ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Εργαστήριο Λογικής κι Επιστήμης Υπολογισμών - CoReLAB

#P:Πολυπλοκότητα και προσεγγιστικές τεχνικές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σοφία Καρύγιαννη

Επιβλέπων: Ζάχος Ευστάθιος
Καθηγητής ΕΜΠ

Αθήνα, Ιούλιος 2007

Εθνικο Μετσοβιο Πολυτεχνειο
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

#P:Πολυπλοκότητα και προσεγγιστικές τεχνικές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σοφία Καρύγιαννη

Επιβλέπων: Στάθης Ζάχος
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 26-7-2007.

.....	.....	.....
Ζάχος Σ.	Παπαϊωάννου Α.	Παγουρτζής Ά.
Καθηγητής ΕΜΠ	Επίκουρος Καθηγητής ΕΜΠ	Λέκτορας ΕΜΠ

Αθήνα, Ιούλιος 2007.

.....

Σοφία Καρύγιαννη
Διπλωματούχος Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών ΕΜΠ

Περίληψη

Η διπλωματική αυτή αφορά την κλάση #P. Ασχολείται κυρίως με το ποιά προβλήματα περιέχει αυτή η κλάση ,πόσο δύσκολα είναι και τι μπορούμε να κάνουμε για να τα λύσουμε αποδοτικά έστω και με προσεγγιστικό τρόπο.
Στο πρώτο κεφάλαιο ορίζουμε ποιά είναι η κλάση #P και συγκρίνουμε την πολυπλοκότητά της με αυτή της πολυωνυμικής ιεραρχίας(PH). Συμπεραίνουμε τελικά ότι το #P δεν περιέχεται σε κανένα επίπεδο της PH και άρα μάλλον είναι πιο 'δύσκολο' από αυτή.
Με δεδομένο λοιπόν ότι δεν είναι πολύ πιθανό να μπορέσουμε να λύσουμε ακριβώς με αποδοτικό τρόπο τα προβλήματα αυτής της κλάσης στρέφουμε την προσοχή μας στην έννοια της προσέγγισης. Στο δεύτερο κεφάλαιο αναφέρουμε όλους τους απαραίτητους ορισμούς - προσεγγιστικοί, πιθανοτικοί αλγόριθμοι - καθώς και την μέρχρι τώρα εικόνα της κλάσης #P ως προς την ύπαρξη ή όχι FPRAS αλγορίθμων.
Η ύπαρξη ή όχι FPRAS για κάποια προβλήματα είναι ακόμη ανοικτό ερώτημα και η απάντηση δεν μπορεί να δοθεί απλά. Για αυτό το λόγο στο τρίτο κεφάλαιο ασχολούμαστε με την συχέτιση του FPRAS με το FPAUS δηλαδή πολυωνυμικούς αλγορίθμους που επιτυχγάνουν σχεδόν ομοίομορφη δειγματοληψία χώρων αγνώστου διάστασης - αλλά πεπερασμένης. Αναγάγουμε με αυτό τον τρόπο την δημιουργία FPRAS στην ύπαρξη FPAUS για κάποιες κατηγορίες προβλημάτων. Στο τελευταίο κεφάλαιο αναφερόμαστε σύντομα σε μία άλλη κατηγοριοποίηση των προβλημάτων του #P, που βασίζεται περισσότερο σε δομικά χαρακτηριστικά των προβλημάτων και επιδιώκουμε την συσχέτιση αυτών με τις κλάσεις που έχουν αναφερθεί στα προηγούμενα.Τα ερωτηματικά σε αυτή την ανάλυση είναι πολλά και η σχέση κάθε άλλο παρά σαφής είναι αυτή τη στιγμή.
Περεταίρω ανάλυση αυτού του θέματος καθώς και του ζητήματος της συσχέτισης FPRAS με FPAUS είναι δυνατή και σίγουρα ενδιαφέρουσα.

Abstract

The theme of this diploma thesis is the class #P. The subjects that are mainly addressed are the problems that are included in this class, their hardness as well as manners to approximate them.
At the first chapter we define the class #P and we try to find out its relationship with the polynomial hierarchy(PH). At last, we prove that #P doesn't belong to any level of the PH and so it is probably harder to solve.
Taking as granded that it is not likely to be able to produce precise solutions to #P problems efficiently we start getting interested in approximation techniques. At the second chapter we provide the reader with all the necessary definitions - approximation and randomized algorithms - and we present the results related to the so far known subclasses of #P with respect to the existence of FPRAS.
The existence of an FPRAS algorithm for a problem is an open matter in many cases and it doesn't seem easy to find out the answer. So, at the third chapter we explore the relation between the FPRAS and FPAUS, that means fully polynomially almost uniform samplers for spaces of unknown but finite distance. Our intention is to show the equivalence between the two for some problems characterized by the property of self reducibility.Finally at the last chapter we present some other subclasses of the #P based mainly on structural properties of the problems. We try to clarify the relation between these classes and the ones presented previously but the connection is not yet very clear.
Further research for this matter as well as for the connection between FPRAS and FPAUS is possible and undoubtedly very interesting.

Ευχαριστίες

Συνήθως προτιμώ να ευχαριστώ τους ανθρώπους που με βοηθούν σε προσωπικό επίπεδο αλλά όταν αφορά πράγματα τα οποία δημοσιοποιούνται επιβάλλεται να αναφέρεται και η συμβολή όλων αυτών χωρίς τους οποίους η κατάσταση μάλλον δεν θα ήταν η ίδια τελικά..Θέλω λοιπόν να ευχαριστήσω πολύ τους κυρίους Σ.Ζάχο και Α.Παγουρτζή για την υποστήριξή και την υπομονή τους σε όλο το διάστημα της εκπόνησης της διπλωματικής εργασίας καθώς και για την εμπιστοσύνη που έδειξαν στο πρόσωπό μου. Επίσης θα ήθελα να ευχαριστήσω όλα τα μέλη του εργαστηρίου (Co.Re.Lab) για την άψογη συνεργασία και την παρουσία τους στις προκαταρκτικές παρουσιάσεις της διπλωματικής. Τέλος θέλω να ευχαριστήσω ιδιαιτέρως την Γεωργία Καούρη,τον Βαγγέλη Μπαμπά και τη Βάλια Μήτσου χωρίς τους οποίους αυτή η διπλωματική δεν θα είχε γραφτεί ποτέ σε LaTex...

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Συνήθως αυτό που μας ενδιαφέρει σε ένα πρόβλημα είναι να δούμε αν αυτό έχει λύση και αν ναι ποιά είναι αυτή. Οι πόροι (χρόνος και χώρος) που χρειαζόμαστε για την έυρεση μιας λύσης ποικίλλουν ανάλογα με το πρόβλημα. Έτσι υπάρχουν προβλήματα που λύνονται σε πολυωνυμικό χρόνο και χώρο ως προς το μέγεθος του input ,σε πολυωνυμικό χώρο αλλά εκθετικό χρόνο και άλλοι πολλοί συνδυασμοί που ο καθένας αντιστοιχεί και σε μία κλάση πολυπλοκότητας.Καθώς όμως αναπτύσσονταν ο κλάδος της θεωρίας της πολυπλοκότητας και οι επιστήμονες άρχισαν να ασχολούνται με τις αναγωγές του ενός προβλήματος στο άλλο διαπίστωσαν πως υπάρχουν πολλά προβλήματα για τα οποία είναι δυνατή η πολυωνυμική αναγωγή στιγμιοτύπων του ενός στο άλλο με τέτοιο τρόπο ώστε να διατηρείται σταθερό το πλήθος των λύσεων. Έτσι το να βρει κανείς μια λύση ενός προβλήματος έπαψε να είναι το μοναδικό μέλημα αφού πλέον και ο αριθμός των δυνατών λύσεων ενός προβλήματος θεωρούνταν σημαντικό χαρακτηριστικό. Το αποτέλεσμα ήταν ο όρισμός κλάσεων πολυπλοκότητας που να περιγράφουν το μέγεθος των πόρων που χρειάζεται κανείς για να υπολογίσει το πλήθος των δυνατών λύσεων.
Μιά τέτοια κλάση θα μας απασχολήσει και σε αυτή τη διπλωματική. Πρόκειται για το #P,του οποίου τον ορισμό τις ιδιότητες και άλλα ενδιάφεροντα χαρακτηριστικά θα δούμε στα επόμενα κεφάλαια. Η κλάση αυτή ορίστηκε πρώτη φορά από τον L.G.Valiant στο [Val]. Πηγή του ορισμού της υπήρξε το πρόβλημα του permanent - το οποίο θα δούμε αναλυτικά στο πρώτο κεφάλαιο - το οποίο αν και έχει σαφείς ομοιότητες με το πρόβλημα της ορίζουσας εντούτοις είναι πολύ πιο δύσκολο να υπολογισθεί. Στην προσπάθειά του ο Valiant να καταδείξει το πόσο δύσκολο είναι αυτό το πρόβλημα όρισε την κλάση #P γιατί διαπίστωσε πως το permanent είναι πλήρες πρόβλημα για αυτή την κλάση. Και από το τότε ξεκίνησε μία συζήτηση που δεν έχει ολοκληρωθεί ακόμη και αφορά την ακριβή κατηγοριοποίηση των προβλημάτων του #P, τις δυνατότητες προσέγγισης αυτού και τη σχέση του με τις άλλες κλάσεις πολυπλοκότητας. Πριν

προχωρήσουμε στην αναλυτική παρουσίαση όλων αυτών των θεμάτων ας δώσουμε κάποιους χρήσιμους ορισμούς. Πρόκειται για θεμελιώδεις έννοιες της θεωρίας της πολυπλοκότητας οπότε απευθύνεται μόνο στους αναγνώστες που δεν έχω ιδιαίτερη επαφή με το αντικείμενο.

Ορισμός 1.0.1 *Μία μηχανή Turing είναι μία συσκευή που διαθέτει μία ταινία ανάγνωσης και εγγραφής-δυνητικά άπειρη-, ένα αλφάβητο, ένα σύνολο καταστάσεων και η λειτουργία της διέπεται από μία συνάρτηση μετάβασης δ, η οποία καθορίζει τις δυνατές μεταβάσεις από την μία κατάσταση στην άλλη με βάσει τα σύμβολα στην ταινία.Σε κάθε βήμα η μηχανή διαβάζει ένα σύμβολο από την ταινία και ανάλογα με την κατάσταση στην οποία βρίσκεται είτε γράφει κάτι στην ταινία είτε μετακινείται προς τα αριστερά ή τα δεξιά αυτής. Ανάλογα με το αν για κάθε δυνατό ζευγάρι (κατάστασης,συμβόλου) υπάρχει μοναδική ή πολλές δυνατές ενέργειες η μηχανή ονομάζεται ντετερμινιστική ή μη ντετερμινιστική αντίστοιχα. Επίσης αν το πλήθος των απαραίτητων βημάτων για την επίλυση ενός προβλήματος φράσσεται από ένα πολυώνυμο του μήκους της αρχικής εισόδου στην μηχανή λέμε ότι πρόκειται για TM πολυωνυμικού χρόνου.Πρόκειται για ένα απλό μοντέλο ιδεατού υπολογιστή, το πρώτο που ορίστηκε ποτε.*

Στην παραπάνω θεμελιώδη έννοια της TM μπορούμε να προσθέσουμε και την δυνατότητα της χρήσης μαντείου για το πρόβλημα A, δηλαδή η TM σε κάθε βήμα της μπορεί να θέτει μία ερώτηση στο μαντείο για κάποιο στιγμιότυπο του προβλήματος A και να πέρνει ακαριαία την απάντηση. Οι πιο βασικές κλάσει πολυπλοκότητας, ή για την ακρίβεια αυτές που περισσότερο χρειάζονται για την κατανόηση των επόμενων κεφαλάιων είναι η κλάση P δηλαδή το σύνολο των προβλημάτων που μπορούν να λυθούν από μία ντετερμινιστική μηχανή Turing σε πολυωνυμικό χρόνο και η κλάση NP που περιέχει το σύνολο των προβλημάτων που μπορεί να λυθεί σε πολυωνυμικό χρόνο από μη ντετερμινιστικές μηχανές Turing(NTM).Στα επόμενα κεφάλαια η αναφορά σε NTM θα αφορά μόνο NTM με το πολύ δύο επιλογές σε κάθε βήμα - το μοντέλο αυτό είναι ισοδύναμο με τη γενική περίπτωση.

Ορισμός 1.0.2 *Η πολυωνυμική ιεραρχία ή PH σε συντομία ορίζει μία επαγωγική σειρά από κλάσεις προβλημάτων.Βασίζεται στη χρήση μαντείων και έχει ως εξής :*

1. $\Sigma_0^p = \Pi_0^p = \Delta_0^p = P$
2. $\Sigma_k^p = NP^{\Sigma_{k-1}^p}$
3. $\Pi_k^p = co - \Sigma_k^p$

4. $\Delta_k^p = P^{\Sigma_{k-1}^p}$

όπου με το co- ενοούμε το συμπλήρωμα και με τους 'εκθέτες' συμβολίζονται τα μαντεία. Η $PH = \bigcup_{k>0} \Sigma_k^p$

Επίσης απαραίτητο είναι να ορίσουμε κάποιες αναγωγές που θα αναφέρονται συχνά στη συνέχεια. Έχουμε λοιπόν :

Ορισμός 1.0.3 *Έστω δύο σύνολα A και B. Λέμε ότι το A μπορεί να αναχθεί κατά Cook στο B αν υπάρχει πολυωνυμικού χρόνου ντετερμινιστική μηχανή Turing η οποία με χρήσ μαντείου για το B μπορεί να αποφασίσει για το A.* ($A \leq_T^p B$)

Εάν το μαντείο χρησιμοποιείται μόνο μία φορά τότε λέμε ότι έχουμε μία αναγωγή κατά Cook[1].

Ορισμός 1.0.4 *Έστω δύο σύνολα A και B. Λέμε ότι το A μπορεί να αναχθεί κατά Karp στο B αν υπάρχει συνάρτηση πολυωνυμικού χρόνου τέτοια ώστε*

$$x \in A \Leftrightarrow f(x) \in B$$

Αλλά φτάνει πια με τα εισαγωγικά....Καιρός να μπούμε στο θέμα μας!!!

Κεφάλαιο 2

Ορισμός και πολυπλοκότητα της μετρητικής κλάσης #P

2.1 Ορισμός της κλάσης #P

Το #P ανήκει στην κατηγορία των μετρητικών κλάσεων δηλαδή των κλάσεων που περιέχουν συναρτήσεις που υπολογίζουν το πλήθος των δυνατών λύσεων για κάποιο στιγμιότυπο ενός προβλήματος. Προκειμένου να το ορίσουμε και τυπικά θα πρέπει να κατασκευάσουμε ένα υπολογιστικό μοντέλο που να μπορεί να περιγράψει πως υπολογίζονται αυτές οι συναρτήσεις. Η κλασσική έννοια της TM δεν αρκεί για τον παραπάνω ορισμό οπότε θα χρειαστεί να την επεκτείνουμε με τον εξής τρόπο:

Ορισμός 2.1.1 *[Val79] Μία μετρητική TM - counting TM - είναι μία κλασσική μη ντετερμινιστική TM η οποία έχει επιπλέον μία βοηθητική συσκευή εξόδου η οποία τυπώνει (με μαγικό τρόπο....), σε δυαδικό σύστημα, σε μία ειδική ταινία τον αριθμό των μονοπατιών που οδηγούν σε αποδοχή του input. Έχει χρονική πολυπλοκότητα - στην χειρότερη περίπτωση - $f(n)$ όπου $f(n)$ το μήκος του μακρύτερου μονοπατιού που προκύπτει από input μήκους n(όταν η TM λειτουργεί όπως στην κλασσική περίπτωση χωρίς τη βοηθητική συσκευή εξόδου).*

Έτσι μπορούμε πλέον να πούμε ότι :

Ορισμός 2.1.2 *[Val79] Το #P είναι η κλάση που περιέχει όλες τις συναρτήσεις που μπορούν να υπολογιστούν από counting TM πολυωνυμικής χρονικής πολυπλοκότητας.*

Δηλαδή το #P περιέχει όλες τις συναρτήσεις που μετράνε το πλήθος των μονοπατιών που αποδέχονται, σε πολυωνυμικού χρόνου μη ντετερμινιστικές

μηχανές Turing. Μέχρι τώρα πολλά ενδιαφέροντα προβλήματα έχει αποδειχθεί ότι ανήκουν στην κλάση αυτή. Για την ακρίβεια όλα τα προβλήματα που αφορούν την μέτρηση των δυνατών λύσεων προβλημάτων που ανήκουν στο NP εύκολα προκύπτει ότι ανήκουν στο #P. Μάλιστα μπορεί εύκολα να αποδειχθεί ότι αυτά τα προβλήματα είναι και complete για την κλάση #P. Το παράδοξο είναι ότι υπάρχουν και προβλήματα για τα οποία ενώ είναι εύκολο (στο P) να βρεις μια λύση - αν υπάρχει - (easy decision version) - εντούτοις το αντίστοιχο πρόβλημα μέτρησης είναι complete για την κλάση #P.΄Ενα τέτοιο πρόβλημα θα δούμε στην επόμενη ενότητα.

