέχεται ως όρισμα πεπερασμένες και διατεταγμένες δομές $A$ με λεξιλόγιο $\sigma$.

3. Έστω ένα σύνολο $T$ συμβόλων κατηγορημάτων και ένα σύνολο $z$ ελεύθερων μεταβλητών πρώτης τάξης.

Η συνάρτηση $f$ ανήκει στην κλάση $\#R\Sigma_2$ αν υπάρχει φόρμουλα $\varphi$ χωρίς ποσοδείκτες με σύμβολα κατηγορημάτων από το $T \cup \sigma$ και ελεύθερες μεταβλητές πρώτης τάξης από το $z$, τέτοια ώστε να ισχύει:

$$f(A) = |\{\langle T, z\rangle : A \vDash (\exists x)(\forall y)\varphi(x, y, T, z)\}|$$

Επιπλέον, πρέπει η $\varphi$ να έχει ισοδύναμη πρόταση σε μορφή CNF, τέτοια ώστε κάθε διάζευξη να περιέχει το πολύ μία εμφάνιση ενός συμβόλου κατηγορήματος του $T$.

Ουσιαστικά περιορίσαμε τη μορφή που έχει η αντίστοιχη πρόταση πρώτης τάξης μετά τους ποσοδείκτες. Το επόμενο θεώρημα μας εξασφαλίζει την υπολογιστική δυσκολία των αντίστοιχων προβλημάτων.

<u>Θεώρημα (SST6)</u>

Κάθε πρόβλημα μέτρησης της κλάσης $\#R\Sigma_2$ έχει FPRAS.

Κλείνοντας αυτή την ενότητα, παρουσιάζουμε ένα ακόμα ενδιαφέρον συμπέρασμα που προέκυψε από τη δουλειά των Saluja, Subrahmanyam και Thakur [SST95].

<u>Θεώρημα (SST7)</u>

Τα αντίστοιχα προβλήματα απόφασης των συναρτήσεων των κλάσεων $\#\Sigma_0$, $\#\Sigma_1$ και $\#R\Sigma_2$ ανήκουν στην κλάση $P$.

Το θεώρημα αυτό προκύπτει αποδεικνύοντας ότι κάθε πρόβλημα των παραπάνω κλάσεων ανάγεται στο $\#DNF$, το οποίο είναι πλήρες για την $\#R\Sigma_2$ (με συγκεκριμένο είδος αναγωγών, το οποίο ορίζεται στην αντίστοιχη δημοσίευση).

# 7. Λογικές Περιγραφές για άλλες Κλάσεις Πολυπλοκότητας

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να ορίσουμε λογικά συστήματα που να περιγράφουν επακριβώς ορισμένες κλάσεις πολυπλοκότητας οι οποίες είναι λιγότερο μελετημένες.

Όπως είδαμε στο προηγούμενο κεφάλαιο, η λογική περιγραφή της κλάσης $\#P$ [SST95] προκύπτει κατ' αναλογία με τη λογική περιγραφή της $NP$ με το θεώρημα του Fagin. Θα προσπαθήσουμε να κάνουμε το ίδιο και για άλλες σχετικές κλάσεις, τροποποιώντας την $SO\exists$ ώστε να ταιριάζει στις ανάγκες μας.

Σημειώνουμε ότι μερικοί από τους ορισμούς που θα δοθούν σε αυτό το κεφάλαιο θα είναι αυθαίρετοι. Αυτό σημαίνει ότι η ονομασία που θα δοθεί σε κάποιους όρους πιθανόν να μην υφίσταται έξω από αυτή την εργασία και, επομένως, δεν θα έχει νόημα να αναζητήσει ο αναγνώστης βιβλιογραφία για τον αντίστοιχο όρο. Επιπλέον, κάποιες έννοιες ενδέχεται να έχουν οριστεί ήδη αλλού με ίδιες ή διαφορετικές ονομασίες, σε βιβλιογραφία την οποία δεν είχαμε υπόψη μας κατά τη συγγραφή αυτής της εργασίας.

Τονίζουμε επίσης ότι και σε αυτό το κεφάλαιο θα αναφερόμαστε σε *πεπερασμένες* και *διατεταγμένες* δομές, δηλαδή πεπερασμένες δομές στις οποίες διαθέτουμε έναν τελεστή '$\leq$' που λειτουργεί ως δυαδική σχέση που καθορίζει μια ολική διάταξη στα στοιχεία του σύμπαντος.

## 7.1. Κλάση ⊕P

### 7.1.1. Ορισμοί

Όπως είχαμε αναφέρει στην ενότητα 4.3 με το θεώρημα του Toda, ένα πρόβλημα της κλάσης $\oplus P$ ("Parity P") ουσιαστικά ισοδυναμεί με τον υπολογισμό του ελάχιστα σημαντικού δυαδικού ψηφίου μιας συνάρτησης $f \in \#P$. Παρακάτω παρουσιάζουμε έναν αυστηρότερο ορισμό [AB09]:

Ορισμός (Κλάση $\oplus P$)

Μία γλώσσα $L$ ανήκει στην κλάση $\oplus P$ αν και μόνο αν υπάρχει μη ντετερμινιστική μηχανή Turing $M$ πολυωνυμικού χρόνου, τέτοια ώστε να ισχύει $x \in L$ αν και μόνο αν το πλήθος των μονοπατιών της $M$ που καταλήγουν σε αποδοχή με είσοδο $x$ είναι περιττό.

Σύμφωνα με τα παραπάνω είναι φανερό ότι θα μπορούσαμε να δούμε την $\oplus P$ σαν μια ευκολότερη ειδική περίπτωση της $\#P$. Στο κεφάλαιο 6 είδαμε ότι η λογική περιγραφή της κλάσης $\#P$ προκύπτει κατ' αναλογία με αυτή της $NP$, αντικαθιστώντας τον υπαρξιακό ποσοδείκτη δεύτερης τάξης με μέτρηση του πλήθους των αντίστοιχων κατηγορημάτων. Παρακάτω θα προσπαθήσουμε να κάνουμε κάτι αντίστοιχο για την $\oplus P$. Για αυτό το σκοπό θα θέλαμε να ορίσουμε κάποιον ποσοδείκτη παρόμοιο με τον κλασικό υπαρξιακό ποσοδείκτη, ο οποίος όμως θα δίνει κάποια εγγύηση για το πλήθος των στοιχείων που τηρούν την αντίστοιχη προϋπόθεση.

## 7.1.2. Λογική Περιγραφή

Σκοπός μας είναι να κατασκευάσουμε ένα λογικό σύστημα που να διαθέτει δυνατότητες μέτρησης. Θα στηριχτούμε στους μετρητικούς ποσοδείκτες που προτείνει ο Leonid Libkin [Lib04].

Αρχικά, ας θεωρήσουμε ότι οι δομές με τις οποίες ασχολούμαστε διαθέτουν δύο σύμπαντα. Δηλαδή, εκτός από το κλασικό σύμπαν $|A|$ που περιέχει στοιχεία (π.χ. κόμβους γραφημάτων), θεωρούμε ότι διαθέτουμε και ένα **σύμπαν που περιέχει αριθμούς, το οποίο θα συμβολίζουμε με** $\boldsymbol{B}$. Με βάση αυτούς τους αριθμούς θα ορίσουμε ποσοδείκτες που να εκφράζουν ιδιότητες για το πλήθος των αντίστοιχων στοιχείων.

Γενικά θα χρησιμοποιούμε τα γράμματα $i, j, k$ για στοιχεία του συνόλου $B$, ενώ για το σύμπαν $|A|$ θα προτιμούμε τα γράμματα $x, y, z$, όπως κάναμε μέχρι τώρα.