2.2 Permanent:΄Ενα #P-complete πρόβλημα

2.2.1 Ορισμός και παράδειγμα για το Permanent

Ορισμός 2.2.1 *΄Εστω ένας πίνακας A, διαστάσεων $n \times n$.Το permanent του A ορίζεται ως εξής :*

$$PermA = \sum_{\sigma} \prod_{i=1}^{n} A(i, \sigma(\iota))$$

όπου η άθροιση γίνεται πάνω σε όλες τις δυνατές μεταθέσεις του συνόλου 1,2,...,n.

Αν και δεν φαίνεται αμέσως το permanent είναι το ίδιο με την διακρίνουσα με θετικά όμως πρόσημα σε όλους τους όρους. Παρόλη όμως την ομοιότητα και ενώ υπάρχουν αποδοτικοί αλγόριθμου υπολογισμού της διακρίνουσας δεν ισχύει το ίδιο και για το permanent, για το οποίο οι μέχρι τώρα γνωστοί αλγόριθμοι απαιτούν εκθετικό χρόνο. Πολλές προσπάθειες έχουν γίνει για την αναγωγή του προβλήματος σε αυτό της διακρίνουσας μέσω ενός απλού μετασχηματισμού πινάκων αλλά όλες υπήρξαν άκαρπες. Μάλιστα ,το permanent είναι complete για την κλάση #P , όπως θα δούμε και στην παρακάτω ενότητα. Το permanent έχειεπίσης και γραφοθεωρητικές ερμηνείες. Για να τις αναφέρουμε όμως χρειαζόμαστε πρώτα τους παρακάτω ορισμούς:

Ορισμός 2.2.2 *΄Εστω πίνακας A $n \times n$ με στοιχεία από το σύνολο {0,1} - στο εξής θα αναφεόμαστε σε αυτούς ως {0,1}-πίνακες. Ο διμερής γράφος $G(V1, V2, E)$ που αντιστοιχεί στον A έχει $V1 = \{1, 2, ..., n\}, V2 = \{1, 2, ..., n\}$ και $(u_i, u_j) \in E \iff A(i, j) = 1$. Ο κατευθυνόμενος γράφος $G'(V, E)$ που αντιστοιχεί στον A έχει $V = \{1, 2, 3...., 2n\}$ και $(u_i, u_j) \in E \iff A(i, j) \neq 0$. Ο G' μπορεί να κατασκευαστεί και στην περίπτωση πινάκων με στοιχεία θετικούς αριθμούς απλά σε αυτή την περίπτωση η ˝κάθε ακμή έχει βάρος ίσο με το αντίστοιχο στοιχείο του πίνακα.*

Ορισμός 2.2.3 *Έστω γράφος $G(V, E)$. Ένα ταίριασμα M είναι ένα σύνολο ακμών που ανα δύο δεν έχουν κοινά άκρα, δηλαδή καμία κορυφή του γράφου δεν καλύπτεται από δύο ακμές. Ένα τέλειο ταίριασμα M' είναι ένα ταίριασμα το οπόιο καλύπτει όλες τις κορυφές του γράφου, δηλαδή για κάθε μία κορυφή υπάρχει μία και μόνο μία ακμή του M' που προσπίπτει σε αυτή.*

Ορισμός 2.2.4 *Έστω γράφος $G(V, E)$. Μία ακολουθία από κορυφές $u_1, u_2, ...u_n$ είναι κύκλος του γράφου αν $u_1 = u_2$ και $\forall i \geq 1 (u_i, u_{i+1}) \in E$.*

Ορισμός 2.2.5 *Έστω γράφος $G(V, E)$. Μία κυκλική κάλυψη (cycle cover) του G είναι ένα σύνολο από κύκλους του γράφου τέτοιο ώστε κάθε κορυφή να ανήκει σε έναν και μόνο κύκλο.*

Στην περίπτωση λοιπόν {0,1}-πίνακα το permanent ισούται με τον αριθμό των τέλειων ταιριασμάτων του διμερή γράφου G καθώς επίσης και με τον αριθμό των διαφορετικών cycle cover του κατευθυνόμενου γράφου G'. Αυτό μπορούμε να το καταλάβουμε καλύτερα αν σκεφτούμε ως εξής:

- Για το πρώτο αρκεί να σκεφτούμε πως η αντιστοίχιση $(i, \sigma(\iota))$ που ορίζεται από την κάθε μετάθεση σ αντιστοιχεί σε ένα τέλειο ταίριασμα ανν $\forall i, A(i, \sigma(i)) = 1$ ή ισοδύναμα $\forall i (i, \sigma(\iota)) \in E$. Για να προσθέρει όμως η μετάθεση σ κάτι στο ολικό άθροισμα θα πρέπει όλα τα A(ι,σ(ι)) που περιέχει να είναι διάφορα του μηδενός. Άρα μόνο οι μεταθέσεις που αντιστοιχούν σε τέλεια ταιριάσματα προσφέρουν στο συνολικό άθροισμα και μάλιστα κατά 1.

- Για το δεύτερο αρκεί να δούμε πως μία μετάθεση ορίζει ένα cycle cover ως εξής: Έχουμε το σύνολο

  $$\Sigma = \{(1, \sigma(1)), (\sigma(1), \sigma(\sigma(1))), (\sigma(\sigma(1)), \sigma(\sigma(\sigma(1)))), ...\}$$

  . Τότε το σύνολο $\Sigma \bigcap E$ - όπου E όπως ορίστηκε **??** - είναι ένα cycle cover.

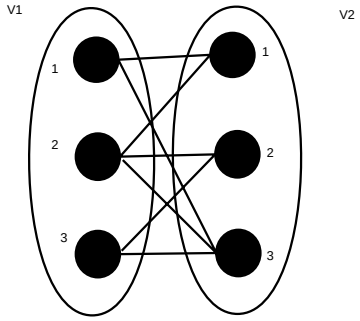
  Σημείωση: Αν πρόκειται για πίνακα με θετικά ορίσματα, όχι μόνο 0,1, τότε μπορούμε να ορίσουμε και την αξία ενός cycle cover ως το γινόμενο των βαρών των ακμών που συμμετέχουν σε αυτό. Σε αυτή την περίπτωση το permanent ισούται με το άθροισμα των αξιών των διαφορετικών cycle cover του γράφου.

Παράδειγμα 2.2.1 *Έστω ο πίνακας A :*

1	*0*	*1*
1	*1*	*1*
0	*1*	*1*

Ο υπολογισμός του permanent έχει : $\{1,2,3\} \longrightarrow A(1,1) * A(2,2) * A(3,3) = 1$
$\{1,3,2\} \longrightarrow A(1,1) * A(2,3) * A(3,2) = 1$
$\{2,1,3\} \longrightarrow A(1,2) * A(2,1) * A(3,3) = 0$
$\{2,3,1\} \longrightarrow A(1,2) * A(2,3) * A(3,1) = 0$
$\{3,2,1\} \longrightarrow A(1,3) * A(2,2) * A(3,1) = 0$
$\{3,1,2\} \longrightarrow A(1,3) * A(2,1) * A(3,2) = 1$
άρα $permA = 3$

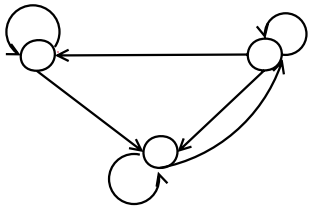
Τότε ο αντίστοιχος διμερής γράφος είναι:



και τα perfect matchings είναι :

$\{ (1,1),(2,2),(3,3) \}$
$\{ (1,1),(2,3),(3,2) \}$
$\{ (1,3),(3,2),(2,2) \}$

Ο αντίστοιχος κατευθυνόμενος :



ενώ τα cycle cover είναι :

$\{(1,1),(2,2),(3,3)\}$,
$\{(1,1),(2,3,2)\}$,
$\{(1,3,2,1)\}$

2.2.2 Permanent και #P

Όπως είπαμε και πριν, το permanent είναι ένα πρόβλημα που δεν έχει ακόμη επιλυθεί σε πολυωνύμικό χρόνο. Αυτό θέτει διάφορα ερωτηματικά για την πολυπλοκότητά του. Στην ενότητα αυτή θα δούμε ότι το permanent είναι complete για την κλάση #P.

Θεώρημα 2.2.1 *Το πρόβλημα του υπολογισμού του permanent ενός $n \times n$ 0,1-πίνακα A είναι $\#P$ - complete.*

Σημαντικό ρόλο στην πορεία της απόδειξης του παραπάνω θεωρήματος έχει το πρόβλημα #3SAT το οπόιο ορίζεται ως εξής :

Ορισμός 2.2.6 *Έστω φόρμουλα f , προτασιακής λογικής σε συζευκτική κανονική μορφή όπου σε κάθε clause έχουμε ακριβώς τρεις μεταβλητές(3CNF μορφή). Τότε το #3SAT(f) είναι το πρόβλημα της εύρεσης του αριθμού των διαφορετικών αναθέσεων τιμών που ικανοποιούν την f.*

Η πορεία που θα ακολουθήσουμε στην απόδειξη είναι η εξής:

1. Αρχικά θα δούμε ότι μπορούμε να ανάγουμε(κατά Karp) το πρόβλημα του υπολογισμού του πλήθους των μονοπατιών μιας TM που αποδέχονται το input, στο πλήθος των αναθέσεων τιμών που ικανοποιούν μια κατάλληλα κατασκευασμένη φόρμουλα f (#3SAT).

2. Στη συνέχεια θα αναγάγουμε (κατά Cook[1])το πρόβλήμα του #3SAT σε αυτό του Integer-permanent (δηλαδή το πρόβλημα του permanent για πίνακες ακεραίων)

3. Μετά θα αναγάγουμε (κατά Cook) το Integer-permanent στο (0,1)-permanent(mod N)

4. Και τέλος η αναγωγή (κατά Cook[1])του (0,1)-permanent(mod N) στο (0,1)-permanent είναι προφανής.

Από όλα τα παραπάνω προκύπτει ότι το (0,1)-permanent είναι #P-hard. Όμως έχουμε δει ότι το πρόβλημα αυτό ισοδυναμεί με την εύρεση του αριθμού των τέλειων ταιριασμάτων σε ένα διμερή γράφο και με δεδομένο ότι το πρόβλημα της εύρεσης ενός τέλειου ταιριάσματος είναι στο P, υπάρχει μη ντετερμινιστική TM της οποίας το πλήθος των μονοπατιών που αποδέχονται είναι ίσο με τον αριθμό των τέλειων ταιριασμάτων. Συνεπώς το permanent ανήκει στο #P. Έτσι προκύπτει ότι το permanent είναι #P-complete.

Ας δούμε όμως πιο αναλυτικά τα βήματα της παραπάνω απόδειξης.

Βήμα 1ο

Θεώρημα 2.2.2 *Υπάρχει μία συνάρτηση $g \in FP$ η οποία αντιστοιχεί μία οποιαδήποτε μη ντετερμινιστική TM M και μία είσοδο x για αυτή σε μία προτασιακή φόρμουλα f σε 3CNF μορφή έτσι ώστε ο αριθμός των αναθέσεων που ικανοποιούν την g(M,x) να ισούται με τον αριθμό των μονοπατιών της M που αποδέχονται το x.*

Απόδειξη: Προκύπτει από την αρχική αναγωγή του Cook (??????). Περισσότερες λεπτομέρειες υπάρχουν στο [Val].

□

Βήμα 2ο

Θεώρημα 2.2.3 *Υπάρχει μία συνάρτηση $f \in FP$ που αντιστοιχεί φόρμουλες σε 3CNF με m clauses σε πίνακες με ορίσματα -1,0,1,2,3 τέτοια ώστε*

$$\forall FPerm(f(F)) = 4^{5m} * s(F)$$

όπου s(F) είναι ο αριθμός των αναθέσεων που ικανοποιούν την F.

Απόδειξη: Η απόδειξη του θεωρήματος βασίζεται στην κατασκευή ενός κατάλληλου κατευθυνόμενου γράφου - **??** για αντιστοίχιση μεταξύ γράφου και πίνακα - με τέτοιο τρόπο ώστε κάθε cycle cover του γράφου να ορίζει μία ανάθεση τιμών για τις μεταβλητές της F. Προκειμένου να ισχύει η σχέση που ορίζει το θεώρημα πρέπει κάθε cycle cover που ορίζει μία ανάθεση που ικανοποιεί την F να έχει αξία ίση με 4^{5m} ενώ όλα τα υπόλοιπα cycle cover να αλληλοαναιρούνται. Για να το πετύχουμε αυτό κατασκευάζουμε κατάλληλα gadgets τα οποία αντιπροσωπεύουν συγκεκριμένα σημεία της F. // Έστω λοιπόν μία φόρμουλα $F = C_1 \bigwedge C_2 \bigwedge ..... \bigwedge C_m$ όπου κάθε clause είναι της μορφής $C_i = (y_{i1} \bigvee y_{i2} \bigvee y_{i3})$ με $y_{ij} \in \{x_1, \tilde{x_1}, x_2, \tilde{x_2}, ..., x_n, \tilde{x_n}$. Για κάθε μεταβλητή κατασκευάζουμε ένα gadget της μορφής 1 όπου οι μεγάλοι κόμβοι έχουν εσωτερική δομή και αποτελούν σήμεία ένωσης με τα gadgets που αφορούν τις clauses και από τη μία μεριά του gadget ενώνονται όλες οι clauses όπου η μεταβλητή εμφανίζεται κανονικά και από την άλλη όλες οι clauses όπου η μεταβλητή εμφανίζεται ως συμπλήρωμα. Έχοντας αυτή τη μορφή, κάθε cycle cover του ολικού γράφου θα πρέπει αναγκαστικά να περιέχει τη μία από τις δύο εξωτερικές πλευρές- αλλά όχι και τις δύο. Ανάλογα με το ποιά πλευρά περιέχει ορίζεται και το ποιά αληθοτιμή ορίζει για την κάθε μεταβλητή.// Για κάθε clause κατασκευάζουμε ένα gagdet της μορφής 2. Όπως και πριν οι μεγάλοι κόμβοι έχουν εσωτερική δομή. Τρεις από αυτούς αποτελούν τα σημεία ένωσης με τα gadgets που αντιστοιχούν στις μεταβλητές που εμφανίζονται στην clause ενώ οι υπόλοιποι δύο είναι απλές εσωτερικές συνδέσεις. Τα gadgets αυτά είναι έτσι κατασκευασμένα ώστε να μην γίνεται να ανήκουν ολόκληρα σε ένα cycle cover. Έπιπλέον αν κάποιο μέρος τους - μία ένωση - διασχιστεί μέσω του gadget που αντιστοιχεί στην μεταβλητή τότε υπάρχει μόνο ένας τρόπος να διασχιστεί το υπόλοιπο έτσι ώστε να προκύψει cycle cover που να ορίζει ανάθεση που ικανοποιεί την F.// Τέλος έχουμε την δομή των ενώσεων. Αυτή παρουσιάζεται στο σχήμα 3. Πρόκειται για γράφους 4 κόμβων και παρατηρούμε πως εδώ οι ακμές έχουν βάρη διαφορετικά της μονάδας σε αντίθεση με όλες τις προηγούμενες κατασκευές. Επίσης μπορούμε να εξάγουμε τα εξής συμπεράσματα για τον πίνακα X που περιγράφει αυτό το gadget :

1. $PermX = 0$

2. $PermX(1;1) = 0$

3. $PermX(4;4) = 0$

4. $PermX(1,4;1,4) = 0$

5. $PermX(1;4) = PermX(4;1) = 4$

Ορίζουμε ως πορεία στο γράφο $f(F)$ το σύνολο όλων των cycle cover τα οποία έχουν το ίδιο σύνολο ακμών εκτός των συνδέσεων. Μία πορεία χαρακτηρίζεται ως καλή όταν εισέρχεται σε όλες τις ενώσεις ακριβώς μία φορά και εξέρχεται από το αντίθετο άκρο. Από την ιδιότητα 5 μπορούμε να συμπεράνουμε ότι μία καλή πορεία έχει αξία ίση με 4^{5m} - γιατί το πλήθος των ενώσεων είναι ίσο με 5m και κάθε μία συμβάλλει κατά 4. Επίσης από τις υπόλοιπες ιδιότητες προκύπτει ότι όλες οι άλλες πορείες έχουν μηδενική αξία. Έπιπλέον αφού κάθε καλή πορεία αντιστοιχεί σε ένα συγκεκριμένο σύνολο ακμών εκτός των ενώσεων που αποτελεί cycle cover του εξωτερικού γράφου ορίζει και μία ανάθεση που ικανοποιεί την F.Έτσι προκύπτει το ζητούμενο αποτέλεσμα.