Πριν προχωρήσουμε σε αυστηρότερους ορισμούς, ας σκεφτούμε τι εκφραστικότητα μπορεί να προσφέρει η προσθήκη αριθμών στη λογική πρώτης τάξης. Ας θεωρήσουμε ότι τα παρακάτω σύμβολα διαθέτουν την εξής σημασία:

- $\exists i\ \varphi(\vec{x}, \vec{\imath})$: «Υπάρχει αριθμός $i \in B$ τέτοιος ώστε να ισχύει $\varphi(\vec{x}, \vec{\imath})$.»
- $\exists iy\ \varphi(y, \vec{x}, \vec{\imath})$: «Υπάρχουν <u>τουλάχιστον</u> $i$ διαφορετικά στοιχεία $y \in |A|$ τέτοια ώστε να ισχύει $\varphi(y, \vec{x}, \vec{\imath})$.»

Σημειώνουμε ότι στη δεύτερη περίπτωση δεσμεύεται από τον ποσοδείκτη μόνο η μεταβλητή $y$ και όχι ο αριθμός $i$.

Τα παραπάνω προφανώς δεν είναι αυστηροί ορισμοί και αναφέρονται απλά για να φανερώσουμε τη χρησιμότητα μιας τέτοιας λογικής. Για τους αυστηρότερους ορισμούς παραπέμπουμε στο βιβλίο του Libkin [Lib04].

Με βάση τους παραπάνω ποσοδείκτες (και έναν τελεστή πρόσθεσης, του οποίου ο ορισμός είναι προφανής), θα μπορούσαμε να εκφράσουμε την έννοια της ύπαρξης άρτιου πλήθους στοιχείων του $|A|$, τέτοια ώστε να ισχύει μια ιδιότητα $\varphi$:

$$\exists i \exists j \Big( (i = j + j) \wedge \exists ix\ \varphi(x) \wedge \big(\forall k (k > i) \rightarrow \neg \exists kx\ \varphi(x)\big)\Big)$$

Παρουσιάζει ενδιαφέρον ότι, αν θέλαμε να έχουμε ποσοδείκτη που να εκφράζει την ύπαρξη <u>ακριβώς</u> $i$ διαφορετικών στοιχείων, τότε αυτός θα μπορούσε να οριστεί με βάση τους ποσοδείκτες που παρουσιάσαμε ήδη:

$$\exists!\, ix\ \varphi(x) \equiv \exists ix\ \varphi(x) \wedge \forall k\big((k > i) \rightarrow \neg \exists kx\ \varphi(x)\big)$$

Ας επιστρέψουμε τώρα στην κλάση $\oplus P$. Κατ' αναλογία με το θεώρημα του Fagin, αυτό που θέλουμε να εκφράσουμε για την $\oplus P$ είναι η ύπαρξη περιττού πλήθους *σχέσεων*. Για την ακρίβεια, θα θέλαμε να έχουμε έναν υπαρξιακό ποσοδείκτη δεύτερης τάξης, ο οποίος **να μπορεί να εκφράσει <u>μόνο</u> την ύπαρξη περιττού πλήθους σχέσεων**, καθώς η ύπαρξη άρτιου πλήθους σχέσεων θέλουμε να μην μπορεί να εκφραστεί από την αντίστοιχη λογική (αλλιώς θα έχουμε μια λογική που είναι υπερσύνολο της $\oplus P$, αντί να την εκφράζει επακριβώς).

Συμπεραίνουμε ότι οι ποσοδείκτες που δείξαμε παραπάνω μάλλον δεν ταιριάζουν ακριβώς σε αυτό που θέλουμε να κάνουμε. Επιλέξαμε να τους παρουσιάσουμε συνοπτικά επειδή προσφέρουν αρκετή εκφραστικότητα σε λογικές που χρειάζονται δυνατότητα μέτρησης, καθώς και επειδή μπορεί να φανούν χρήσιμοι για τη λογική περιγραφή άλλων κλάσεων πολυπλοκότητας.

Για τους σκοπούς αυτής της υποενότητας θα προτιμήσουμε να ορίσουμε έναν λιγότερο εκφραστικό ποσοδείκτη, κατ' αναλογία με ένα δεύτερο είδος ποσοδεικτών που προτείνει ο Libkin.

<u>Ορισμός (Ποσοδείκτης $\exists_{ODD}$)</u>

Έστω μία φόρμουλα πρώτης τάξης $\varphi(x,\vec{y})$, με ελεύθερες μεταβλητές $x,\vec{y}$. Ορίζουμε έναν ποσοδείκτη $\exists_{ODD}$ με τον οποίο μπορεί να κατασκευαστεί μία νέα φόρμουλα $\exists_{ODD}x\varphi(x,\vec{y})$, με ελεύθερες μεταβλητές $\vec{y}$. Ο ποσοδείκτης θα έχει την παρακάτω σημασιολογία, όπου $\vec{a}$ η ερμηνεία των $\vec{y}$:

$$A \vDash \exists_{ODD}x\varphi(x,\vec{a}) \quad \leftrightarrow \quad |\{b \in |A|: A \vDash \varphi(b,\vec{a})\}| \ mod\ 2 = 1$$

Ο παραπάνω ποσοδείκτης ορίστηκε για μεταβλητές πρώτης τάξης, ωστόσο με παρόμοιο τρόπο θα μπορούσε να οριστεί και για μεταβλητές δεύτερης τάξης, για τις οποίες θα τον χρησιμοποιήσουμε στη συνέχεια.

Εφόσον σκοπεύουμε να περιγράψουμε την κλάση $\oplus P$, οφείλουμε να προσέξουμε μία λεπτομέρεια. Στην περιγραφή της $NP$ κατά Fagin χρησιμοποιείται ο υπαρξιακός ποσοδείκτης δεύτερης τάξης για σχέσεις, εκφράζοντας την ύπαρξη μονοπατιού που καταλήγει σε αποδοχή στη μηχανή Turing. Στην περίπτωση της $\oplus P$ πρέπει να προσέξουμε ότι **θέλουμε να εκφράσουμε την ύπαρξη περιττού πλήθους από *ν-άδες* σχέσεων**, και όχι την ύπαρξη περιττού πλήθους σχέσεων για κάθε δεσμευμένη σχέση ξεχωριστά.

Ενδεχομένως αυτή η διαφορά να ακούγεται ασήμαντη, καθώς για τον κλασικό υπαρξιακό ποσοδείκτη είναι αρκετά προφανές ότι οι δύο παρακάτω εκφράσεις είναι ισοδύναμες:

$$\exists(x,y,z)\varphi(x,y,z) \equiv \exists x\exists y\exists z\varphi(x,y,z)$$

Ωστόσο, αξίζει να αναρωτηθούμε εάν ισχύει το ίδιο για τις δύο παρακάτω εκφράσεις:

- $\exists_{ODD}x\exists_{ODD}y\varphi(x,y)$
- $\exists_{ODD}(x,y)\varphi(x,y)$

Εκ πρώτης όψεως η απάντηση δεν είναι προφανής. Ας χωρίσουμε τα στοιχεία $x$ σε δύο κατηγορίες: εκείνα για τα οποία το πλήθος αντίστοιχων $y$ είναι περιττό και εκείνα για τα οποία είναι άρτιο. Έστω ότι στο πρώτο σύνολο ανήκουν $\alpha$ στοιχεία, ενώ στο δεύτερο ανήκουν $\beta$. Τότε, το πλήθος δυάδων $x,y$ είναι:

$$\delta = (2\kappa+1)\alpha + 2\lambda\beta$$

Εύκολα παρατηρούμε ότι το $\delta$ είναι περιττό αν και μόνο αν το $\alpha$ είναι περιττό, το οποίο ουσιαστικά σημαίνει ότι **οι δύο παραπάνω εκφράσεις τελικά είναι ισοδύναμες**. Επαγωγικά μπορεί αυτό το αποτέλεσμα να γενικευθεί για $\nu$-άδες στοιχείων.

Τονίζουμε ότι όταν ορίζουμε έναν τέτοιο ποσοδείκτη είναι σημαντικό να ελέγξουμε εάν ισχύει αυτή η ιδιότητα. **Για τον αντίστοιχο ποσοδείκτη $\exists_{EVEN}$ αυτές οι εκφράσεις <u>δεν</u> θα ήταν ισοδύναμες**, καθώς <u>δεν ισχύει</u> ότι το $\delta$ είναι άρτιο αν και μόνο αν το $\beta$ είναι άρτιο.

Με βάση τα παραπάνω, καταλήγουμε ότι δεν είναι αναγκαίο να προσέξουμε τον ορισμό του $\exists_{ODD}$ για $\nu$-άδες στοιχείων.

Ακολουθεί το βασικό θεώρημα αυτής της υποενότητας:

<u>Θεώρημα ($\oplus P = SO\exists_{ODD}$)</u>

Η κλάση πολυπλοκότητας $\oplus P$ περιέχει ακριβώς τα προβλήματα που μπορούν να περιγραφούν σε λογική δεύτερης τάξης εφοδιασμένη με τον ποσοδείκτη $\exists_{ODD}$ για σχέσεις.

<u>Απόδειξη ($\oplus P = SO\exists_{ODD}$)</u>

<u>1. $\oplus P \subseteq SO\exists_{ODD}$:</u>

Κατ' αντιστοιχία με το δεύτερο σκέλος της απόδειξης του θεωρήματος του Fagin (την οποία παρουσιάσαμε στην ενότητα 3.3), σκοπός μας είναι να βρούμε πρόταση $SO\exists_{ODD}$ $\Phi$, τέτοια ώστε για μια μη ντετερμινιστική πολυωνυμική μηχανή Turing $N$ να ισχύει $A \vDash \Phi$ αν και μόνο αν η $N$ έχει περιττό πλήθος μονοπατιών που αποδέχονται τη δυαδική αναπαράσταση της δομής $A$. Ας πάρουμε την πρόταση που είχαμε δει στην απόδειξη του Fagin, αντικαθιστώντας τον υπαρξιακό ποσοδείκτη με το νέο ποσοδείκτη μας:

$$\Phi \equiv \left(\exists_{ODD} C_1^{2k} \dots C_g^{2k} \Delta^k\right)\varphi$$

Με βάση την ανάλυση που είχαμε κάνει για τη σημασία αυτής της πρότασης στην απόδειξη του Fagin, είναι εύκολο να δούμε ότι χρησιμοποιώντας τον ποσοδείκτη $\exists_{ODD}$, είναι $A \vDash \Phi$ αν και μόνο αν το πλήθος των μονοπατιών της $N$ που καταλήγουν σε αποδοχή είναι περιττό. Επομένως, δεν χρειάζεται να κάνουμε κάποια αλλαγή στην πρόταση που έχουμε ήδη διατυπώσει.

Σημειώνουμε ότι δεν έχει σημασία εάν ο ποσοδείκτης $\exists_{ODD}$ εφαρμόζεται σε κάθε κατηγόρημα ξεχωριστά ή στο tuple όλων των κατηγορημάτων, καθώς (όπως δείξαμε προηγουμένως) οι δύο αυτές εναλλακτικές εκφράσεις είναι ισοδύναμες.

2. $SO\exists_{ODD} \subseteq \oplus P$:

Σκοπός μας είναι να κατασκευάσουμε μια μη ντετερμινιστική πολυωνυμική μηχανή Turing $N$ τέτοια ώστε για κάθε δομή $A$ να είναι $A \vDash \Phi$ ($\Phi$: πρόταση $SO\exists_{ODD}$) αν και μόνο αν η $N$ αποδέχεται τη δυαδική αναπαράσταση της $A$ με περιττό πλήθος μονοπατιών. Έστω:

$$\Phi \equiv \exists_{ODD} R_1^{r_1} \dots R_k^{r_k} \psi$$

Διευκρινίζουμε ότι η $\psi$ είναι φόρμουλα πρώτης τάξης. Κατ' αναλογία με το πρώτο σκέλος της απόδειξης του Fagin, η μηχανή μας θα εξετάσει μη ντετερμινιστικά όλους τους διαφορετικούς συνδυασμούς τιμών των σχέσεων $R_i$, ελέγχοντας εάν ισχύει:

$$(A, R_1, \dots, R_k) \vDash \psi$$

Στην απόδειξη του Fagin είπαμε ότι η μηχανή θα αποδεχτεί αν και μόνο αν αυτό ισχύει και, επειδή μιλάμε για μη ντετερμινιστικό έλεγχο, αυτό ουσιαστικά είναι ισοδύναμο με το να *υπάρχουν* σχέσεις $R_i$ τέτοιες ώστε να ισχύει το παραπάνω. Κατ' αναλογία, στην περίπτωσή μας το πλήθος των διαφορετικών μονοπατιών με τα οποία θα αποδεχτεί η μηχανή είναι <u>ίσο</u> με το πλήθος των $k$-άδων σχέσεων $R_i$ που υπάρχουν ώστε να ισχύει η $\psi$. Επομένως, το πλήθος αυτών των μονοπατιών είναι περιττό αν και μόνο αν το πλήθος των $k$-άδων σχέσεων $R_i$ που υπάρχουν ώστε να ισχύει η $\psi$ είναι περιττό, δηλαδή αν και μόνο αν $A \vDash \exists_{ODD} R_1^{r_1} \dots R_k^{r_k} \psi$.

Σχετικά με το χρόνο που χρειάζεται η μηχανή σημειώνουμε ότι επειδή είναι $FO \subseteq L \subseteq P$, ο έλεγχος $(A, R_1, \dots, R_k) \vDash \psi$ γίνεται σε πολυωνυμικό χρόνο (αφού η $\psi$ είναι φόρμουλα πρώτης τάξης). ■

Σημειώνουμε ότι κατ' αναλογία με ό,τι κάναμε για την $\oplus P$ θα μπορούσαμε να βρούμε λογικές περιγραφές και για τις κλάσεις $Mod_k P$, ωστόσο επιλέξαμε να το παραλείψουμε επειδή οι αντίστοιχες αποδείξεις θα ήταν ουσιαστικά ίδιες.

## 7.2. Κλάση PP

### 7.2.1. Ορισμοί

Στην ενότητα 4.3 με το θεώρημα του Toda κάναμε μια σύντομη αναφορά στην κλάση $PP$. Σε αυτή την υποενότητα θα δούμε αυστηρότερους ορισμούς για αυτή την κλάση.

Αρχικά θα πρέπει να ορίσουμε την έννοια της *πιθανοτικής* μηχανής Turing (probabilistic Turing machine), την οποία **θα γράφουμε ως "PTM" για συντομία**. Η διαφορά μιας PTM από μια μη ντετερμινιστική TM έγκειται κυρίως στο πώς ερμηνεύουμε τον γράφο των δυνατών υπολογισμών της μηχανής [AB09]: σε μια μη ντετερμινιστική TM μάς ενδιαφέρει εάν *υπάρχει* μια ακολουθία επιλογών που οδηγεί τη μηχανή σε αποδοχή, ενώ σε μια PTM μάς ενδιαφέρει το *ποσοστό* αυτών των ακολουθιών. Αυτή την ιδέα θα εκφράσουμε με τον παρακάτω ορισμό [Jan98].