□

Βήμα 3ο

Έχοντας τελειώσει και με την παραπάνω μετατροπή έχουμε κατασκευάσει έναν πίνακα ακεραίων και έχουμε βρει τη σχέση που συνδέει το permanent αυτού με το πλήθος των αναθέσεων που ικανοποιούν μία φόρμουλα f. Αυτό που μας μένει να κάνουμε είναι να ανάγαγουμε τον υπολογισμό του permanent του πίνακα ακεραίων στον υπολογισμό του permnanet κάποιου(ων) (0,1)-πίνακα(ων). Αυτό θα γίνει σε δύο στάδια. Αρχικά για να απαλείψουμε τις ακμές με αρνητικό βάρος θα χρησιμοποιήσουμε το Κινέζικο Θεώρημα Υπολοίπων και πίνακες mod και μετά χρησιμοποιώντας το επόμενο θεώρημα για να απαλλαγούμε από τις ακμές με βάροι ¿ 1.

Θεώρημα 2.2.4 *Υπάρχει συνάρτηση h , υπολογίσιμη σε πολυωνυμικό χρόνο ως προς το μέγεθος του πίνακα και του n, η οποία αντιστοιχεί πίνακες με στοιχεία από το σύνολο {0,1,2,3,....,n} σε (0,1) πίνακες έτσι ώστε:*

$$\forall A Perm A = Perm h(A)$$

Απόδειξη: Για να κατασκευάσουμε τον h(A) αντικαθιστούμε στον A κάθε ακμή με βάρος k ¿ 1 με έναν υπογράφο (σχήμα.....για k = 2). Εάν η (x,y) δεν περιέχεται σε ένα cycle cover του A τότε υπάρχει μόνο ένας τρόπος να καλυφθούν οι επιπλέον κόμβοι του υπογράφου στον h(A). Εάν περιέχεται τότε υπάρχουν k τρόποι με τους οποίους μπορούν να καλυφθούν οι εναπομείναντες κόμβοι του h(A) - καθένας ορίζεται κατά μοναδικό τρόπο από την επιλογή χρήσης ενός self-loop.

□

Επίσης γνωρίζουμε το εξής θεώρημα - γνωστό ως Κινέζικο θεώρημα υπολοίπων :

Θεώρημα 2.2.5 *Έστω $n_1, n_2, ...n_k$ ακέραιοι οι οποίοι είναι ανά δύο πρώτοι μεταξύ τους. Τότε για οποιοδήποτε σύνολο ακεραίων $\{a_1, a_2, ..., a_k\}$ υπάρχει x τέτοιο ώστε να επαληθεύει το σύστημα :// $x = a_1 mod n_1 // x = a_2 mod n_2 // ..... // x = a_k mod n_k$ Επίσης, όλα τα x που ικανοποιούν το παραπάνω σύστημα είναι ισουπόλοιπα ως προς $N = n_1 * n_2 * ... * n_k$.*

Έχοντας λοιπόν έναν πίνακα A, $n \times n$, με στοιχεία κατά απόλυτη τιμή μικρότερη από m ισχύει ότι $|PermA| \leq m^n * n!$. Συνεπώς για να υπολογίσουμε το Perm A αρκεί - σύμφωνα με το προηγούμενο θεώρημα - να υπολογίσουμε το $(PermA) mod n_i = Perm(A mod n_i)$ για ένα κατάλληλο σύνολο από n_i (ανά δύο πρώτοι μεταξύ τους και με γινόμενο μεγαλύτερο από $2 * m^n * n!$ έτσι ώστε να είμαστε σίγουροι ότι ο αριθμός που βρήκαμε είναι ο σωστός και όχι απλά ισουπόλοιπος με τον ζητούμενο. Οι πίνακες $A mod n_i$ όμως έχουν στοιχεία στο σύνολο $\{0, 1, 2, ..n_i\}$ και σύμφωνα με το θεώρημα 2.2.4 μπορούν να μετατραπούν σε (0,1)-πίνακες με το ίδιο permanent.

2.3 Η σχέση του #P με την πολυωνυμική ιεραρχία PH

Το #P είναι μία κλάση της οποίας ο ορισμός όπως είδαμε βασίζεται στο πλήθος των μονοπατιών των TM που αποδέχονται. Ανήκει δηλαδή σε μία καινούρια κατηγορία κλάσεων, τις μετρητικές. Όπως θα δούμε σε επόμενη ενότητα μπορούμε να ορίσουμε ολόκληρη ιεραρχία μετρητικών κλάσεων. Αυτό που θα μας απασχολήσει όμως στην παρούσα ενότητα είναι η σχέση του #P με ένα μεγάλο μέρος των μη μετρητικών κλάσεων, που αντιπροσωπεύονται συνολικά από την πολυωνυμική ιεραχία(PH). Θέλουμε να δούμε αν το #P είναι υπολογιστικά δυνατότερο από την PH. Αυτό που θα αποδείξουμε λοιπόν είναι πως όλα τα προβλήματα της PH μπορούν να αναχθούν με Cook[1] στο #P. Δηλαδή ότι [Tod91] :

$$PH \leq^p_{T-1} \#P \iff PH \subseteq P^{\#P[1]}.$$

Η απόδειξη αυτή θα πραγματοποιηθεί σε δύο βήματα. Πριν όμως ξεκινήσουμε να δούμε καθένα από αυτά αναλυτικά θα ορίσουμε ένα κατάλληλο σύστημα τελεστών - για πιθανοτικές κλάσεις πολυπλοκότητας - που θα μας

χρειαστεί στη συνέχεια για να παρουσιάσουμε διάφορα ενδιάμεσα αποτελέσματα.

Ορισμοί

Έστω K μία κλάση από σύνολα, L ένα σύνολο και $\Sigma = (0,1)$ το αλβάβητο της γλώσσας μας - όλα τα στοιχεία των συνόλων ανήκουν στο Σ^*. Τότε :

Ορισμός 2.3.1 *$L \in \oplus \cdot K$ εάν υπάρχει ένα σύνολο $A \in K$ και ένα πολυώνυμο p τέτοιο ώστε για όλα τα $x \in \Sigma^*$,*

$$x \in L \Longleftrightarrow ||w \in \{0,1\}^{p(|x|)} : wx \in A||isodd.$$

Εάν το K είναι κλειστό ως προς την πράξη της σημαδεμένης ένωσης με σύνολα της μορφής $\{x0^{p(|x|} : x \in \Sigma*\}$ τότε το $\oplus K$ είναι κλειστό ως προς συμπλήρωμα.

Ορισμός 2.3.2 *$L \in BP \cdot K$ εάν υπάρχει ένα σύνολο $A \in K$,ένα πολυώνυμο p, και μία σταθερά ε ¿ 0 , τέτοια ώστε για όλα τα $x \in \Sigma*$,*

$$x \in L \Longleftrightarrow Prob\{w \in \{0,1\}^{p(|x|)} : wx \in A\} \geq 1/2 + \varepsilon$$

(two-sided bounded error).Εάν το σύνολο K είναι κλειστό ως προς συμπλήρωμα , τότε και το $BP \cdot K$ είναι κλειστό ως προς συμπλήρωμα.

Ορισμός 2.3.3 *$L \in R \cdot K$ εάν υπάρχει ένα σύνολο $A \in K$,ένα πολυώνυμο p, και μία σταθερά ε ¿ 0 , τέτοια ώστε για όλα τα $x \in \Sigma*$,*

$$x \in L \Longleftrightarrow Prob\{w \in \{0,1\} : wx \in A\} \geq 1/2 + \varepsilon$$

$$x \notin L \Longleftrightarrow Prob\{w \in \{0,1\}^{p(|x|)} : wxnot \in A\} = 1$$

.(one-sided bounded error) Δηλαδή υπάρχει NTM για το $R \cdot K$ τέτοια ώστε αν $x \in L$ τότε περισσότερα από τα μισά μονοπάτια αποδέχονται ενώ αν $x \notin L$ κανένα μονοπάτι δεν αποδέχεται.Εάν το σύνολο K είναι κλειστό ως προς συμπλήρωμα , τότε και το $R \cdot K$ είναι κλειστό ως προς συμπλήρωμα.

Ορισμός 2.3.4 *$L \in R \cdot K$ εάν υπάρχει ένα σύνολο $A \in K$ και ένα πολυώνυμο p τέτοια ώστε για όλα τα $x \in \Sigma*$,*

$$x \in L \Longleftrightarrow Prob\{w \in \{0,1\}^{p(|x|)} : wx \in A\} \geq 1/2$$

.(two-sided error).Εάν το σύνολο K είναι κλειστό ως προς συμπλήρωμα , τότε και το $C \cdot K$ είναι κλειστό ως προς συμπλήρωμα.

Στη συνέχεια την κλάση $C \cdot P$ θα την συμβολίζουμε με PP. Επίσης να σημειώσουμε ότι οι παραπάνω τελεστές ορίζουν στην ουσία πιθανοτικές αναγωγές δηλαδή αν $K1 \subseteq A \cdot K2$ όπου A ένας από τους τελεστές BP, C , R και K1, K2 σύνολα, τότε αυτό σημαίνει ότι το K1 ανάγεται στο K2 μέσω της αντίστοιχης αναγωγής δηλαδή μπορούμε να αποφασίσουμε για το K1 μέσω του K2 έχοντας όμως τις πιθανότητες λάθους που ορίζει ο αντίστοιχος τελεστής.

Βήμα 1ο

Το 1979 οι Valiant και Vazirani απέδειξαν ότι όλα τα σύνολα στο NP μπορούν να αναχθούν σε ένα σύνολο στο $\oplus P$ με πιθανοτική αναγωγή πολυωνυμικού χρόνου με one-sided bounded error(R). Στην ενότητα αυτή θα επεκτείνουμε το αποτέλεσμα αυτό και θα δούμε ότι όλα τα σύνολα της πολυωνυμικής ιεραρχίας (PH) μπορούν να αναχθούν σε ένα σύνολο στο $\oplus P$ με πιθανοτική αναγωγή πολυωνυμικού χρόνου με two-sided bounded error(BP)([Tod91]). Θα αποδείξουμε δηλαδή ότι :

$$PH \subseteq BP \cdot \oplus P$$

Προκειμένου να αποδείξουμε αυτό το αποτέλεσμα θα χρειαστούμε κάποια ενδιάμεσα αποτελέσματα - λήμματα. Πριν όμως τα δούμε αναλυτικά ας κάνουμε μία διαισθητική περιγραφή της πορείας μας. Αρχικά θα δούμε ότι το Σ_k^P περιέχεται στο $BP \cdot \oplus \cdot \Pi_{k-1}^P$. Στη συνέχεια θα δούμε ότι μπορούμε να εναλλάξουμε έναν $\oplus$ με έναν BP τελεστή. Δηλαδή : $\oplus \cdot BP \cdot \oplus P \subseteq BP \cdot \oplus \cdot \oplus P$. Μετά θα επισημάνουμε την δυνατότητα να μειώσουμε σε έναν δύο συνεχόμενους $\oplus$ ή BP τελεστές και στο τέλος θα τα βάλουμε όλα αυτά μαζί για να αποδείξουμε το ζητούμενο μέσω επαγωγής στα επίπεδα της πολυωνυμικής ιεραρχίας. Πάμε τώρα να δούμε αυτά τα λήμματα αναλυτικά.

Λήμμα 2.3.1 *Για κάθε* $k \geq 1, \Sigma_k^P \bigcup \Pi_k^P \subseteq BP \cdot \oplus \cdot \Pi_{k-1}^P$.

Ιδέα Απόδειξης: Σύμφωνα με τις ιδιότητες που έχουμε δει στους ορισμούς 2.3.2 και 2.3.1 το $BP \cdot \oplus \cdot \Pi_{k-1}^P$ είναι κλειστό ως προς συμπλήρωμα. Έτσι, με δεδομένο ότι $\Pi_k^P = co - \Sigma_k^P$ αρκεί να αποδείξουμε ότι $\Sigma_k^P \subseteq BP \cdot \oplus \cdot \Pi_{k-1}^P$. Έστω $L \in \Sigma_k^P$. Τότε σύμφωνα με τον ορισμό της πολυωνικής ιεραρχίας με βάσει τους ποσοδείκτες έχουμε [L.J77] $\exists A \in \Pi_{k-1}^P$ και πολυώνυμο p τέτοιο ώστε $\forall x, x \in L \iff \exists y \in \{0,1\}^{p(|x|)}, xy \in A$. Σκοπός μας πλέον είναι να ορίσουμε ένα κατάλληλο σύνολο C, το οποίο να ανήκει στο $\oplus \Pi_{k-1}^P$ με τέτοιο τρόπο ώστε να μπορούμε να αποφασίσουμε για το L χρησιμοποιώντας το C μέσω μιας πιθανοτικής διαδικασίας με two-sided bounded error probability(BP). Για να μπορέσουμε να εξάγουμε πιθανότητες χρησιμοποιούμε ένα θεώρημα που αποδείχθηκε στο [LV86] και το οποίο λέει πως αν έχουμε ένα σύνολο S από strings μήκους n και επιλέξουμε τυχαία $\{w_1, w_2, .., w_n\}$ strings από τον

χώρο $\{0,1\}^n$ τότε η πιθανότητα να υπάρχει i τω το πλήθος των γραμμικώς ανεξάρτητων διανυσμάτων του S ως προς τη βάση $\{w_1, w_2, ...w_i\}$ - γινόμενο μηδέν με όλα τα διανύσματα της βάσης - να είναι 1 είναι μεγαλύτερη του 1/4.Φτιάχνουμε λοιπόν το C μέ τέτοιο τρόπο ώστε να περιέχει για κάθε x όλους του δυνατούς συνδυασμούς πολυωνυμικών βάσεων - και ως προς το μέγεθος κάθε διανύσματος της βάσης αλλά και ως προς το πλήθος αυτών - τέτοιες ώστε σε κάποιο επίπεδο τους (π.χ εώς το i διάνυσμα) το πλήθος των γραμμικών ανεξάρτητων μαρτύρων του x για το L να είναι περιττό. Εάν το x ανήκει στο L, τότε υπάρχει τουλάχιστον ένα y που είναι μάρτυρας ως προς το A. Αν ταυτίσουμε το σύνολο των μαρτύρων y με το S του θεωρήματος προκύπτει ότι αν επιλέξουμε τυχαία μια βάση η πιθανότητα να πληρεί τις προυποθέσεις του C είναι μεγαλύτερη του 1/4. Ενω αν το χ δεν ανήκει στο L τότε δεν υπάρχει καμία βάση για την οποία το x να ανήκει στο C.Άρα έχουμε ότι :

$$x \in L \Longleftrightarrow Prob(\{u \in \{\}^{p(|x|)^2} : xu \in C\}) \geq 1/4$$

$$x \notin L \Longleftrightarrow Prob(\{u \in \{0,1\}^{p(|x|)^2} : xu \in C\}) = 0$$

Με λίγη περεταίρω επεξεργασία για την αλλαγή του ορίου της πιθανότητας (δες [Tod91]) προκύπτει το ζητούμενο.

□

Λήμμα 2.3.2 $\oplus P^{\oplus P} = \oplus P$ *.Ετσι προκύπτει ότι* $\oplus \cdot \oplus P = \oplus P$.

Απόδειξη: [C.H83]

□

Λήμμα 2.3.3 $\oplus \cdot BP \cdot \oplus P \subseteq BP \cdot \oplus \cdot \oplus P$

Ιδέα Απόδειξης: 'Εστω L $\in \oplus \cdot BP \cdot \oplus P$.Προκειμένου να μπορέσουμε να εναλλάξουμε την σειρά των τελεστών BP και $\oplus$ χρησιμοποιούμε τους ορισμούς που δώσαμε πιο πάνω για να 'μεταφράσουμε' τι σημαίνει $x \in L$. Χρησιμοποιούμε σε αυτή τη διαδικασία δύο σύνολα ,$A \in BP \cdot \oplus P$ και $B \in \oplus P$. Στη συνέχεια χρησιμοποιούμε ένα από τα amplifying λήμματα που έχει αποδείξει ο Schöning [U.S89] και μας επιτρέπει να φράξουμε την πιθανότητα στο σύνολο A πολυωνυμικά ως προς το μήκος του string x καθώς και να εισάγουμε τον καθολικό ποσοδείκτη στο εσωτερικό της πιθανότητας. Μετά αρκεί να ορίσουμε δύο νέα σύνολα A' και B' προκειμένου να καταφέρουμε την αντιμετάθεση των δύο τελευταίων string που έχουν προκύψει στον ορισμό και άρα την αντιμετάθεση των τελεστών . Η πλήρης απόδειξη βρίσκεται στο [Tod91].

□

Λήμμα 2.3.4 $BP \cdot BP \cdot \oplus P = BP \cdot \oplus P$

Ιδέα Απόδειξης: Όπως και παραπάνω χρησιμοποούμε τους ορισμούς και το λήμμα που αναφέραμε για να αναπτύξουμε τους ορισμούς και στη συνέχεια επιχειρούμε την ένωση των δύο strings που αφορούν τα δύο BP επίπεδα του ορισμού μας δημιουργώντας ένα νέο σύνολο C και υπολογίζουμε τις πιθανότητες σε σχέση με το C για x ∈ L και x $\notin L$.

□

Και πλέον μπορούμε να δούμε το βασικό θεώρημα :

Θεώρημα 2.3.1 $PH \subseteq BP \cdot \oplus P$

Απόδειξη: Όπως είπαμε και παραπάνω το θεώρημα αποδεικνύεται με επαγωγή. Έχουμε :

1. Για $\kappa = 0$ έχουμε : $\Sigma_0^P = P \subseteq BP \cdot \oplus P$ που είναι προφανές
2. Έστω ότι ισχύει για κάποιο k, δηλαδή $\Sigma_k^P \subseteq BP \cdot \oplus P$. Επειδή $BP \cdot \oplus P$ είναι κλειστό ως προς συμπλήρωμα ισχύει ότι $\Pi_k^P \subseteq BP \cdot \oplus P$. από λήμμα 2.3.1 έχουμε όμως :

$$\Sigma_{k+1}^P \subseteq BP \cdot \oplus \cdot \Pi_k^P // \subseteq BP \cdot \oplus \cdot BP \cdot \oplus P$$

από επαγωγική υπόθεση

$$\subseteq BP \cdot BP \cdot \oplus \oplus P$$

από λήμμα 2.3.3

$$= BP \cdot \oplus P$$

από λήμμα 2.3.4

□

Βήμα 2ο

Αυτό που μας έχει μείνει να αποδείξουμε προκειμένου να έχουμε το ζητούμενο αποτέλεσμα είναι:

$$C \cdot \oplus P \subseteq P^{\#P[1]}$$

Απαραίτητο για την απόδειξη αυτής της σχέσης είναι το παρακάτω λήμμα :

Λήμμα 2.3.5 *Έστω X συνολο στο $\oplus P$ και πολυώνυμο q. Υπάρχει NTM N1 τέτοια ώστε για κάθε y μήκους n :*

1. *Εάν* $y \in X$ *τότε* $\#acc_{N1}(y) = 0(mod 2^{q(n)})$

2. *Εάν* $y \notin X$ *τότε* $\#acc_{N1}(y) = -1(mod 2^{q(n)})$

Ιδέα Απόδειξης: Το παραπάνω λήμμα βασίζεται σε ένα αντίστοιχο που υπάρχει για τους ακέραιους αριθμούς : έχοντας έναν αρχικό αριθμό m ορίζουμε την ακολουθία $s_i = 3 * s_{i-1}^4 + 4 * s_{i-1}^3$. Μπορεί εύκολα να αποδειχθεί ότι εάν το m είναι άρτιο τότε $\forall i, \exists k : s_i = k * 2^{2^i}$ ενώ αν το m είναι περιττό τότε ισχύει το ίδιο για το $s_i + 1$. Χρησιμοποιούμε αυτή την ιδιότητα για να ορίσουμε αναδρομικά μία συνάρτηση f πάνω στις NTM και τις εισόδους αυτών,τέτοια ώστε αν $\#acc_N(y)$ είναι άρτιο τότε $f_N(y, \lceil logq(n) \rceil) = 0(mod 2^{q(n)})$ ενώ αν $\#acc_N(y)$ είναι περιττό τότε $f_N(y, \lceil logq(n) \rceil) = -1(mod 2^{q(n)})$. Συνεπώς το μόνο που μένει να αποδείξουμε είναι ότι ότι μπορεί να κατασκευαστεί μια NTM Q με $\#acc_Q(y) f_N(y, \lceil logq(n) \rceil)$. Η λειτουργία της μηχανής αυτής ορίζεται με βάσει τη συνάρτηση f και περισσότερες λεπτομέρειες μπορούν να βρεθούν στο [Tod91].

□

Μετά από αυτό το λήμμα είμαστε σε θέση να δούμε το βασικό θεώρημα αυτού του βήματος καθώς και την απόδειξή του.

Θεώρημα 2.3.2 $C \cdot \oplus P \subseteq P^{\#P[1]}$

Απόδειξη: Έστω $L \in \oplus P$. Τότε υπάρχει σύνολο X $\in \oplus P$ τέτοιο ώστε για όλα τα x, θέτοντας $W_x = \{w \in \{0,1\}^{p(|x|)} : xw \in X\}$, έχουμε $x \in L \iff ||W_x|| > 2^{p(|x|)-1}$. Τότε σύμφωνα με το παραπάνω λήμμα υπάρχει NTM N τέτοια ώστε για όλα τα y , με μήκος m έχουμε:

1. Εάν $y \in X$ τότε υπάρχει ακέραιος a ¿ 0 τέτοιος ώστε : $\#acc_N(y) = 2^m * a - 1$

2. Εάν $y \notin X$ τότε υπάρχει ακέραιος b ¿ 0 τέτοιος ώστε : $\#acc_N(y) = 2^m * b$

Ορίζουμε μία καινούρια NTM Z τέτοια ώστε :

1. Μαντεύει ένα w $\in \{0,1\}^{p(|x|)}$.

2. Τρέχει την N για xw και αποδέχεται αν και μόνο αν αποδέχεται η N.

Η Z τρέχει σε πολυωνυμικό χρόνο και αν ορίσουμε ως $\bar{W}_x = \{0,1\}^{p(|x|)} - W_x$ έχουμε :

$$\#acc_Z(x) = \sum_{w \in W_x} \#acc_N(xw) + \sum_{w \in \bar{W}_x} \#acc_N(xw) = ... = 2^{|x|+1+p|x|} * (\sum_{w \in W_x} a_{xw} + \sum_{w \in \bar{W}_x} b_{xw}) - ||W_x||$$

.
Αφού τα a_{xw}, b_{xw} είναι ακέραιοι έχουμε ότι το $\#acc_Z(x) + ||W_x||$ είναι πολλαπλάσιο του $2^{|x|+1+p(|x|)}$. Όμως $||W_x|| \leq 2^{p(|x|)}$ άρα το $||W_x||$ μπορεί να υπολογιστεί απλά συμπληρώντας ως προς 2 τα τελευταία $p(|x|)$ bits του $\#acc_Z(x)$.

□

Μάλιστα μπορούμε - με λιγο κόπο παραπάνω - να αποδείξουμε και ένα ακόμη πιο ισχυρό αποτέλεσμα :

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

. Το αποτέλεσμα αυτό θα μας χρειαστεί στην επόμενη ενότητα οπότε ας αφιερώσουμε λίγο χρόνο ακόμη για να δούμε ένα σκελέτο της πορείας απόδειξής του. Έχουμε ότι :

$$PP^{PH} \subseteq PP^{BP\cdot\oplus P} \subseteq PP^{BPP^{\oplus P}}$$

. Η πρώτη σχέση υποσυνόλου οφείλεται στο προηγούμενο θεώρημα και η δεύτερη προκύπτει από τον ορισμό του BP.Επίσης έχει αποδειχθεί ότι $PP^{BP^{\oplus P}} = PP^A$ [J.K89] για κάθε μαντείο A. Χρησιμοποιώντας τη σχέση αυτή στις παραπάνω σχέσεις έχουμε ότι $PP^{PH} \subseteq PP^{\oplus P}$. Όμως το $PP^{\oplus P}$ είναι στην ουσία το σύνολο $C \cdot \oplus P$ που προηγουμένως αποδείξαμε ότι είναι υποσύνολο του $P^{\#P[1]}$. Συνεπώς προκύπτει το ζητούμενο.

2.4 Η σχέση του #PH με την ιεραρχία μετρητικών κλάσεων - #PH

Στην προηγούμενη ενότητα συγκρίναμε το #P με την PH και αποδείξαμε ότι η PH μπορεί να αναχθεί κατά Cook[1] στο #P. Ενδιαφέρον θα είχε τώρα να δούμε τι σχέση έχει το #P με την πολυωνυμική ιεραρχία συναρτήσεων (FPH) καθώς και με την πολυωνυμική ιεραρχία μετρητικών κλάσεων (#PH). Πριν προχωρήσουμε όμως σε αυτό πρέπει να δούμε τον ακριβή ορισμό των παραπάνω κλάσεων.

Ορισμός 2.4.1 *Ορίζουμε ως FP^A το σύνολο των συναρτήσεων που μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο με NTM με μαντείο A. Η FPH είναι:*

$$PFH = \bigcup_{k\geq 0} PF^{\Sigma_k^P}.$$

Ορισμός 2.4.2 *Ορίζουμε ως $\#P^A$ το σύνολο των συναρτήσεων που μετρούν το πλήθος των μονοπατιών που αποδέχονται σε μη ντετερμινιστικές TM,πολυωνυμικού χρόνου, με μαντείο το A. Η #PH είναι :*

$$\#PH = \bigcup_{k\geq 0} \#P^{\Sigma_k^P}$$

Πριν προχωρήσουμε στα αποτελέσματα αυτής της ενότητας θα πρέπει να προσέξουμε λίγο τη σχέση μεταξύ της κλάσης #P και PP. Είναι προφανές πως κάθε σύνολο $L \in PP$ μπορεί να αναχθεί κατά Cook[1] σε μία συνάρτηση του #P- για να αποφασίσουμε αν $x \in L$ αρκεί να ρωτήσουμε το μαντείο για την τιμή της συνάρτησης που αντιστοιχεί στην NTM που αποφασίζει για το $xw\mu ew \in \{0,1\}^{p(|x|)}$. Αν είναι μεγαλύτερη από $2^{p(|x|)-1}$ τότε αποδεχόμαστε, διαφορετικά απορρίπτουμε. Από την άλλη , αποδείχθηκε το 1977 ότι μπορύμε να ανάγουμε και κάθε συνάρτηση του #P στο PP μέσω μιας διαδικασίας δυαδικής αναζήτησης πάνω στο γράφο της συνάρτησης. [J.S77]. Συνεπώς τα #P και PP είναι Cook-ισοδύναμα.
Με βάσει αυτή την παρατήρηση μπορούμε να δούμε ότι οι κλάσεις #PH και PP^{PH} είναι Cook-ισοδύναμες. Συνεπώς, από τα αποτελέσματα της προηγούεμης ενότητας, προκύπτει ότι η $\#PH \subseteq P^{\#P}$. (αφού $PP^{PH} \subseteq P^{\#P[1]}$). Παρατηρούμε ότι μιλάμε πια για Cook-αναγωγή και όχι Cook[1]. Αυτό έγινε γιατί υπάρχει το ενδιάμεσο βήμα μετάβασης στο σύνολο PP^{PH} το οποίο εισάγει επιπλέον ερωτήσεις στο μαντείο. Όμως, το αν μπορούμε να πραγματοποιήσουμε την παραπάνω αναγωγή με μία μόνο ερώτηση στο μαντείο είναι και το θέμα της υπόλοιπης ενότητας. Ο λόγος που μας ενδιαφέρει είναι γιατί γνωρίζουμε ότι η #PH δεν ανάγεται κατά Karp στο #P - αυτό προκύπτει από το γεγονός ότι $\#P \neq \#P^{NP}$ όπως αποδείχθηκε στο [J.K89]. Έτσι προκύπτει το ερώτημα του πόσο ισχυρή - με την έννοια των μέσων που παρέχει - πρέπει να είναι η αναγωγή προκειμένου να μπορούμε να ανάγουμε όλη την #PH στο #P. Το επόμενο θεώρηαμ απαντά σε αυτό το ερώτημα.

Θεώρημα 2.4.1 *Κάθε συνάρτηση στο #PH μπορεί να αναχθεί κατά Cook-[1] σε μία συνάρτηση στο #P. Δηλαδή :*

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

Προκειμένου να αποδειχθεί το θεώρημα αυτό χρειάζεται να ορίσουμε - με τελεστή- την έννοια του μετρήματος. Έτσι έχουμε :

Ορισμός 2.4.3 *Έστω σύνολο K. Τότε το $NUM \cdot K$ είναι το σύνολο των συναρτήσεων f για τις οποίες υπάρχει σύνολο $L \in K$ και πολυώνυμο p τέτοιο ώστε*

$$\forall x \in \Sigma*, f(x) = ||\{w \in \Sigma^{p(|x|)} : xw \in L\}||$$

Εύκολα μπορεί να αποδειχθεί ότι $\#PH = NUM \cdot PH$.Μπορούμε πλέον να δούμε την βασική πορέια της απόδειξης του παραπάνω θεωρήματος.
Ιδέα Απόδειξης: [ST92]. Αρχικά αντικαθιστούμε την PH με την κλάση $BP \cdot \oplus P$, αφού από την προηγούμενη ενότητα γνωρίζουμε ότι την περικλείει.Στη συνέχεια,αναπτύσσουμε τα σύνολα με χρήση των ορισμών των τελεστών, εώς το επίπεδο ενός συνόλου Λ3 (στο P) και στη συνέχεια ορίζουμε μία NTM η οποία μαντεύει πιθανά strings - ένα για κάθε επίπεδο/τελεστη - και ελέγχει εάν το συνολικό αποτελέσμα ανήκει ή όχι στο σύνολο L3. Μετά, με κατάλληλες πράξεις αλλά και επιμέρους λήμματα αποδεικνύεται ότι κάθε συνάρτηση f (#PH) μπορεί να υπολογιστεί μέσω του αριθμού των μονοπατιών που αποδέχεται η M ($\#acc_M(x)) \in \#P$.

□

Από το παραπάνω θεώρημα προκύπτουν - σχετικά άμεσα - κάποια σημαντικά συμπεράσματα.