Παρακάτω θα συμβολίζουμε ως $Q$ το σύμβολο καταστάσεων της μηχανής και ως $\Sigma$ το αλφάβητο εισόδου. Σημειώνουμε ότι στη βιβλιογραφία οι PTMs μπορεί μερικές φορές να αναφέρονται και ως "randomized" Turing machines (π.χ. [Jan98]).

Ορισμός (Πιθανοτική Μηχανή Turing – PTM)

Μια πιθανοτική μηχανή Turing ορίζεται ως μία μη ντετερμινιστική μηχανή Turing, η οποία σε κάθε βήμα έχει να επιλέξει το πολύ ανάμεσα σε δύο διαφορετικές μεταβάσεις. Αυτό σημαίνει ότι $\forall q \in Q, a \in \Sigma$ υπάρχουν το πολύ δύο τριάδες $(q', a', m)$, όπου $m$ είναι μία κίνηση της κεφαλής της μηχανής, είτε προς τα αριστερά είτε προς τα δεξιά. Εάν υπάρχουν δύο τέτοιες διαφορετικές μεταβάσεις σε κάποιο βήμα, τότε επιλέγεται μία από τις δύο με πιθανότητα $1/2$.

Σημειώνουμε ότι με βάση τον παραπάνω ορισμό προκύπτει ότι μία PTM δεν παράγει το ίδιο αποτέλεσμα κάθε φορά που τρέχει με συγκεκριμένη είσοδο, δηλαδή μπορεί σε ένα τρέξιμο να απορρίψει μία είσοδο την οποία προηγουμένως αποδέχτηκε.

Με βάση τον ορισμό των PTMs, θα ορίσουμε την κλάση $PP$:

Ορισμός (Κλάση $PP$)

Μία γλώσσα $L$ ανήκει στην κλάση $PP$ αν και μόνο αν υπάρχει PTM $M$ πολυωνυμικού χρόνου, τέτοια ώστε για κάθε $x \in L$ η $M$ να αποδέχεται με πιθανότητα αυστηρά μεγαλύτερη του $1/2$ και για κάθε $x \notin L$ η $M$ να αποδέχεται με πιθανότητα μικρότερη ή ίση του $1/2$.

Όπως είχαμε αναφέρει και στην ενότητα 4.3 με το θεώρημα του Toda, ένα πρόβλημα της κλάσης $PP$ ουσιαστικά ισοδυναμεί με τον υπολογισμό του πλέον σημαντικού δυαδικού ψηφίου μιας συνάρτησης $f \in \#P$ [AB09]. Αυτό συμβαίνει διότι το πλέον σημαντικό ψηφίο του πλήθους λύσεων ενός προβλήματος είναι 1 αν και μόνο αν περισσότερα από τα μισά μονοπάτια της μη ντετερμινιστικής μηχανής καταλήγουν σε αποδοχή, δηλαδή αν και μόνο αν η αποδοχή από αντίστοιχη PTM γίνεται με πιθανότητα μεγαλύτερη του $1/2$.

Επιπλέον, παρατηρούμε ότι το «σφάλμα» στην απάντηση ενός προβλήματος της $PP$ μπορεί να μειωθεί, αν τρέξουμε τον ίδιο πιθανοτικό αλγόριθμο πολλές φορές. Για αυτό το λόγο πρακτικά θα λέγαμε ότι στην $PP$ ανήκουν τα προβλήματα που μπορούν να επιλυθούν με οποιοδήποτε (σταθερό) ποσοστό σφάλματος, επαναλαμβάνοντας έναν πολυωνυμικό αλγόριθμο με τυχαιότητα πεπερασμένο πλήθος φορών.

## 7.2.2. Λογική Περιγραφή

Στην προηγούμενη υποενότητα παρατηρήσαμε ότι το αν η είσοδος σε ένα πρόβλημα της κλάσης $PP$ θα γίνει αποδεκτή καθορίζεται από το αν η *πλειοψηφία* των δυνατών μονοπατιών της αντίστοιχης PTM καταλήγει σε αποδοχή. Είναι φυσικό ότι για τη λογική περιγραφή της $PP$ θα χρειαστούμε κάποιον ποσοδείκτη που να εκφράζει την έννοια της πλειοψηφίας.

Στην ενότητα 7.1 ασχοληθήκαμε με την κλάση $\oplus P$ και δώσαμε λογική περιγραφή για αυτή. Είδαμε ότι για την απόδειξη $\oplus P \subseteq SO\exists_{ODD}$ χρειάστηκε μονάχα να τροποποιήσουμε την πρόταση που χρησιμοποιήθηκε για την απόδειξη του θεωρήματος του Fagin:

$$\Phi \equiv \left(\exists_{ODD} C_1^{2k} \dots C_g^{2k} \Delta^k\right)\varphi$$

Έτσι, η νέα πρόταση αληθεύει εάν υπάρχει περιττό πλήθος μονοπατιών που καταλήγουν σε αποδοχή. Μια πρώτη σκέψη θα ήταν ότι πάλι θέλουμε να τροποποιήσουμε τον ποσοδείκτη αυτής της πρότασης. Ωστόσο, οφείλουμε να προσέξουμε ότι η απαίτηση να έχουμε πλειοψηφία μονοπατιών που καταλήγουν σε αποδοχή <u>δεν</u> ισοδυναμεί με το να ισχύει η $\varphi$ για την πλειοψηφία των δυνατών σχέσεων $C_1^{2k} \dots C_g^{2k} \Delta^k$.

Συγκεκριμένα, η *ύπαρξη* σχέσεων $C_1^{2k} \dots C_g^{2k} \Delta^k$ τέτοιων ώστε να ισχύει η $\varphi$ συνεπάγεται ύπαρξη μονοπατιού που καταλήγει σε αποδοχή (όπως είδαμε στην υποενότητα 3.3). Όμως, <u>δεν</u> αντιστοιχεί κάθε συνδυασμός σχέσεων $C_1^{2k} \dots C_g^{2k} \Delta^k$ σε μονοπάτι της αντίστοιχης μηχανής Turing. Επομένως, η πρόταση αυτή θα χρειαστεί περαιτέρω τροποποίηση για να καταλήξουμε σε λογική περιγραφή της κλάσης $PP$.

Ο ποσοδείκτης που θα ορίσουμε θέλουμε να περιορίζει το σύνολο των πραγμάτων για τα οποία αναζητούμε πλειοψηφία. Δεν θέλουμε να αναφέρεται σε πλειοψηφία όλων των αντικειμένων του σύμπαντος ή όλων των δυνατών $k$-αδικών σχέσεων, γιατί έτσι θα καταλήξουμε στο πρόβλημα που εξηγήσαμε παραπάνω.

Ορίζουμε αρχικά τον ποσοδείκτη μας για στοιχεία πρώτης τάξης:

<u>Ορισμός (Ποσοδείκτης $MAJ$)</u>

Έστω φόρμουλες πρώτης τάξης $\varphi(x,\vec{y}), \psi(x,\vec{y})$, με ελεύθερες μεταβλητές $x, \vec{y}$. Ορίζουμε έναν ποσοδείκτη $MAJ$ (majority) με τον οποίο μπορεί να κατασκευαστεί μία νέα φόρμουλα $MAJ\ x\ [\psi(x,\vec{y})]\ \varphi(x,\vec{y})$, με ελεύθερες μεταβλητές $\vec{y}$. Ο ποσοδείκτης θα έχει την εξής σημασιολογία, όπου $\vec{a}$ η ερμηνεία των $\vec{y}$:

$$A \vDash MAJ\ x\ [\psi(x,\vec{a})]\ \varphi(x,\vec{a}) \quad \leftrightarrow \quad |\{b \in |A| : A \vDash \psi(b,\vec{a}) \wedge \varphi(b,\vec{a})\}| > \frac{|\{b \in |A| : A \vDash \psi(b,\vec{a})\}|}{2}$$

Με λόγια, η σημασία αυτού του ποσοδείκτη είναι ότι *περισσότερα από τα μισά* στοιχεία $x$ που ικανοποιούν την $\psi$, ικανοποιούν και την $\varphi$.

Με προφανή τρόπο μπορούμε να επεκτείνουμε αυτό τον ορισμό και για στοιχεία δεύτερης τάξης. Για παράδειγμα, η παρακάτω πρόταση θα σημαίνει ότι για περισσότερες από τις μισές σχέσεις $R^1$ για τις οποίες ισχύει $\psi(R)$, ισχύει και $\varphi(R)$.

$$MAJ\ R^1\ [\psi(R)]\ \varphi(R)$$

Θεωρούμε επίσης ότι μπορούμε να χρησιμοποιήσουμε tuples σχέσεων δίπλα σε αυτόν τον ποσοδείκτη, όπως στην παρακάτω πρόταση:

$$MAJ\ (R^1, Q^3)\ [\psi(R,Q)]\ \varphi(R,Q)$$

Παρακάτω δίνουμε έναν αυστηρότερο ορισμό για tuples σχέσεων:

<u>Ορισμός (Ποσοδείκτης $MAJ$ – Γενίκευση για tuples σχέσεων)</u>

Έστω δομή $A$, σύμβολα κατηγορημάτων $R_1^{r_1}, \dots, R_k^{r_k}$ και φόρμουλες πρώτης τάξης $\varphi\left(R_1^{r_1} \dots R_k^{r_k}\right)$, $\psi\left(R_1^{r_1} \dots R_k^{r_k}\right)$. Χάριν συντομίας θα γράφουμε $\varphi(\vec{R})$ και $\psi(\vec{R})$. Ορίζουμε έναν ποσοδείκτη $MAJ$, με τον οποίο μπορεί να κατασκευαστεί μία νέα φόρμουλα $MAJ\ \left(R_1^{r_1} \dots R_k^{r_k}\right)\ [\psi(\vec{R})]\ \varphi(\vec{R})$.

Έστω επίσης $B$ το σύνολο των συνδυασμών τιμών που μπορούν να πάρουν τα κατηγορήματα $R_1^{r_1}, \dots, R_k^{r_k}$ στη δομή $A$. Για να ορίσουμε αυστηρά το σύνολο $B$, θα χρησιμοποιήσουμε τον συμβολισμό $Sub(T)$ για το σύνολο των υποσυνόλων ενός συνόλου $T$. Έτσι, είναι:

$$B = Sub(|A|^{r_1}) \times \dots \times Sub(|A|^{r_k})$$

Ο νέος ποσοδείκτης θα έχει την εξής σημασιολογία:

$$A \vDash MAJ\ \left(R_1^{r_1} \dots R_k^{r_k}\right)\ [\psi(\vec{R})]\ \varphi(\vec{R}) \leftrightarrow$$

$$\leftrightarrow \left|\left\{\vec{S} = (S_1, \dots, S_k) \in B : A \vDash \psi(\vec{S}) \wedge \varphi(\vec{S})\right\}\right| > \frac{\left|\left\{\vec{S} = (S_1, \dots, S_k) \in B : A \vDash \psi(\vec{S})\right\}\right|}{2}$$

Ακολουθεί το βασικό θεώρημα αυτής της υποενότητας:

<u>Θεώρημα ($PP = SO[MAJ]$)</u>

Η κλάση πολυπλοκότητας $PP$ περιέχει ακριβώς τα προβλήματα που μπορούν να περιγραφούν σε λογική δεύτερης τάξης εφοδιασμένη με τον ποσοδείκτη $MAJ$ για tuples σχέσεων, με την επιπλέον προϋπόθεση ότι ο ποσοδείκτης αυτός επιτρέπεται να χρησιμοποιηθεί το πολύ μία φορά και αποκλειστικά και μόνο στην αρχή της πρότασης. Αυτή η λογική, μαζί με την προϋπόθεση που αναφέραμε, θα καλείται $SO[MAJ]$.

Απόδειξη ($PP = SO[MAJ]$)

1. $PP \subseteq SO[MAJ]$:

Κατ' αντιστοιχία με το δεύτερο σκέλος της απόδειξης του θεωρήματος του Fagin (την οποία παρουσιάσαμε στην ενότητα 3.3), σκοπός μας είναι να βρούμε πρόταση $SO[MAJ]\ \Phi$, τέτοια ώστε για μια πολυωνυμική PTM $M$ να ισχύει $A \vDash \Phi$ αν και μόνο αν η πλειοψηφία των πιθανών μονοπατιών της $M$ καταλήγει σε αποδοχή.

Υπενθυμίζουμε την πρόταση $SO\exists$ που είχε δοθεί για την απόδειξη του θεωρήματος του Fagin:

$$\Phi \equiv \left(\exists C_1^{2k} \dots C_g^{2k} \Delta^k\right)\varphi$$

Οι αντίστοιχες σχέσεις είχαν την εξής σημασία:

- $C_i^{2k}$: Το κελί $\vec{s}$ τη χρονική στιγμή $\vec{t}$ έχει περιεχόμενο $\gamma_i \in \Gamma$.
- $\Delta^k$: Τη χρονική στιγμή $\vec{t}$ η μηχανή $N$ λαμβάνει την απόφαση '1' (αλλιώς λαμβάνει την απόφαση '0').

Για την φόρμουλα πρώτης τάξης $\varphi$ είχαμε:

$$\varphi \equiv \alpha \wedge \beta \wedge \eta \wedge \zeta$$

Τέλος, οι φόρμουλες $\alpha, \beta, \eta, \zeta$ εξέφραζαν τα παρακάτω:

- $\alpha$: Για $\vec{t} = 0$ πρέπει το περιεχόμενο των κελιών να περιέχει τη δυαδική αναπαράσταση της δομής $A$.
- $\beta$: Δεν ισχύει $C_i(\vec{s}, \vec{t}) \wedge C_j(\vec{s}, \vec{t})$ για $i \neq j$.
- $\eta$: Το περιεχόμενο των κελιών τη στιγμή $\vec{t} + 1$ καθορίζεται από το περιεχόμενό τους τη στιγμή $\vec{t}$, με βάση την απόφαση $\Delta(\vec{t})$.
- $\zeta$: Για $\vec{t} = n^k - 1$ η μηχανή περιέχει την κατάσταση αποδοχής.

Οι προτάσεις $\alpha, \beta, \eta, \zeta$ είχαν διατυπωθεί στην αντίστοιχη απόδειξη, είτε ρητά είτε περιγραφικά. Δεν θα επαναλάβουμε τη διατύπωσή τους, καθώς δεν προσφέρει κάτι καινούργιο σε αυτή την απόδειξη.

Αυτό που πρέπει να προσέξουμε είναι ότι θέλουμε η πλειοψηφία των έγκυρων μονοπατιών (δηλαδή των μονοπατιών **για τα οποία ισχύουν οι προτάσεις $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\eta}$**) να καταλήγει σε αποδοχή, δηλαδή **να ικανοποιεί την πρόταση $\boldsymbol{\zeta}$**. Επομένως, η πρόταση που θέλουμε αυτή τη φορά είναι η εξής:

$$\Phi' \equiv MAJ\ \left(C_1^{2k} \dots C_g^{2k} \Delta^k\right)\ [\alpha \wedge \beta \wedge \eta]\ \zeta$$

Η πρόταση αυτή αληθεύει αν και μόνο αν περισσότερα από τα μισά μονοπάτια της $M$ καταλήγουν σε αποδοχή, επομένως αποδείξαμε το ζητούμενο.