1. Αρχικά μπορούμε να διαπιστώσουμε ότι και η FPH μπορεί να αναχθεί κατα Cook[1] στο #P ($FPH \subseteq FP^{\P[1]}$). Για να το αποδείξουμε αυτό αρκεί να δείξουμε ότι κάθε συνάρτηση f στο FPH μπορεί να αναχθεί κατά Cook[1] σε μια συνάρτηση g του #PH. Άρκεί λοιπόν να κατασκευάσουμε μία NTM M με μαντείο τέτοια ώστε για κάθε x,το πλήθος των μονοπατιών που αποδέχονται- g(x) - να σχετίζεται με άμεσο τρόπο με το f(x). Αυτό μπορεί να γίνει εύκολα αν θεωρήσουμε ότι η M είναι η NTM που λειτουργεί ως εξής: αρχικά υπολογίζει σε πολυωνυμικό χρόνο - $p(|x|)$ - την τιμή της f χρησιμοποιώντας το κατάλληλο μαντείο (ανάλογα με το επίπεδο της ιεραρχίας στο οποίο ανήκει η f) και στη συνέχεια μαντεύει έναν αριθμό k $1 \preceq k \preceq 2^{p(|x|+1}$. Εάν το $k \preceq 2^{p(|x|} + f(x)$ αποδέχεται , διαφορετικά απορρίπτει το x. Τότε το $f(x) = g(x) - 2^{p(|x|}$ και άρα η f μπορεί να αναχθεί στη g η οποία ανήκει στην #PH.

2. Εάν το $FP^{\P[1]}$ είναι υποσύνολο του $\#P^{\Sigma_k^P}$ για κάποιο k , τότε η PH καταρρέει στο επίπεδο k + $1(PH = \Sigma_{k+1}^P)$.Αυτό μπορούμε να το δούμε έυκολα αν αντιμετωπίσουμε κάθε σύνολο της PH μέσω της χαρακτηριστικής του συνάρτησης(χ). Οι συναρτήσεις αυτές ανήκουν προφανώς στην FPH και σύμφωνα με το 1 αλλά και την υπόθεση μας ανήκουν στο $\#P^{\Sigma_k^P}$.Άρα υπάρχει NTM M και μαντείο $A \in \Sigma_k^P$ τετοια ώστε να συμπίπτουν η τιμή της συνάρτησης χ με το πλήθος των μονοπατιών που αποδέχονται. Επειδή όμως η χ παίρνει μόνο τις τιμές 0,1 , στην ουσία μας ενδιαφέρει αν υπάρχει μονοπάτι στην M^A που να αποδέχεται.Αυτό συνεπάγεται ότι $PH = \Sigma_{k+1}^P$

3. Εάν κάθε συνάρτηση του #P ανάγεται κατά Cook σε μία συνάρτηση του $PF^{\Sigma_k^P}$ τότε $PH = \Delta_{k+1}^P = P^{\#P}$. Αυτό προκύπτει επειδή : $FP^{\Sigma_k^P} \subseteq FPH \subseteq FP^{\#P} \subseteq FP\Sigma_k^P$ το οποίο συνεπάγεται ότι $PH = \Delta_{k+1}^P = P^{\#P}$.

4. Εάν είτε $\#P \subseteq FPH$, είτε $FPH \subseteq \#P$ τότε η PH καταρρέει σε ένα πεπερασμένο επίπεδο.Αυτό σημαίνει πως τα δύο σύνολα, δηλαδή η πολυωνυμική ιεραρχία των συναρτήσεων και το σύνολο των συναρτήσεων που μετράνε το πλήθος των μονοπατιών που αποδέχονται σε μία NTM δεν μπορούν να συγκριθούν εκτός και αν η PH καταρρέει.

Αναλυτικές αροδείξεις των παραπάνω καθώς και επιπλέον συμπεράσματα μπορούν να βρεθούν στο [ST92].

Κεφάλαιο 3

Προσεγγισιμότητα της μετρητικής κλάσης #P

Όπως είδαμε στο προηγούμενο κεφάλαιο η πολυπλοκότητα της κλάσης #P μοιάζει να είναι πολύ υψηλή - μάλλον δεν περιέχεται σε κανένα επίπεδο της πολυωνυμικής ιεραρχίας. Συνεπώς οι αλγόριθμοι που επιλύουν ακριβώς τα προβλήματα αυτής της κλάσης είναι μη αποδοτικοί- όχι πολυωνυμικοί. Προκειμένου όμως να μπορέσουμε να επιλύσουμε αποδοτικά αυτά τα προβλήματα θα χαλαρώσουμε λίγο τις απαιτήσεις μας ως προς τα αποτελέσματα των αλγορίθμων. Δηλαδή, δεν θα απαιτούμε πλέον ο αλγόριθμος να μας δίνει την ακριβώς σωστή τιμή αλλά μια καλή προσέγγιση αυτής. Και παλι όμως το πρόβλημα θα παραμείνει πάνω από το P. Έτσι θα χαλαρώσουμε κι άλλο τις απαιτήσεις μας και θα επεκτείνουμε τη μελέτη μας και στους πιθανοτικούς αλγόριθμους, τους αλγόριθμους δηλαδή που δίνουν ώς αποτέλεσμα μια καλή προσέγγιση της λύσης ενός προβλήματος με μεγάλη πιθανότητα.

3.1 Ορισμός της έννοιας του προσεγγιστικού αλγόριθμου

Ορισμός 3.1.1 *Έστω δύο συναρτήσεις* $f, g : \{0,1\} * -> \aleph$ *και συνάρτηση* $\varepsilon \aleph -> \Re$. *Λέμε ότι η* g *ε-προσεγγίζει την* f *εάν για κάθε* $x \in \{0,1\}*$ *ισχύει :*

$$e^{-\varepsilon(n)} \cdot f(x) \leq g(x) \leq e^{\varepsilon(n)} \cdot f(x)$$

όπου n *είναι το μήκος του* x. *Ο παράγοντας προσέγγισης σε αυτή την περίπτωση είναι* $\varepsilon(n)$.

Προσθέτοντας επιπλέον περιορισμούς για το χρόνο υπολογισμού της g μπορούμε να ορίσουμε επιμέρους κλάσεις προσεγγιστικών αλγορίθμων.

Ορισμός 3.1.2 *Εάν το ε είναι σταθερό και η g υπολογίζεται σε πολυωνυμικό χρόνο ως προς το μήκος του x - δηλαδή το n - τότε λέμε ότι η g αποτελεί ένα πολυωνυμικού χρόνου προσεγγιστικό σχήμα για την f. (PTAS)*

Ορισμός 3.1.3 *Εάν επιπλέον η g υπολογίζεται σε πολυωνυμικό χρόνο και ως προς τον αντίστροφο του παράγοντα προσέγγισης ($poly(n, \varepsilon^{-1})$τότε λέμε ότι η g αποτελεί ένα πλήρους πολυωνυμικού χρόνου προσεγγιστικό σχήμα για την f. (FPTAS)*

3.2 Πολυπλοκότητα της εύρεσης προσεγγιστικού αλγόριθμου για τα προβλήματα της κλάσης #P

Όπως απέδειξε ο Stockmeyer το 1985 - [Sto85] - το πρόβλημα της εύρεσης προσεγγιστικού αλγορίθμου για ένα οποιοδήποτε πρόβλημα της κλάσης #P ανήκει στην πολυωνυμική ιεραρχία και μάλιστα στο Δ_3^p όπου σύμφωνα με τον συμβολισμό της πολυωνυμικής ιεραρχίας είναι το σύνολο $P^{\Sigma_2^p}$ με $\Sigma_2^p = NP^{NP}$.

Συγκεκριμένα απέδειξε ότι :

Θεώρημα 3.2.1 *Έστω $f \in \#P$ και ε, d θετικές σταθερές. Τότε υπάρχει $g \in \Delta_3^p$ τέτοια ώστε η g να προσεγγίζει την f με παράγοντα $(1+\varepsilon n^{-d})$ όπου n το μήκος του input.*

Η απόδειξη αυτού του θεωρήματος βασίζεται στην τεχνική της απεικόνισης ενός συνόλου αγνώστου μεγέθους σε ένα σύνολο με γνωστό πληθάριθμο.Πιο αναλυτικά έχουμε :

Απόδειξη:

Έστω M η NTM που έχει f(x) μονοπάτια που αποδέχονται - για κάθε input x- και έστω p(—x—) το πολυώνυμο που φράσσει το πλήθος των βημάτων υπολογισμού κάθε μονοπατιού. Έστω n = —x— και t = p(n). Ορίζουμε το εξής κατηγόρημα :

$Hash(x, m) \Leftrightarrow \exists m \times t(0,1) - \pi\nu\alpha\kappa\varepsilon\varsigma H_1, ..., H_m \tau\tau o\iota o\iota\sigma\tau\varepsilon \forall z \in Acc_M(x) \exists i \tau\tau o\iota o\sigma\tau\varepsilon H_i z \neq H(i)z' \forall z' \in Acc_M(x) - z.$

Δηλαδή το κατηγόρημα Hash(x,m) αληθεύει αν υπάρχουν m πίνακες μεγέθους $m \times t$ τέτοιοι ώστε για κάθε μονοπάτι της μηχανής που αποδέχεται να υπάρχει τουλάχιστον ένας που πολλαπλασιαζόμενος με αυτό δίνει διαφορετικό αποτέλεσμα σε σχέση με όλα τα άλλα μονοπάτια. Υπάρχει δηλαδή ένας πίνακας που μπορεί να 'ξεχωρίσει' το μονοπατι αυτό από όλα τα υπόλοιπα αντιστοιχίζοντάς το σε ένα διάνυσμα. Η σημαντική ιδιότητα που έχει αυτό το κατηγόρημα

αποδείχθηκε από τον Sipser και είναι η εξής :

$$\exists \sigma \tau \alpha \theta \varepsilon \rho c : |Acc_M(x)| \leq 2^{m-c} \Rightarrow Hash(x,m)$$

Από την άλλη, αν το Hash(x,m) αληθεύει τότε κάθε μονοπάτι $z \in Acc_M(x)$ μπορεί να αντιστοιχιστεί σε ένα ζευγάρι $(i, H_i z)$ με $1 \leq i \leq m \kappa \alpha \iota H_i z \in \{0,1\}^m$. Συνεπώς :

$$Hash(x,m) \Rightarrow |Acc_M(x)| \leq m2^m$$

Μία ντετερμινιστική μηχανή πολυωνυμικού χρόνου με ένα μαντείο για το Hash(x,m) μπορεί να βρει το ελάχιστο m για το οποίο ισχύει το κατηγόρημα.Εάν το m είναι ελάχιστο τότε από τις παραπάνω σχέσεις για το $|Acc_M(x)|$ προκύπτει ότι :

$$2^{m-c-1} \leq |Acc_M(x)| \leq m2^m$$

Άρα έχουμε υπολογίσει το $|Acc_M(x)|$ με παράγοντα προσσέγγισης $m2^{c+1}$ Προκειμένου να επιτύχουμε τον μικρότερο παράγοντα $(1 + \varepsilon n^{-d})$ αρκεί μόνο να δημιουργήσουμε μία μηχανή R τέτοια ώστε :

$$|Acc_R(x)| = (|Acc_M(x)|)^k$$

Εφαρμόζοντας την παραπάνω διαδικασία στην R μπορούμε να υπολογίσουμε το $|Acc_M(x)|$ με παράγοντα $(m2^{c+1})^{1/k}$. Επιλέγοντας κατάλληλα το k μπορεί να προκύψει το ζητούμενο. Επίσης πρέπει να παρατηρήσουμε ότι το Hash(x,m) ανήκει στο Σ_2^p - αφού το τελευταίο 'υπάρχει' στον ορισμό του πρόκειται για μία αναζήτηση σε χώρο πεπερασμένης,πολυωνυμικής διάστασης ως προς το n οπότε μπορεί να αντικατασταθεί από μία ντετερμινιστική αναζήτηση πολυωνυμικού χρόνου.Αν αυτό αφαιρεθεί μετά μένει μία καθαρή μορφή $\exists\forall$. Έτσι ολοκληρώσαμε την απόδειξη.

□

Τα ζητήματα που προκύπτουν τώρα είναι δύο. Πρώτον, κατά πόσο η παραπάνω πρόταση ισχύει και στην περίπτωση που επιτρέψουμε την χρήση μαντείων κατά τον υπολογισμό των συναρτήσεων του #P (κλάσεις $\#P^A$). Και δεύτερον, υπάρχει περίπτωση να μπορούμε να λύσουμε το πρόβλημα και σε χαμηλότερο επίπεδο της πολυωνυμικής ιεραρχίας-δηλαδη λύση σε πολυωνυμικό χρόνο αλλά με μαντείο χαμηλότερης πολυπλοκότητας ; Η απάντηση στο πρώτο ερώτημα είναι θετική, δηλαδή μπορούμε να προσεγγίσουμε κάθε συνάρτηση του $\#P^A$ με μία συνάρτηση στο $\Delta_3^{p,A}$. Αποδείχθηκε από τον Stockmeyer το 1985 και η πορεία της απόδειξης είναι παρόμοια με την παραπάνω. Όσο αφορά το δεύτερο οριστική απάντηση δεν έχει δοθεί αλλά έχει αποδειχθεί ότι

ακόμη και αν ισχύει κάτι τέτοιο, δηλαδή μπορούμε να προσεγγίσουμε το #P με συναρτήσεις στο Δ_2^p τότε υπάρχει σύνολο A και συνάρτηση που ανήκει στο $\#P^A$ τέτοια ώστε καμία συνάρτηση στο Δ_2^p να μην μπορεί να την προσεγγίσει. Με δεδομένο ότι η μεταφορά από την περίπτωση χωρίς μαντείο στην περίπτωση με μαντείο απαιτεί απλές επεκτάσεις καταλαβαίνουμε ότι ακόμη και αν το πρόβλημα της προσσέγγισης του #P έχει λύση στο Δ_2^p πρόκειται για μία 'περίεργη' λύση που μάλλον δεν θα εξυπηρετεί τους σκοπούς μας....

3.3 Ορισμός πιθανοτικών αλγορίθμων και AP-αναγωγών

Όπως είδαμε και παραπάνω η εύρεση προσεγγιστικών λύσεων για τις συναρτήσεις του #P δεν είναι εύκολη στην γενική περίπτωση - δεν υπάρχουν απαραίτητα για όλες τις συναρτήσεις στο P που να τις προσεγγίζουν. Έτσι θα προσπαθήσουμε να επεκτείνουμε την έννοια της προσσέγγισης, εισάγοντας και την έννοια της τυχαιότητας στους ορισμούς μας. Στον προηγούμενο ορισμο, χρησιμοποιήσαμε μόνο συναρτήσεις. Εδώ, επειδή κατά την διάρκεια του υπολογισμού πρέπει να υπάρχει η δυνατότητα τυχαίων επιλογών, θα χρησιμοποιήσουμε την έννοια της NTM. Το ίδιο μπορούσαμε να είχαμε κάνει και πριν μόνο που εκεί θα μιλούσαμε για μία ντετερμινιστική μηχανή (αντί της g).

Ορισμός 3.3.1 *Έστω μία συνάρτηση* $f : \{0,1\}* -> \aleph$ *και NTM M η οιποία δέχεται ως είσοδο ένα ζευγάρι* $(x, \varepsilon) \in \{0,1\} * \times (0,1)$. *Λέμε ότι η M είναι ένα πιθανοτικό σχήμα προσσέγγισης (RAS) για την f εάν για κάθε* $x \in \{0,1\}*$ *ισχύει :*

$$Pr(e^{-\varepsilon} \cdot f(x) \leq Y \leq e^{\varepsilon} \cdot f(x)) \geq 3/4$$

όπου Y η έξοδος της M.

Όπως και πριν, επιβάλλοντας περισσότερους περιορισμούς στο χρόνο εκτέλεσης της M προκύπτουν πιο αυστηρά σχήματα.