2. $SO[MAJ] \subseteq PP$:

Σκοπός μας είναι να κατασκευάσουμε μια πολυωνυμική PTM $M$ τέτοια ώστε για κάθε δομή $A$ να είναι $A \vDash \Phi$ ($\Phi$: πρόταση $SO[MAJ]$) αν και μόνο αν η πλειοψηφία των πιθανών μονοπατιών της $M$ καταλήγει σε αποδοχή. Έστω η παρακάτω πρόταση:

$$\Phi \equiv MAJ\left(R_1^{r_1} \dots R_k^{r_k}\right)[\psi]\,\varphi$$

Διευκρινίζουμε ότι οι $\varphi, \psi$ είναι φόρμουλες πρώτης τάξης. Κατ' αναλογία με το πρώτο σκέλος της απόδειξης του Fagin, η μηχανή μας θα εξετάσει τυχαία έναν από τους συνδυασμούς τιμών των σχέσεων $R_i$, ελέγχοντας εάν ισχύουν τα παρακάτω:

$$(A, R_1, \dots, R_k) \vDash \psi$$

$$(A, R_1, \dots, R_k) \vDash \varphi$$

Θέτοντας $n = \|A\|$, σχετικά με το πλήθος $\sigma$ των συνδυασμών αυτών έχουμε:

$$\sigma = 2^{\sum_{i=1}^{k} n^{r_i}}$$

Η μηχανή $M$ θα δίνει τις παρακάτω απαντήσεις, αναλόγως με τα αποτελέσματα των ελέγχων της:

| $(A, R_1, \dots, R_k) \vDash \psi$ | $(A, R_1, \dots, R_k) \vDash \varphi$ | Απόκριση Μηχανής $M$ | Πλήθος συνδυασμών |
|---|---|---|---|
| Ψευδής | Ψευδής | Αποδοχή/Απόρριψη με πιθανότητα 1/2 | $a$ |
| Ψευδής | Αληθής | | |
| Αληθής | Ψευδής | Απόρριψη | $b$ |
| Αληθής | Αληθής | Αποδοχή | $c$ |

Σημειώνουμε ότι είναι $\sigma = a + b + c$. Με βάση τα παραπάνω, έχουμε πιθανότητα αποδοχής:

$$P(A) = \frac{1}{\sigma}\left(\frac{1}{2}a + c\right) = \frac{1}{\sigma}\left(\frac{1}{2}(\sigma - b - c) + c\right) = \boldsymbol{\frac{\sigma + c - b}{2\sigma}}$$

Στόχος μας είναι να έχουμε $P(A) > 1/2$ όταν $A \vDash \Phi$ και $P(A) \leq 1/2$ όταν $A \nvDash \Phi$. Διακρίνουμε λοιπόν τις περιπτώσεις:

α) Είναι $A \vDash \Phi$:

Σε αυτή την περίπτωση η μηχανή **οφείλει να αποδεχτεί με πιθανότητα μεγαλύτερη του $\mathbf{1/2}$**. Αφού είναι $A \vDash MAJ\left(R_1^{r_1} \dots R_k^{r_k}\right)[\psi]\,\varphi$, θα έχουμε $c > b$, άρα $\boldsymbol{c - b \geq 1}$. Επομένως έχουμε:

$$P(A) = \frac{\sigma + c - b}{2\sigma} \geq \frac{\sigma + 1}{2\sigma} > \frac{1}{2}$$

β) Είναι $A \nvDash \Phi$:

Σε αυτή την περίπτωση η μηχανή **οφείλει να αποδεχτεί με πιθανότητα μικρότερη ή ίση του $\mathbf{1/2}$**. Είναι $A \nvDash MAJ\left(R_1^{r_1} \dots R_k^{r_k}\right)[\psi]\,\varphi$, άρα $c \leq b$, δηλαδή $\boldsymbol{c - b \leq 0}$. Προκύπτει ότι:

$$P(A) = \frac{\sigma + c - b}{2\sigma} \leq \frac{\sigma}{2\sigma} = \frac{1}{2}$$

Σχετικά με το χρόνο που χρειάζεται η μηχανή για τους ελέγχους σημειώνουμε ότι επειδή είναι $FO \subseteq L \subseteq P$, οι έλεγχοι $(A, R_1, \dots, R_k) \vDash \psi, (A, R_1, \dots, R_k) \vDash \varphi$ γίνονται σε πολυωνυμικό χρόνο (αφού οι $\varphi, \psi$ είναι φόρμουλες πρώτης τάξης). ■

### 7.2.3. Εφαρμογές

Για να φανεί η χρησιμότητα της λογικής που ορίσαμε, θα δείξουμε με αυτή ότι η κλάση $PP$ είναι κλειστή ως προς συμπλήρωμα.

Θεώρημα

Η κλάση $PP$ είναι κλειστή ως προς συμπλήρωμα. Ισοδύναμα, η άρνηση μιας πρότασης $SO[MAJ]$ ανήκει επίσης στη λογική $SO[MAJ]$.

Απόδειξη

Έστω η εξής πρόταση:

$$\Phi \equiv \neg\, MAJ\, \left(R_1^{r_1} \dots R_k^{r_k}\right) \left[\psi\left(R_1^{r_1} \dots R_k^{r_k}\right)\right] \varphi\left(R_1^{r_1} \dots R_k^{r_k}\right)$$

Για συντομία θα γράφουμε:

$$\Phi \equiv \neg\, MAJ\, \vec{R}\, \left[\psi(\vec{R})\right] \varphi(\vec{R})$$

Επίσης, ορίζουμε τα εξής για ευκολία στη γραφή:

- $x = \left|\left\{\vec{S} \in B : A \vDash \psi(\vec{S}) \land \varphi(\vec{S})\right\}\right|$
- $y = \left|\left\{\vec{S} \in B : A \vDash \psi(\vec{S}) \land \neg\varphi(\vec{S})\right\}\right|$
- $z = \left|\left\{\vec{S} \in B : A \vDash \psi(\vec{S})\right\}\right|$

Υπενθυμίζουμε ότι με $B$ συμβολίζουμε το σύνολο των συνδυασμών τιμών που μπορούν να πάρουν τα κατηγορήματα $R_1^{r_1}, \dots, R_k^{r_k}$ στη δομή $A$. Δηλαδή:

$$B = Sub(|A|^{r_1}) \times \dots \times Sub(|A|^{r_k})$$

Θα δείξουμε ότι για την $\Phi$ υπάρχει ισοδύναμη πρόταση $\Phi' \in SO[MAJ]$. Από τον ορισμό του ποσοδείκτη $MAJ$ έχουμε:

$$A \vDash MAJ\, \vec{R}\, \left[\psi(\vec{R})\right] \varphi(\vec{R}) \leftrightarrow x > \frac{z}{2}$$

Άρα είναι:

$$A \vDash \Phi \leftrightarrow x \leq \frac{z}{2}$$

Επειδή έχουμε $z = x + y$, είναι:

$$A \vDash \Phi \leftrightarrow y \geq \frac{z}{2}$$

Επειδή $x, y, z$ ακέραιοι, είναι:

$$y \geq \frac{z}{2} \leftrightarrow y > \frac{z-1}{2}$$

Το ίδιο θα ίσχυε αν από το δεξί μέλος αφαιρούσαμε **οποιονδήποτε άλλο αριθμό $\boldsymbol{\varepsilon} \in (\mathbf{0}, \mathbf{1/2})$**, αντί για το $1/2$ που αφαιρέσαμε παραπάνω:

$$y \geq \frac{z}{2} \leftrightarrow y > \frac{z}{2} - \varepsilon, \qquad \varepsilon \in \left(0, \frac{1}{2}\right)$$