Ορισμός 3.3.2 *Εάν η M τρέχει σε πολυωνυμικό χρόνο ως προς το μήκος του x - δηλαδή το n - τότε λέμε ότι η M αποτελεί ένα πολυωνυμικού χρόνου πιθανοτικό σχήμα προσσέγγισης για την f. (PRAS)*

Ορισμός 3.3.3 *Εάν επιπλέον η M τρέχει σε πολυωνυμικό χρόνο και ως προς τον αντίστροφο του παράγοντα προσσέγγισης (*$poly(n, \varepsilon^{-1})$*τότε λέμε ότι η M αποτελεί ένα πλήρους πολυωνυμικού χρόνου πιθανοτικό σχήμα προσσέγγισης για την f. (FPRAS)*

Αυτό που θα μας απασχολήσει στην συνέχεια είναι να δούμε αν οι συναρτήσεις του #P έχουν ή όχι FPRAS. Σε προηγούμενες προσπάθειες κατηγοριοποίησης προβλημάτων ως προς την πολυπλοκότητα σημαντικό ρόλο έπαιξε η έννοια της αναγωγής (κατά Cook, κατά Karp κτλ).Για να είναι χρήσιμη μία αναγωγή όμως πρέπει να εξασφαλίζει πως η αναγωγή ενός προβλήματος σε ένα άλλο σημαίνει κάτι σημαντικό για την συσχέτιση της πολυπλοκότητας των δύο ως προς τη δεδομένη κλάση αλγορίθμων που μας ενδιαφέρει κάθε φορά π.χ αν θέλουμε να ελέγξουμε την ύπαρξη πολυωνυμικού αλγορίθμου χρησιμη μπορεί να φανεί η κατά Karp αναγωγή ενός προβλήματος σε κάποιο άλλο με γνωστή πολυωνυμική λύση, αλλά όχι η κατά Cook.Προκειμένου λοιπόν να διευκολύνουμε την κατηγοριοποίηση ως προς την ύπαρξη ή όχι FPRAS ορίζουμε ένα νέο έιδος αναγωγής, τις AP αναγωγές (AP: approximation preserving), οι οποίες εξασφαλίζουν πως αν ένα πρόβλημα ανάγεται σε ένα άλλο μέσω αυτών και το δεύτερο έχει FPRAS τότε έχει και αυτό. Για την ακρίβεια οι AP αναγωγές αναφέρονται στην γενικότερη περίπτωση πιθανοτικών σχημάτων (RAS) αλλά εμείς θα περιοριστούμε στην περίπτωση των FPRAS γιατί αυτά θα μας απασχολήσουν στη συνέχεια. Ο ορισμός λοιπόν έχει ως εξής :

Ορισμός 3.3.4 *Έστω δύο συναρτήσεις* $f, g : \{0,1\} * -> \aleph$. *Λέμε ότι η* f *είναι AP-αναγώγιμη στην* g *ανν υπάρχει NTM η οποία παίρνει ως είσοδο ένα ζεύγος* $(x, \varepsilon) \in \{0,1\} * \times (0,1)$ *και χρησιμοποιώντας ένα FPRAS μαντείο για την* g *στο οποίο κάνει ερωτήσεις της μορφής (x,δ) με* $\delta^{-1} \leq poly(|x|, \varepsilon^{-1})$ *δίνει σε χρόνο* $poly(|x|, \varepsilon^{-1}$ *ένα αποτέλεσμα που πληρεί την γενική συνθήκη των πιθανοτικών αλγορίθμων-* **??**.

Στην ουσία έχουμε για την f ένα FRRAS το οποίο όμως χρησιμοποιεί ένα FRRAS μαντείο για την g προκειμένου να ολοκληρώσει τους υπολογισμούς του.Ο συμβολισμός που χρησιμοποιούμε είναι ο εξής : $f \leq_{AP} g$ όταν υπάρχει AP-αναγωγή της f στην g και $f =_{AP} g$ όταν φ ανάγεται στη g αλλά και η g ανάγεται στην f.Σε αυτή την περίπτωση πρόκειται για AP-ισοδύναμες συναρτήσεις και με ομάδες τέτοιων συναρτήσεων μέσα στο #P θα ασχοληθούμε στη συνέχεια.

3.4 Κλάσεις AP-ισοδύναμων προβλημάτων στο #P

Πριν αναφερθούμε στις κλάσεις που θα μας απασχολήσουν πρέπει να ορίσουμε δύο προβλήματα που παίζουν σημαντικό ρόλο στην παρακάτω κατηγοριοποίηση. Αυτά είναι :
#SAT
Πρόκειται για το πρόβλημα της καταμέτρησης του πλήθους των διαφορετικών αναθέσεων αληθοτιμών που ικανοποιούν μία προτασιακή φόρμουλα σε CNF

μορφή.
#BIS
Πρόκειται για το πρόβλημα της καταμέτρησης του πλήθους των διαφορετικών IS οποιουδήποτε μεγέθους σε ένα διμερή γράφο. Με IS εννοούμε το 'ανεξάρτητο σύνολο' δηλαδή ένα υποσύνολο των καορυφών του γράφου τέτοιο ώστε καμία κορυφή να μην ενώνεται με ακμή με καμία άλλη στο σύνολο.
Τρεις είναι οι κλάσεις που θα μας απασχολήσουν κυρίως σε αυτό το σημείο. Η πρώτη είναι αυτή των προβλημάτων που δέχονται FPRAS.Πρόκειται για τα 'εύκολα να προσεγγισθούν' προβλήματα της κλάσης #P και εύκολα μπορεί να αποδειχθεί ότι είναι όλα AP-ισοδύναμα μεταξύ τους - υπάρχει FPRAS για το καθε ένα ξεχωριστά έτσι δεν χρειάζεται κανένα μαντείο κατά τον υπολογισμό του αλγορίθμου, πρόκειται για ειδική περίπτωση του παραπάνω ορισμού. Η δεύτερη είναι η κλάση των 'δύσκολων να προσεγγισθούν προβλημάτων, είναι αυτά που είναι AP-ισοδύναμα με το #SAT. Και η τρίτη κλάση είναι είναι αυτή των προβλημάτων που είναι AP-ισοδύναμα με το #BIS. Πρόκειται για μια ενδιάμεση κλάση πολυπλοκότητας μιας και ούτε έχει βρεθεί FPRAS για κανένα από τα προβλήματα αυτής της κατηγορίας αλλά ούτε έχει μπορέσει να αναχθεί με AP-αναγωγή το #SAT σε κανένα από αυτά - προκειμένου να αποδειχθεί ότι η όλα είναι AP-ισοδύναμα με το #SAT. Ας δούμε όμως κάποιες περισσότερες πληροφορίες για την κάθε περίπτωση ξεχωριστά.

3.4.1 Προβλήματα που δέχονται FPRAS

Δυστυχώς τα προβλήματα που ανήκουν σε αυτή την κατηγορία δεν είναι πολλά. Προφανώς σε αυτή ανήκουν όλα όσα δέχονται ακριβή λύση π.χ. το πλήθος των spanning trees ενός γράφου. Το ενδιαφέρον όμως κυρίως επικεντρώνεται στα προβλήματα τα οποία είναι #P-πλήρη ως προς Cook-αναγωγή αλλά δέχονται FPRAS. μερικά τέοτια παραδείγματα είναι :

1. Το πρόβλημα του permanent
2. Το πρόβλημα #Matchings δηλαδή το πρόβλημα της καταμέτρησης των ταιριασμάτων όλων των μεγεθών ενός γράφου.
3. Το πρόβλημα #DNF δηαλαδή το πρόβλημα της καταμέτρησης όλων των αναθέσεων που επαληθεύουν μία προτασιακή φόρμουλα σε DNF μορφή.

3.4.2 Προβλήματα AP-ισοδύναμα με #SAT

Το SAT , το πρόβλημα δηλαδή της ικανοποιησιμότητας μιας προτασιακής φόρμουλας σε CNF, έχει αποδειχθεί ότι είναι πλήρες για το NP ως προς την αναγωγή κατά Karp. Θα ήταν πολύ βολικό αν μπορούσαμε να ισχυριστούμε πως

αυτό αρκεί για να δεχτούμε ότι και το #SAT είναι πλήρες για το #P ως προς την AP-αναγωγή. Αλλά κάτι τέτοιο δεν μπορεί να γίνει τόσο ασυλλόγιστα γιατί στη μία περίπτωση ενδιαφερόμαστε απλά για την ύπαρξη λύσης ενώ στη δεύτερη για το πλήθος των λύσεων. Συνεπώς θα πρέπει να εξετάσουμε κατά πόσο οι αναγωγές που εμπλέκονται στις παραπάνω περιπτώσεις επηρεάζουν ή όχι το πλήθος των λύσεων. Μπορούμε εύκολα να διαπιστώσουμε πως η αναγωγή που αποδεικνύει τη πληρότητα του SAT ως προς το NP, με ελαφρές τροποποιήσεις, ανήκει στην κατηγορία των αναγωγών που διατηρούν το πλήθος των λύσεων- parsimonious αναγωγές. Και με δεδομένο ότι οι parsimonious αναγωγές εμπεριέχονται στις AP-αναγωγές ως ειδική περίπτωη εύκολα προκύπτει ότι το #SAT είναι πλήρες ως προς την AP-αναγωγή για την κλάση #P. Επίσης, ο Zuckerman to 1996, [D.Z96], απέδειξε ότι το #SAT δεν μπορεί να δεχθεί FPRAS εκτός και αν NP = RP - γεγονός που συνεπάγεται την κατάρρευση της πολυωνυμικής ιεραρχίας και άρα δεν είναι και τόσο πιθανό. Ετσι είναι μάλλον απίθανο να υπάρχει FPRAS για το #SAT καθώς και για όλα τα άλλα προβλήματα τα οποία είναι AP-ισοδύναμα με αυτό. Και με δεδομένο ότι το #SAT είναι πλήρες ως προς την AP-αναγωγή για το #P , AP-ισοδύναμα με αυτό έιναι όλα τα προβλήματα στα οποία αυτό μπορεί να αναχθεί.Στην ουσία δηλαδή αναζητάμε όλα τα προβλήματα τα οποία είναι πλήρη για την κλάση #P ως προς την AP-αναγωγή. Θα ήταν πολύ βολικό αν μπορούσαμε να μεταφράσουμε απλά την πληρότητα ενός προβλήματος ως προς το NP σε πληρότητα της συνάρτησης που μετράει το πλήθος των λύσεων αυτού ως προς το #P - όπως κάναμε για το SAT και το #SAT. Αυτό εξαρτάται έντονα παό τα είδη των αναγωγών που χρησιμοποιούμε.Για παράδειγμα για το ζεύγος Karp αναγωγή στο NP και Cook αναγωγή στο #P κάτι τέτοιο δεν έχει μπορέσει να αποδειχθεί στη γενική περίπτωση αλλά ούτε έχει βρεθεί αντιπαράδειγμα. Στην περίπτωση των AP-αναγωγών όμως η απόδειξη είναι δυνατή. Αυτό φαίνεται στο παρακάτω θεώρημα.

Θεώρημα 3.4.1 *Έστω A ένα NP πλήρες πρόβλημα . Τότε το αντίστοιχο πρόβλημα μέτρησης, #A, είναι πλήρες για το #P ως προσ την AP-αναγωγή.*

Απόδειξη: Το γεγονός ότι #A ανήκει στο #P είναι προφανές. Το ζήτημα είναι να αποδείξουμε ότι το #SAT μπορεί να αναχθεί κατά AP στο #A. Θα χρησιμοποιήσουμε κάτι που αποδείχθηκε στο [LV86], το ότι υπάρχει FPRAS για το #SAT που χρησιμοποιεί μαντείο για το SAT. Το μαντείο αυτό όμως μπορεί να αντικατασταθεί από ένα FPRAS για το #A αφού το SAT μπορεί να αναχθεί στο A και έναs FPRAS αλγόριθμος μπορεί να ξεχωρίσει αξιόπιστα τις περιπτώσεις μη ύπαρξης λύσης από όλες τις υπόλοιπες.. Έτσι μπορούμε να κατασκευάσουμε ένα FPRAS για το #SAT που να πληρεί τις προυποθέσεις του ορισμού 3.3.4 και άρα αποδείξαμε το ζητούμενο.

□

Όμως εκτός από τα NP-πλήρη προβλήματα υπάρχουν και προβλήματα που ανήκουν στο #P και είναι ππλήρη ως προς την AP-αναγωγή ενώ αντιστοιχούν σε εύκολα -στο P- προβλήματα απόφασης. Ένα τέτοιο παράδειγμα παοτελέι το πρόβλημα της καταμέτρησης του σπλήθους των IS σε ένα γενικό γράφο - #IS.([MD04]).

3.4.3 Προβλήματα AP-ισοδύναμα με #BIS

Όπως είπαμε και παραπάνω πρόκειται για μια ενδιάμεση κατηγορία προβλημάτων η πολυπλοκότητα προσεγγισης της οποίας είναι ακόμη αδιευκρίνιστη. Κανένας εκπρόσωπος αυτής της κατηγορίας δεν έχει αποδειχθεί να έχει FPRAS αλλά ούτε να είναι AP-ισοδύναμος με το #SAT.πριν δούμε μερικούς αντιπροσώπους της κατηγορίας αυτής θα πρέπει να ορίσουμε την έννοια του H-χρωματισμού. Έστω λοιπόν γράφος H με q κορυφές. Το πρόβλημα του H-χρωματισμού ενός γράφου G έγκειται στην εύρεση ενός ομομορφισμού από τον G στον H.Δηλαδή, αν αντιμετωπίσουμε τις κορυφές του H σαν χρώματα και τις ακμές αυτού σαν ενδείξεις των δυνατών γειτνιάσεων των χρωμάτων, τότε αυτό που αναζητάμε είναι η εύρεση ενός q-χτωματισμού του G που να υπακούεισ τους κανόνες γειτνίασης που ορίζει ο H.Μπορούμε τώρα να παρουσιάσουμε μερικά προβλήματα που ανήκουν στην οικογένεια του #BIS [MD04]:

1. #P4-COL: Πρόκειται για το πρόβλημα της καταμέτρησης των δυνατών P4-χρωματισμών ενός γράφου G, όπου P4 είναι το μονοπάτι μήκους 3.

2. #Downsets: Πρόκειται για το πρόβλημα της καταμέτρησης του αριθμού των αλυσίδων σε ένα μερικώς διατεταγμένο σύνολο.

3. #1P1NSAT : Πρόκειται για το πρόβλημα της καταμέτρησης του αριθμού των αναθέσεων που ικανοποιούν μία προτασιακή φόρμουλα σε CNF μορφή ,όπου σε κάθε clause υπάρχει το πολύ μία θετική και το πολύ μία αρνητική μεταβλητή.

4. #BeachConfigs : Πρόκειται για το πρόβλημα της καταμέτρησης του αριθμού των P4*-χρωματισμών ενός γράφου G, όπου P4* είναι το μονοπάτι μήκους 3 με βρόγχους σε όλες τις κορυφές του.

5. #2-Particle-WR-Configs : πρόκειται για το πρόβλημα της καταμέτρησης του αριθμού των S2*-χρωματισμών ενός γράφου G, όπου S2* είναι το αστέρι με 2 φύλλα που περιέχει και βρόγχο σε όλες του τις κορυφές.

Για όλα αυτά τα προβλήματα ισχύει το παρακάτω θεώρημα :

Θεώρημα 3.4.2 *Τα προβλήματα #BIS, #P4-COL,#2-Particle-WR-Configs, #BeachConfigs,#Downsets,#1P1NSAT είναι όλα AP-ισοδύναμα.*

Απόδειξη: [MD04]

□

Κεφάλαιο 4

Το πρόβλημα της ομοιόμορφης δειγματοληψίας ενός χώρου λύσεων -sampling- και η σχέση του με την ύπαρξη FPRAS για προβλήματα του #P

Όπως είπαμε και στην εισαγωγή, το θέμα μας είναι η μελέτη των προβλημάτων που ανήκουν στην κλάση #P. Η κλάση αυτή ανήκει στην κατηγορία των μετρητικών κλάσεων δηλαδή περιέχει συναρτήσεις που μετρούν το πλήθος των λύσεων κάποιου προβλήματος. Εκτός όμως από το να μετρήσουμε τις λύσεις υπάρχουν και άλλα ερωτήματα που μπορεί ναμ μας απασχολήσουν όσο αφορά ένα συγκεκριμένο πρόβλημα π.χ. αν έχει έστω και μία λύση, η κατασκευή μίας λύσης αλλά και η τυχαία επιλογή μίας λύσης από όλες τις δυνατές-δειγματοληψία.Σε αυτό το κεφάλαιο θα ασχοληθούμε αρχικά με το να ορίσουμε όλα τα ερωτήματα που συνήθως μας απασχολούν όσο αφορά το στιγμιότυπο ενός προβλήματος και κυρίως αυτό της δειγματοληψίας και στη συνέχεια να το συσχετίσουμε με το πρόβλημα της καταμέτρησης των λύσεων .