Άρα:

$$\boldsymbol{A \vDash \Phi \leftrightarrow y > \frac{z}{2} - \varepsilon}, \qquad \varepsilon \in \left(0, \frac{1}{2}\right)$$

Σε αυτό το σημείο θα προσπαθήσουμε να ορίσουμε τη ζητούμενη πρόταση $\Phi'$. Θέτουμε $n = \|A\|$. Τότε, το πλήθος των συνδυασμών των τιμών των $\vec{R}$ είναι:

$$\sigma = 2^{\sum_{i=1}^{k} n^{r_i}}$$

Ορίζουμε κάποιο άλλο σύνολο συμβόλων κατηγορημάτων $\vec{Q}$, το οποίο να είναι *σημαντικά* μεγαλύτερο στο πλήθος συνδυασμών τιμών που μπορεί να πάρει συγκριτικά με το $\vec{R}$. Συγκεκριμένα, αν για το $\vec{Q}$ υπάρχουν $\sigma'$ συνδυασμοί τιμών, απαιτούμε να ισχύει:

$$\sigma' > 2\sigma$$

Θεωρούμε μία φόρμουλα $\chi(\vec{Q})$, **η οποία να ικανοποιείται για έναν ακριβώς συνδυασμό τιμών των $\vec{Q}$**. Συγκεκριμένα, θα ικανοποιείται μόνο στην περίπτωση που όλες οι σχέσεις $Q_i$ ικανοποιούνται για όλες τις τιμές των ορισμάτων τους. Η $\chi(\vec{Q})$ διατυπώνεται ως εξής:

$$\chi(\vec{Q}) \equiv \forall x_1 \dots x_{q_1} Q_1^{q_1}(x_1, \dots, x_{q_1}) \wedge \dots \wedge \forall x_1 \dots x_{q_k} Q_k^{q_k}(x_1, \dots, x_{q_k})$$

Έστω $B'$ ένα σύνολο παρόμοιο με το $B$, αλλά με τις πληθικότητες των $\vec{Q}$ αντί για τα $\vec{R}$. Θεωρούμε την εξής πρόταση:

$$\Phi' \equiv MAJ\ (\vec{R}, \vec{Q})\ [\psi(\vec{R})] \left(\neg\varphi(\vec{R}) \vee \chi(\vec{Q})\right)$$

Έχουμε:

$$A \vDash \Phi' \leftrightarrow \left|\left\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S}) \wedge \left(\neg\varphi(\vec{S}) \vee \chi(\vec{S}')\right)\right\}\right| > \frac{\left|\left\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S})\right\}\right|}{2}$$

Η πρόταση στο αριστερό μέλος της ανισότητας γράφεται ισοδύναμα ως:

$$\psi(\vec{S}) \wedge \neg\varphi(\vec{S}) \vee \psi(\vec{S}) \wedge \chi(\vec{S}')$$

Επομένως, είναι:

$$A \vDash \Phi' \leftrightarrow \left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S}) \wedge \neg\varphi(\vec{S}) \vee \psi(\vec{S}) \wedge \chi(\vec{S}')\}\right| > \frac{\left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S})\}\right|}{2}$$

Σχετικά με τις ποσότητες που εμφανίζονται στην παραπάνω ανισότητα έχουμε:

- $\left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S}) \wedge \neg\varphi(\vec{S})\}\right| = \sigma' y$
  Οι τιμές των $\vec{S}'$ είναι αδιάφορες για τις φόρμουλες $\psi(\vec{S}), \varphi(\vec{S})$ και επομένως, για καθέναν από τους $y$ συνδυασμούς τιμών που είχαμε αρχικά (πριν την προσθήκη των $\vec{S}'$), τώρα έχουμε $\sigma'$ συνδυασμούς.

- $\left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S}) \wedge \chi(\vec{S}')\}\right| = z$
  Η $\chi(\vec{S}')$ ικανοποιείται μόνο για έναν συνδυασμό $\vec{S}'$, ενώ η $\psi(\vec{S})$ για $z$ συνδυασμούς $\vec{S}$.

- $\left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S}) \wedge \neg\varphi(\vec{S}) \vee \psi(\vec{S}) \wedge \chi(\vec{S}')\}\right| = \sigma' y + z - y$
  Πρόκειται για τη διάζευξη των δύο προηγούμενων προτάσεων, επομένως το αποτέλεσμα είναι ίσο με το άθροισμα των προηγούμενων δύο πλην το πλήθος συνδυασμών που ικανοποιούν την αντίστοιχη σύζευξη. Το τελευταίο είναι ίσο με $y$, αφού η $\chi(\vec{S}')$ ικανοποιείται μόνο για έναν συνδυασμό $\vec{S}'$ και η $\psi(\vec{S}) \wedge \neg\varphi(\vec{S})$ για $y$ συνδυασμούς $\vec{S}$.

- $\left|\{\vec{S} \in B, \vec{S}' \in B' : A \vDash \psi(\vec{S})\}\right| = \sigma' z$
  Ομοίως με την πρώτη ποσότητα.

Με βάση τα παραπάνω, καταλήγουμε:

$$A \vDash \Phi' \leftrightarrow \sigma' y + z - y > \frac{\sigma' z}{2} \leftrightarrow$$

$$\leftrightarrow y > \frac{z}{2} - \frac{z-y}{\sigma'}$$

Είχαμε απαιτήσει $\sigma' > 2\sigma$ και είναι $z - y < \sigma$. Επομένως:

$$\frac{z-y}{\sigma'} < \frac{1}{2}$$

Άρα η παραπάνω ανισότητα γράφεται ως:

$$\boldsymbol{y} > \frac{\boldsymbol{z}}{\boldsymbol{2}} - \boldsymbol{\varepsilon}, \qquad \varepsilon = \frac{z-y}{\sigma'} \in \left(0, \frac{1}{2}\right)$$

Το παραπάνω, όπως είδαμε πρωτύτερα, είναι ισοδύναμο με $\boldsymbol{A \vDash \Phi}$. Στην ειδική περίπτωση όπου $z = y,\ \varepsilon = 0$, είναι εύκολο να δούμε ότι $A \vDash \Phi$ και $A \vDash \Phi'$.

Συμπεραίνουμε ότι ισχύει $\boldsymbol{A \vDash \Phi \leftrightarrow A \vDash \Phi'}$, με $\Phi' \in SO[MAJ]$. ■

Σημειώνουμε πως έγινε και μία προσπάθεια να αποδειχθεί με αντίστοιχο τρόπο η κλειστότητα της $PP$ ως προς τομή και ένωση, ωστόσο αυτή η ιδιότητα φαίνεται να είναι αρκετά πιο δύσκολη στην απόδειξή της.

# 8. Συμπεράσματα – Παρατηρήσεις

Με βάση όσα παρουσιάστηκαν στην εργασία, είναι φανερή η χρησιμότητα της εύρεσης λογικών περιγραφών για την παραγωγή συμπερασμάτων για κλάσεις πολυπλοκότητας. Είδαμε ότι στην κλάση $\#P$ μπορούμε να έχουμε εγγυήσεις για το αν ένα πρόβλημα λύνεται σε πολυωνυμικό χρόνο ή επιδέχεται FPRAS, αναλόγως με την εκφραστικότητα που απαιτεί η λογική του περιγραφή.