4.1 Ορισμός του προβλήματος της δειγματοληψίας και πολυπλοκότητα αυτού

Ας δούμε όμως αναλυτικά τα ερωτήματα που αναφέραμε παραπάνω. Έστω λοιπόν ένα πρόβλημα το οποίο θα αναπαριστούμε με την σχέση R και ένα

στιγμιότυπο x $\in \{0,1\}^*$ αυτού. Έχουμε:

1. Ύπαρξη: Υπάρχει y $\in \{0,1\}^*$ τέτοιο ώστε xRy, δηλαδή το y να είναι λύση για το x ;

2. Κατασκευή : Κατασκεύασε ένα y τέτοιο ώστε xRy - εφόσον υπάρχει.

3. (Ομοιόμορφη) δειγματοληψία : Παρήγαγε ένα y τέτοιο ώστε xRy με τέοιο τρόπο ώστε όλα τα y που ικανοποιούν την σχέση xRy να μπορούν να προκύψουν με ίση πιθανότητα. Σε αυτό το πρόβλημα θα αναφερόμαστε στο εξής ως πρόβλημα του sampling.

4. Καταμέτρηση : Μέτρησε το πλήθος των y για τα οποία ισχύει xRy.

Όπως είπαμε και πριν αυτό που θέλουμε να κάνουμε είναι να δούμε την σχέση μεταξύ του sampling και του προβλήματος της καταμέτρησης γιατί αυτό θα μας επιτρέψει να βρούμε πιο εύκολα FPRAS για τα προβλήματα #P. Για αυτό το λόγο θα το μελετήσουμε λίγο περισσότερο. Αρχικά θα δούμε ένα υπολογιστικό μοντέλο για το πρόβλημα του sampling δηλαδή μία NTM η οποία όταν πληρεί κάποιες συγκεκριμένες υποθέσεις αποτελεί έναν sampler για το πρόβλημά μας.

Ορισμός 4.1.1 *Έστω μία NTM M. Λέμε ότι η M είναι ένας sampler για το πρόβλημα που αναπαριστά η σχέση R όταν*

1. *Υπάρχει μία συνάρτηση* $\varphi : \{0,1\} * - > (0,1]$ *τέτοια ώστε για κάθε* $x,y \in \{0,1\}^*$

$$Pr(inputx, Moutputsy) = 0 if notxRy$$
$$Pr(inputx, Moutputsy) = \varphi(x) if xRy$$

2.
$$Pr(Macceptsx) \geq 1/2$$

για κάθε είσοδο x που έχει τουλάχιστον μία λύση.

Πρόκειται δηλαδή για μία μηχανή η οποία παράγει μόνο λύσεις για κάθε στιγμιότυπο του προβλήματος και μάλιστα κάθε λύση έχει την ίδια πιαθνότητα με όλες τις άλλες να παραχθεί. Επίσης, η μηχανή μπορεί να απορρίψει το input. Αυτό πρέπει να συμβαίνει γιατί μπορεί να μην υπάρχει λύση για το x άρα η μηχανή δεν επιτρέπεται να δώσει output. Στην περίπτωση που υπάρχει λύση υπάρχει πάντα η πιθανότητα η μηχανή μας να κάνει λάθος και να την απορρίψει μη δίνοντας έξοδο αλλά θέλουμε η πιθανότητα να συμβεί αυτό να

είναι φραγμένη σε κάποια σταθερά στο διάστημα (0,1). Στον παραπάνω ορισμό επιλέξαμε το 1/2 ως φράγμα αλλά η αλήθεια είναι ότι δεν έχει σημασία η τιμή της σταθεράς αφού μέσω διαδοχικών επαναλήψεων μπορούμε να άυξήσουμε την πιθανότητα αυτή όσο θέλουμε..
Έχοντας ορίσει πλέον τις προυποθέσεις που πρέπει να πληρεί μία NTM για να λύνει το πρόβλημα του sampling λογικό είναι να αρχίσουμε να αναρωτιόμαστε για το πόσο 'πολυπλοκη'- με την έννοια των απαιτήσεων σε χρόνο - είναι μία τέτοια μηχανή. Το παρακάτω θεώρημα δίνει μία απάντηση στο θέμα της πολυπλοκότητας του προβλήματος του sampling.Πριν όμως το δούμε θα πρέπει να ορίσουμε τι σημαίνει πολυωνυμική σχέση R- για συντομία π-σχέση. Στην ουσία πρόκειται για μία σχέση στην οποία το μήκος του y φράσσεται από κάποιο πολυώνυμο ως προς το μήκος του x , και μπορεί να ελεχθεί σε πολυωνυμικό χρόνο αν ένα ζευγάρι (x,y) ανήκει στη σχέση. Με μια πρώτη ματιά οι απαιτήσεις αυτές μπορεί να φαίνονται ασήμαντες αλλά αν αναλογιστούμε ότι στην περίπτωσή μας οι σχέσεις R αντιπροσωπεύουν προβλήματα και τα x,y κωδικοποιούν στιγμιότυπα και λύσεις αυτών αντίστοιχα καταλαβαίνουμε πως με αυτό τον τρόπο περιορίζουμε την ανάλυσή μας σε προβλήματα για τα οποία οι υπολογισμοί των οποιονδήποτε μοντέλων επίλυσής τους έχουν το πολύ πολυωνυμικό μήκος ως προς το input.Είμαστε πλέον έτοιμοι να δούμε το θεώρημα.

Θεώρημα 4.1.1 *[MJ86] Έστω μία π-σχέση R. Τότε υπάρχει sampler για την R με την εξής μορφή :*

1. *Μία πολυωνυμικού χρόνου NTM με μαντείο για το #P*
2. *Μία πολυωνυμικού χρόνου NTM με μαντείο για το Σ_2^p*

Ιδέα Απόδειξης: Η ιδέα της απόδειξης βασίζεται στο εξής : θα ήταν πολύ εύκολο για μας να κατασκευάσουμε μία πιθανή λύση για το x επιλέγοντας τυχαία το κάθε ψηφίο του y. Με αυτό τον τρόπο όλες οι δυνατές λύσεις θα είχαν την ίδια πιθανότητα να προκύψουν. Όμως η πιαθανότητα να φτιάξουμε ένα y που όντως θα είναι λύση για το x δεν θα είναι φραγμένη όπως απαιτεί ο παραπάνω ορισμός. Για αυτό δεν αρκεί να κάνουμε τελέιως τυχαίες επιλογές, πρέπει να έχουμε κάποια επιπλέον πληροφόρηση. Τις πληροφορίες που χρειαζόμαστε για να κάνουμε την 'καλύτερη' επιλογή για κάθε ψηφίο της λύσης θα τις πάρουμε από το μαντείο το οποίο μας παρέχεται.Αυτό που θα μας βοηθούσε πολύ είναι να ξέρουμε πόσες λύσεις υπάρχουν που έχουν το ίδιο πρόθεμα με αυτή που έχουμε μέχρι στιγμής εμείς κατασκευάσει. Αν το μαντείο μας είναι το ίδιο το #P τότε μπορούμε να έχουμε τον ακριβή αριθμό των λύσεων σε κάθε βήμα. Αν το μαντείο μας είναι το Σ_2^p τότε σύμφωνα με το θεώρημα για

την πολυπλοκότητα της προσσεγγισιμότητας του #P του Sockmeyer που είδαμε στο προηγούεμνο κεφάλαιο μπορούμε να πάρουμε προσσεγιστικές τιμές για το πλήθος των λύσεων που ικανοποιούν τους περιορισμούς μας. Και με δεδομένο ότι δεν επιδιώκουμε να κατασκευάσουεμ λύση με πιθανότητα 1 αλλά με κάποια άλλη σταθερά μπορούμε να ρυθμίσουμε έτσι τις σταθερές προσσέγγισης ώστε να μας εξασφαλίζουν το όριο που θέλουμε. Μια πιο λεπτομερής παρουσίαση ύπάρχει στο [MJ86].

□

Συνεπώς το πρόβλημα του sampling ανήκει στην πολυωνυμική ιεραρχία, αντίθετα από το #P - εκτός και αν η PH καταρρέει. Αυτό σημαίνει ότι το πρόβλημα του sampling δεν μπορεί να είναι πιο δύσκολο από το προβλημα της καταμέτρησης. Μάλιστα υπάρχει πρόβλημα, το DNF, για το οποίο μπορούμε να κατασκευάσουμε πολυωνυμικό sampler ενώ το αντίστοιχο πρόβλημα καταμέτρησης είναι #P πλήρες. Επίσης μπορούμε να ισχυριστούμε πως το πιθανότερο είναι πως το sampling είναι πιο δύσκολο από το πρόβλημα της κατασκευής. Η διαφορά των δύο έγκειται στο ότι το πρώτο απαιτεί οι λύσεις να προκύπτουν με ίση πιθανότητα. Το παρακάτω θεώρημα ενισχύει αυτή την άποψη. Πριν το δούμε όμως πρέπει να ορίσουμε το πρόβλημα στο οποίο αναφέρεται-GenCycle.

Ορισμός 4.1.2 *Έστω κατευθυνόμενος γράφος G. Το ζητούμενο είναι η ομοιόμορφη παραγωγή -sampling- κύκλων του G.*

Αν το πρόβλημα του sampling είναι ισοδύναμο με το πρόβλημα της κατασκευής για κάθε πρόβλημα τότε θα είναι και για το πρόβλημα GenCycle.Και αφού το πρόβλημα της κατασκευής ενός κύκλου σε έναν κατευθυνόμενο γράφο λύνεται σε πολυωνυμικό χρόνο τότε και το GenCycle θα λύνεται αποδοτικά. Κάτι τέτοιο όμως συνεπάγεται ότι το NP = RP σύμφωνα με το παρακάτω θεώρημα.

Θεώρημα 4.1.2 *[MJ86] Αν υπάρχει πολυωνυμικού χρόνου NTM που επιλύει το GenCycle τότε NP = RP.*

Ιδέα Απόδειξης: Αρκεί να αποδείξουμε ότι ένα NP πλήρες πρόβλημα βρίσκεται στο RP. Τότε, επειδή $RP \subseteq NP$, θα ισχύει και RP = NP. Το πρόβλημα που μπορούμε εύκολα να αποδείξουμε ότι ανήκει στο RP αν ισχύουν οι υποθέσεις του θεωρήματος είναι το DHC, δηλαδή το πρόβλημα της ύπαρξης κύκλου Hamilton σε έναν κατευθυνόμενο γράφο. Έστω ένας γράφος G. Η ιδέα είναι να κατασκευάσουμε έναν γράφο G' από τον G τέτοιο ώστε η ύπαρξη κύκλου στο G' ενός συγκεκριμένου μεγέθους (α) να συνεπάγεται την ύπαρξη κύκλου

Hamilton στον αρχικό και μάλιστα στον G' θέλουμε οι κύκλοι αυτού του μεγέθους να είναι περισσότεροι από τους μισούς συνολικούς κύκλους αυτού του μεγέθους. Σε αυτή την περίπτωση αν ο G έχει κύκλο Hamilton τότε μία τυχαία επιλογή ενός κύκλου του G' - που μπορεί να γίνει σε πολυωνιμικό χρόνο σύμφωνα με τις υποθέσεις μας - με πιθανότητα μεγαλύτερη από 1/2 θα δώσει κύκλο μεγέθους α ενώ αν ο G δεν έχει κύκλο Hamilton τότε η πιθανότητα είναι 0. Συνεπώς, μέσω του πολυωνυμικό sampling για το GenCycle μπορούμε να αποδείξουμε ότι το DHC ανήκει στο RP.

□

4.2 Σχέση FPRAS και FPAUS

Γιατί όμως να μπούμε στον κόπο να ασχοληθούμε με το πρόβλημα του sampling; Είναι όπως είδαμε μάλλον πιο εύκολο από το πρόβλημα της καταμέτρησης αλλά μέχρι στιγμής δεν έχει προκύψει κάποια άλλη συσχέτιση μεταξύ τους που να μπορεί να φανεί χρήσιμη...
Ο λόγος που ασχολουμστε είναι ότι για κάποιες κατηγορίες προβλημάτων καταμέτρησης μία ελαφρώς διαφοροποιημένη εκδοχή του sampling ταυτίζεται με την δημιουργία FPRAS για τα προβλήματα αυτά. Η εκδοχή του sampling που θα μας απασχολήσει από εδώ και στο εξής είναι η σχεδόν ομοιόμορφη δειγματοληψία η αλλιώς almost uniform sampling. Η διαφορά με πριν είναι ότι σε αυτή την περίπτωση επιτρέπουμε οι πιθανότητες με τις οποίες προκύπτουν οι λύσεις να είναι ελαφρώς διαφορετικές. Πιο επίσημα για την κλάση του almost uniform sampling έχουμε το παρακάτω υπολογιστικό μοντέλο :

Ορισμός 4.2.1 *Έστω μία NTM M. Λέμε ότι η M είναι ένας almost uniform sampler για το πρόβλημα που αναπαριστά η σχέση R όταν πάρνει ως είσοδο ένα ζευγάρι (x,ε) και*

1. *Υπάρχει μία συνάρτηση* $\varphi : \{0,1\} * -> (0,1]$ *τέτοια ώστε για κάθε* $x,y \in \{0,1\}^*$

$$Pr(input(x,\varepsilon), Moutputsy) = 0 if notxRy$$
$$(1+\varepsilon)^{-1}\varphi(x) \leq Pr(input(x,\varepsilon), Moutputsy) \leq (1+\varepsilon)\varphi(x) if xRy$$

2. $$Pr(Maccepts(x,\varepsilon)) \geq 1/2$$

για κάθε είσοδο x που έχει τουλάχιστον μία λύση.

Δηλαδή υπάρχει απλά μία επιπλέον παράμετρος εισόδου στην μηχανή που καθορίζει την 'ανεκτικότητα' στην απόκλιση από την ομιόμορφη δειγματοληψία.Αν επιπλέον υπάρχει πολυώνυμο g τέτοιο ώστε κάθε δυνατή ακολουθία υπολογισμών της μηχανής να έχει μήκος το πολύ g(—x—,log(1/ε)) λέμε ότι έχουμε έναν πολυωνυμικού χρόνου σχεδόν ομοιόμορφο δειγματολήπτη (FPAUS). Επιπλέον, τα προβλήματα τα οποία θα μας απασχολήσουν από εδώ και πέρα είναι αυτά τα οποία έχουν την ιδιότητα της αυτοαναγωγής- self reducibility και ορίζονται ως εξής :

Ορισμός 4.2.2 *Έστω μία σχέση R. Λέμε ότι αυτή είναι self-reducible αν*

1. *Υπάρχει ένα πολυώνυμο g τέτοιο ώστε* $xRy- > |y| \leq g(|x|)$.
2. *Υπάρχουν πολυωνυμικού χρόνου συναρτήσεις* $\psi : \{0,1\} * \times \{0,1\} * \rightarrow \{0,1\}$ *και* $\sigma : \{0,1\} * \rightarrow \aleph$ *που ικανοποιούν τις συνθήκες :*

$$\sigma(x) = O(log|x|)$$

$$g(|x|) > 0 \Rightarrow \sigma(x) > 0$$

$$|\psi(x,w)| < |x|$$

και για όλα τα $x \in \{0,1\} *, y = y_1 y_2 y_3 ... y_k \in \{0,1\} *$ *ισχύει :*

$$xRy \Leftrightarrow \psi(x, y_1 y_2 y_3 ... y_{\sigma(x)}) R y_{\sigma(x)+1} y_{\sigma(x)+2} ... y_k$$

Στην ουσία ο παραπάνω ορισμός μας λέει πως το σύνολο των λύσεων που αντιστοιχεί σε ένα στιγμιότυπο του προβλήματος μπορεί να συσχετιστεί - και να παραχθεί -από τα σύνολα λύσεων άλλων μικρότερων στιγμιοτύπων. Ο ρόλος της συνάρτησης g είναι να περιορίζει πολυωνυμικά το μήκος των λύσεων ενώ της συνάρτησης σ να καθορίζει τη βαρύτητα των λύσεων ως εξής : έστω ένα στιγμιότυπο x και w ένα πρόθεμα της λύσης μήκους σ(x). Τότε, μέσω της συνάρτησης ψ μπορούμε να πάρουμε ένα άλλο στιγμιότυπο x' - μικρότερο σε μήκος - του οποίου οι λύσεις ενωμένες με το πρόθεμα w συνιστούν λύσεις για το x.Ενδεχομένως ο παραπάνω ορισμός να φαίνεται λίγο δυσνότητος αλλά η κεντρική του ιδέα είναι απλή : περιγράφει προβλήματα στα οποία για να βρούμε τη λύση ˚για ένα στιγμιότυπο αρκεί να επιλύσουμε το πρόβλημα για κάποια μικρότερα στιγμιότυπα και να 'συνθέσουμε' τις λύσεις που βρήκαμε. Πολλά από τα προβλήματα που συνήθως μας απασχολούν έχουν την παραπάνω ιδιότητα. Μερικά τέοια παραδείγματα είναι τα : DNF,SAT κτλ..
Επιπλέον θα χρειαστούμε δύο ακόμη ορισμούς.