Επιπλέον, είδαμε ότι τα περισσότερα προβλήματα μέτρησης είναι αρκετά δυσκολότερα από τα αντίστοιχα προβλήματα απόφασης. Συγκεκριμένα, είδαμε ότι ακόμα και μερικά προβλήματα της κλάσης $P$ δίνουν αντίστοιχα μετρητικά προβλήματα που είναι $\#P$-πλήρη, ενώ τα προβλήματα της $\#P$ που λύνονται σε πολυωνυμικό χρόνο είναι ελάχιστα. Συμπεραίνουμε ότι για την πλειονότητα των προβλημάτων μέτρησης κρίνεται σκόπιμο να προσανατολιστούμε σε προσεγγιστικές λύσεις, π.χ. FPRAS. Αυτό καταδεικνύει και την αξία των εγγυήσεων για ύπαρξη FPRAS που δίνει η λογική περιγραφή της κλάσης $\#P$, όπως αναφέραμε παραπάνω.

Στο τελευταίο κεφάλαιο είδαμε πώς μπορούμε να επεκτείνουμε ήδη υπάρχουσες λογικές περιγραφές για να παράξουμε περιγραφές για κλάσεις σχετικές με μετρητικά προβλήματα. Παρατηρήσαμε ότι η λογική που χρειάστηκε για την κλάση $PP$ είναι αρκετά περίπλοκη και δύσχρηστη. Με βάση αυτή τη λογική δόθηκε μία απόδειξη για την κλειστότητα της $PP$ ως προς συμπλήρωμα, ωστόσο αυτή η απόδειξη μάλλον είναι δυσκολότερη και πιο περίπλοκη από την κλασική απόδειξη (η οποία δεν στηρίζεται σε περιγραφική πολυπλοκότητα). Προφανώς ενδέχεται να υπάρχει περιθώριο βελτίωσης - απλούστευσης της απόδειξης ή της λογικής που δόθηκε, ωστόσο μάλλον οδηγούμαστε στο συμπέρασμα ότι οι λογικές περιγραφές δεν είναι εξίσου εύχρηστες για όλες τις κλάσεις.

Με την ίδια λογική που ορίσαμε για την $PP$ προσπαθήσαμε να αποδείξουμε και την κλειστότητα της $PP$ ως προς τομή ή ένωση. Μετά από πολλές προσπάθειες και δοκιμές, φαίνεται δύσκολο να αποδειχθεί κάτι τέτοιο με χρήση αυτής της λογικής. Αυτό δεν μας εκπλήσσει, καθώς το ερώτημα για το αν η $PP$ είναι κλειστή ως προς τομή ή ένωση παρέμεινε ανοιχτό για πολλά χρόνια. Επιπλέον, η υπάρχουσα απόδειξή του [BRS95] είναι επίσης αρκετά περίπλοκη και δύσκολη.

Μια άλλη ενδιαφέρουσα κλάση την οποία θα μπορούσαμε να είχαμε μελετήσει είναι η TotP [PZ06]. Στη διατριβή [Cha22] έχει δοθεί, μεταξύ άλλων, ένας λογικός χαρακτηρισμός αυτής της κλάσης. Η κλάση TotP περιέχει σημαντικά προβλήματα μέτρησης, όπως το PERMANENT και το $\#DNF$.

Ένα ενδιαφέρον ανοιχτό ερώτημα είναι να χαρακτηρίσει κανείς με λογικό τρόπο υποκλάσεις της TotP και να διερευνηθεί αν μπορούμε να πάρουμε με αυτόν τον τρόπο αποτελέσματα σχετικά με την προσεγγισιμότητά τους.

# 9. Βιβλιογραφία


[ACJR21] Arenas, M., Croquevielle, L., Jayaram, R., & Riveros, C. (2021). When Is Approximate Counting for Conjunctive Queries Tractable? *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing*, (pp. 1015-1027).

[AMR20] Arenas, M., Muñoz, M., & Riveros, C. (2020). Descriptive Complexity for Counting Complexity Classes. *Logical Methods in Computer Science, 16*(1), pp. 9:1–9:42.

[AB09] Arora, S., & Barak, B. (2009). *Computational Complexity: A Modern Approach.* Cambridge University Press.

[BCP20] Eleni Bakali, Aggeliki Chalki, and Aris Pagourtzis. Characterizations and approximability of hard counting classes below #P. In Proc. of TAMC 2020, volume 12337 of Lecture Notes in Computer Science, pages 251–262. Springer, 2020.

[BRS95] Beigel, R., Reingold, N., & Spielman, D. (1995). PP is Closed Under Intersection. *Journal of Computer and System Sciences, 50*(2), pp. 191-202.

[Cha22] Aggeliki Chalki. Structural and Descriptive Complexity of Easy-to-Decide Counting Problems. PhD thesis, National Technical University of Athens, Greece, 2022.

[DGGJ04] Dyer, M., Goldberg, L., Greenhill, C., & Jerrum, M. (2004). On the Relative Complexity of Approximate Counting Problems. *Algorithmica, 38*, pp. 471–500.

[EF99] Ebbinghaus, H.-D., & Flum, J. (1999). *Finite Model Theory.* Springer.

[Fag74] Fagin, R. (1974). Generalized First-Order Spectra, and Polynomial Time Recognizable Sets. *Complexity of Computation, 7*, pp. 43-73.

[GSS08] Gabbay, D., Schmidt, R., & Szalas, A. (2008). *Second-Order Quantifier Elimination.* College Publications.

[GJ79] Garey, M., & Johnson, D. (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness.* New York: W. H. Freeman.

[Imm99] Immerman, N. (1999). *Descriptive Complexity.* Springer.

[Jan98] Jansen, T. (1998). *Lectures on Proof Verification and Approximation Algorithms.* (E. Mayr, H. Prömel, & A. Steger, Eds.) Berlin: Springer.

[KLM89] Karp, R., Luby, M., & Madras, N. (1989). Monte-Carlo Approximation Algorithms for Enumeration Problems. *Journal of Algorithms, 10*, pp. 429-448.

[Lib04] Libkin, L. (2004). *Elements of Finite Model Theory.* (W. Brauer, G. Rozenberg, & A. Salomaa, Eds.) Berlin: Springer.

[Mun17] Muñoz, M. (2017). *Descriptive Complexity for Counting Complexity Classes.* Santiago de Chile.

[Pap94] Papadimitriou, C. (1994). *Computational Complexity.* Addison-Wesley.

[PZ06] Aris Pagourtzis and Stathis Zachos. The complexity of counting functions with easy decision version. In Proc. of MFCS 2006, volume 4162 of Lecture Notes in Computer Science, pages 741–752, 2006.

[SST95] Saluja, S., Subrahmanyam, K., & Thakur, M. (1995). Descriptive Complexity of #P Functions. *Journal of Computer and System Sciences, 50*, pp. 493-505.

[Sip97] Sipser, M. (1997). *Introduction to the Theory of Computation.* Boston: PWS Publishing.

[Sto77] Stockmeyer, L. (1977). The Polynomial-Time Hierarchy. *Theoretical Computer Science, 3*, pp. 1-22.

[Tod91] Toda, S. (1991). PP is as Hard as the Polynomial-Time Hierarchy. *SIAM Journal on Computing, 20*(5), pp. 865-877.

[Val76] Valiant, L. (1976). Relative Complexity of Checking and Evaluating. *Information Processing Letters, 5*(1), pp. 20-23.

[Val79] Valiant, L. (1979). The Complexity of Computing the Permanent. *Theoretical Computer Science, 8*, pp. 189-201.

[Vaz04] Vazirani, V. (2004). *Approximation Algorithms.* Berlin: Springer.