Ορισμός 4.2.3 *Έστω μία σχέση R. Ορίζουμε την* $Ext_R(x,w) = |y : xRwy|$.

Δηλαδή η παραπάνω συνάρτηση μετράει το πλήθος των λύσεων για το x που έχουν ως αρχικό πρόθεμα το w.

Ορισμός 4.2.4 *Έστω μία σχέση R. Ορίζουμε την* $N_R(x) = |y : xRy|$.

Δηλαδή η παραπάνω συνάρτηση μετράει το πλήθος των λύσεων για το x. Η σχέση που συνδέει τις δύο συναρτήσεις είναι προφανώς : $N_R(x) = Ext_R(x, \perp)$ όπου $\perp$ συμβολίζει το κενό string. Και τώρα που έχουμε ορίσει τις απαραίτητες έννοιες μπορούμε πλέον να δούμε το κεντρικό θεώρημα που συσχετίζει την ύπαρξη FPRAS για ένα πρόβλημα καταμέτρησης με την ύπαρξη FPAUS.

Θεώρημα 4.2.1 *[MJ86] Έστω R μία self-reducible π-σχέση. Εάν υπάρχει FPRAS για την* $N_R(x)$ *τότε υπάρχει και FPAUS για την R.*

Επίσης ισχύει και το αντίστροφο.

Θεώρημα 4.2.2 *[MJ86] Έστω R μία self-reducible π-σχέση. Εάν υπάρχει FPAUS για την R τότε υπάρχει και FPRAS για την* $N_R(x)$.

Ιδέα Απόδειξης: Η βασική ιδέα αυτού του θεωρήματος είναι ότι μπορούμε να χρησιμοποιήσουμε το FPAS που έχουμε για να εκτιμήσουμε το λόγο των λύσεων που έχουν ένα συγκεκριμένο πρόθεμα προς το συνολικό αριθμό λύσεων. Δηλαδή μπορούμε να εκτιμήσουμε λόγους της μορφής :

$$Ext_R(x, w)/N_R(x)$$

Όμως εμείς χρειαζόμαστε μία εκτίμηση για τον παρονομαστή αυτού του κλάσματος. Προκειμένου να το επιτύχουμε αυτό θα ανάγουμε τον υπολογισμό του αριθμητή σε κάτι νέο μέσω της ιδιότητας self-reducibility που έχει η R. Συγκεκριμένα, μπορούμε εύκολα να δούμε ότι $Ext_R(x, w) = N_R(\psi(x, w))$. Και έτσι αναγάγαμε το πρόβλημα του υπολογισμού του $N_R(x)$ στο πρόβλημα του υπολογισμού του $N_R(\psi(x, w))$ το οποίο είναι της ίδιας μορφής αλλά αφορά μικρότερο στιγμιότυπο εισόδου.Με αυτό τον τρόπο, αναδρομικά, μπορούμε μειώνοντας σε κάθε βήμα το μέγεθος να καταλήξουμε τελικά σε πολύ μικρά μεγέθη input όπου το πρόβλημα είναι trivial. Και έτσι το ζητούμενο μπορεί να προκύψει από απλό πολλαπλασιασμό των ενδιάμεσων λόγων εκτίμησης.

□

Και στην πράξη ή πορεία που ακολουθούμε προκειμένου να κατασκευάσουμε FPRAS από ένα FPAUS είναι παρόμοια με την ιδέα της παραπάνω απόδειξης. Ένα παράδειγμα θα δούμε στην παρακάτω ενότητα.

4.3 Ένα παράδειγμα:#Matchings

Στην ενότητα αυτή θα δούμε πως μπορούμε αν έχουμε ένα FPAUS για το #Matchings να κατασκευάσουμε ένα FPRAS. Έστω λοιπόν ένας almost uniform sampler S που τρέχει σε χρόνο το πολύ T(n,m,ε) , οπου n,m είναι το πλήθος των κορυφών και των ακμών του γράφου G στο οποίο αναφερόμαστε. Έστω επίσης μία διάταξη των ακμών του γράφου $E = \{e_1, e_2, e_3, ..., e_m\}$ και G_i ο γράφος με το ίδιο σύνολο κορυφών με τον αρχικό αλλά $E_i = \{e_1, e_2, e_3, ..., e_i\}$. Δηλαδή ο G_{i-1} προκύπτει από τον G_i με αφαίρεση μίας ακμής. Η ποσότητα ποθ θέλουμε να εκτιμήσουμε είναι : $|M(G)|$ και μπορεί να εκφραστεί ως ένα γινόμενο :

$$|M(G)| = (\rho_1\rho_2....\rho_m)^{-1}$$

όπου

$$\rho_i = |M(G_{i-1})|/|M(G_i)|$$

. Επειδή ισχύει ότι $M(G_{i-1}) \subseteq M(G_i)$ και επίσης κάθε ταίριασμα στο $M(G_i)$ μπορεί να αντιστοιχισθεί σε ένα ταίριασμα στο $M(G_{i-1})$ - $M' = M\ \{e_i\}$ - μπορούμε να δούμε ότι

$$1/2 \leq \rho_i \leq 1(1)$$

. Μπορούμε να υποθέσουμε ότι 0 ¡ ε ¡ 1 και m ¿= 1.Για να εκτιμήσουμε το κάθε ρ_i τρέχουμε τον S με δ = ε/6m στον γράφο G_i και αποκτάμε ένα ταίριασμα M. Έστω Z_i η τυχαία μεταβλητή που δηλώνει αν το M ανήκει η όχι και στο G_{i-1}. Έστω μ_i η μέση τιμή αυτής. Τότε σύμφωνα με τις ιδιότητες της τυπικής απόκλισης έχουμε ότι :

$$\rho_i - \varepsilon/6m \leq \mu_i \leq \rho_i + \varepsilon/6m$$

ή , χρησιμοποιώντας την σχέση (1) έχουμε :

$$\rho_i(1 - \varepsilon/3m) \leq \mu_i \leq \rho_i(1 + \varepsilon/3m)(2)$$

Έτσι αν πραγματοποιήσουμε έναν αρκετά μεγάλο αριθμό ανεξάρτητων δοκιμών - έστω $s = \lceil 74\varepsilon^{-2}m \rceil \leq 75m\varepsilon^{-2}$ - μπορούμε μέσω του δειγματικού μέσου των $Z_i^1, Z_i^2, ..., Z_i^s$, τον $\bar{Z}_i = s^{-1}\sum_{n=1}^{n=s} Z_i^n$να εκτιμήσουμε τα ρ_i με ικανοποιητική ακρίβεια. Συγκεκριμένα έχουμε :

$$VarZ_i = E((Z_i - \mu_i)^2) = Pr(Z_i = 1)(1 - \mu_i)^2 + Pr(Z_i = 0)\mu_i^2 = \mu_i(1 - \mu_i)$$

Επίσης από τις σχέσεις 1 και 2 συμπεραίνουμε ότι $\mu_i \geq 1/3$. Άρα

$$\mu_i^{-2}VarZ_i = \mu_i^{-1} - 1 \leq 2$$

και έτσι :
$Var\ ^{-}Z_i\ /\mu_i^2 \leq 2/s \leq \varepsilon^2/37m$

Σαν εκτιμητή του $|M(G)|$ θα χρησιμοποιήσουμε την τυχαία μεταβλητή $N = (\Pi_{i=1}^{i=m}(^{-}Z_i))^{-1}$. Για το N ισχύει ότι :

1. $$E(1/N) = \mu_1\mu_2...\mu_m$$

2. $Var(1/N)/(\mu_1\mu_2...\mu_m)^2 = E(\bar{Z_1}^2\bar{Z_2}^2.....\bar{Z_m}^2)/(\mu_1\mu_2...\mu_m)^2) - 1 = \Pi(E(\bar{Z_i}^2/\mu_i^2)) - 1 = \Pi(1 + Var(\bar{Z_i})/\mu_i^2)) - 1 \leq (1+\varepsilon^2/37m)^m - 1 \leq exp(\varepsilon^2/37m) - 1 \leq \varepsilon^2/36m$ λόγω του ότι $exp(x/k+1) \leq 1 + x/k \gamma\iota\alpha 0 < x < 1$

Έτσι από την ανισότητα του Chebyshev προκύπτει ότι :

$$(1 - \varepsilon/3)\mu_1\mu_2...\mu_m \leq \bar{Z_1}\bar{Z_2}.....\bar{Z_m} \leq (1 + \varepsilon/3)\mu_1\mu_2...\mu_m$$

με πιθανότητα ίση με 3/4.Επειδή όμως ισχύει και ότι $exp(-x/k) \leq 1 - x/(k+1) \gamma\iota\alpha 0 < x < 1$μπορούμε να πούμε για την παραπάνω ανισότητα ότι :

$$e^{-\varepsilon/2}\mu_1\mu_2...\mu_m \leq \bar{Z_1}\bar{Z_2}.....\bar{Z_m} \leq e^{\varepsilon/2}\mu_1\mu_2...\mu_m(3)$$

Αλλά από την (2) και την ιδιότητα της εκθετικής έχουμε :

$$e^{-\varepsilon/2}\rho_1\rho_2...\rho_m \leq \mu_1\mu_2...\mu_m \leq e^{\varepsilon/2}\rho_1\rho_2...\rho_m(4)$$

Από (3) και (4) παίρνουμε τελικά ότι:

$$e^{-\varepsilon}\rho_1\rho_2...\rho_m \leq \bar{Z_1}\bar{Z_2}.....\bar{Z_m} \leq e^{\varepsilon}\rho_1\rho_2...\rho_m(4)$$

με πιθανότητα 3/4. Με δεδομένο ότι $N^{-1} = (\Pi_{i=1}^{i=m}(\bar{Z_i}))$ και $\rho_1\rho_2...\rho_m = |M(G)|^{-1}$ καθώς και ότι ο χρόνος εκτέλεσης της παραπάνω διαδικασίας είναι $smT(n, m, \varepsilon/6m) \leq 75m^2\varepsilon^{-2}T(n, m, \varepsilon/6m)$ συμπεραίνουμε ότι η διαδικασία που περιγράφηκε συνιστά έναν FPRAS για το $|M(G)|$.

4.4 Δημιουργία FPAUS :Markov Chain Monte Carlo (MCMC) μέθοδος

Είδαμε λοιπόν ότι η ύπαρξη FPAUS συνδέεται στενά με την ύπαρξη FPRAS - για κάποιες κατηγορίες προβλημάτων τουλάχιστον. Για αυτό, στην ενότητα αυτή θα αφιερώσουμε λίγο χρόνο στην παρουσίαση της Markov Chain Monte Carlo μεθόδου που χρησιμοποιείται συχνά για την σχεδίαση FPAUS.

4.4.1 Τι είναι οι Μαρκοβιανές αλυσίδες

Θα ασχοληθούμε με Μαρκοβιανές αλυσίδες διακριτού χρόνου με πεπερασμένο χώρο καταστάσεων Ω. Σε αυτή την περίπτωση μία Μαρκοβιανή αλυσίδα είναι απλά μία ακολουθία από τυχαίες μεταβλητές η οποία όμως έχει την Μαρκοβιανή ιδιότητα : κάθε χρονική στιγμή η τιμή της επόμενης τυχαίας μεταβλητής εξαρτάται μόνο από την τιμή της τρέχουσας και όχι από τις προηγούμενες τιμές. Εναλλακτικά, βλέποντας τις τυχαίες μεταβλητές ως καταστάσεις μπορούμε να πούμε ότι αρκεί η επόμενη κατάσταση να εξαρτάται μόνο από την τωρινή και όχι από το πως φτάσαμε σε αυτήν. Δηλαδή θέλουμε να ισχύει η εξής ιδιότητα:

$$Pr(X_{t+1} = a|X_t = b, X_{t-1} = c....., X_0 = z) = Pr(X_{t+1} = a|X_t = b)$$

Εμάς βέβαια θα μας απασχολήσουν μόνο οι χρονικά σταθερές Μαρκοβιανές αλυσίδες, δηλαδή αυτές για τις οποίες το δεξί μέλος της παραπάνω σχέσης είναι ανεξάρτητο από το χρόνο. Σε αυτή την περίπτωση η Μαρκοβιανή αλυσίδα χαρακτηρίζεται πλήρως από τον πίνακα μετάβασης που ορίζει την πιθανότητα μετάβασης παό την μία κατάσταση στην άλλη σε ένα βήμα και ορίζεται ως εξής :

$$P(x, y) = Pr(X_{t+1} = y|X_t = x)$$

Μπορούμε να ορίσουμε και τον πίνακα μετάβασης που καθορίζει τις πιθανότητες μετάβασης από μία κατάσταση σε μία άλλη σε t - βήματα δηλαδή :

$$P^t(x, y) = Pr(X_t = y|X_0 = x)$$

ως εξής :

$$P^t(x, y) = \sum_{y' \in \Omega} P^{t-1}(x, y')P(y', y) \gamma \iota \alpha t > 0$$

Σημαντικό ρόλο στον σχεδιασμό FPAUS παίζει η stationary κατανομή μίας MA καθώς και οι ιδιότητες αυτής που εξασφαλίζουν την ύπαρξή της κατανομής.Πιο συγκεκριμένα :

Ορισμός 4.4.1 *Η stationary κατανομή μίας MA με πίνακα μετάβασης P είναι μία κατανομή πιθανότητας πάνω στο χώρο κατάστασης Ω (π: Ω-¿[0,1]) τέτοια ώστε*

$$\pi(y) = \sum_{y' \in \Omega} \pi(y')P(y', y)$$

Κάθε Μαρκοβιανή αλυσίδα με πεπερασμένο χώρο καταστάσεων έχει τουλάχιστον μία stationary κατανομή. Το παρακάτω θεώρημα μας λέει σε ποιές περιπτώσεις αυτή είναι και μοναδική. Πριν το δούμε όμως πρέπει να δούμε κάποιους απαραίτητους ορισμούς.

Ορισμός 4.4.2 *Μία Μαρκοβιανή αλυσίδα με πίνακα μετάβασης P λέγεται μη περιοδική αν για κάθε κατάσταση x ισχύει $gcd(t : P^t(x,x) > 0) = 1$ δηλαδή δεν υπάρχει κατάσταση για την οποία να επιστρέφουμε στην ίδια μόνο με πλήθος βημάτων πολλαπλάσια ενός συγκεκριμένου αριθμού.*

Ορισμός 4.4.3 *Μία Μαρκοβιανή αλυσίδα με πίνακα μετάβασης P λέγεται αμείωτη αν για κάθε ζεύγος καταστάσεων (x,y) υπάρχει t ¿ 0 τω $P^t(x,y) > 0$ δηλαδή αν από οποιαδήποτε κατάσταση μπορείς να μεταβείς σε οποιαδήποτε άλλη - όχι απαραίτητα σε ένα βήα βέβαια.*

Μία Μαρκοβιανή αλυσίδα λέγεται εργοδική αν έχει και τις δύο παραπάνω ιδιότητες. Σε αυτή την περίπτωση ισχύει το εξής :

Θεώρημα 4.4.1 *Μία εργοδική Μαρκοβιανή αλυσίδα έχει μοναδική stationary κατανομή. Μάλιστ ισχύει ότι : $P^t(x,y) -> \pi(y), t -> \infty$ για όλα τα x.*

Αυτό σημαίνει πως μία εργοδική Μαρκοβιανή αλυσίδα , 'ξεχνάει' σταδιακά την αρχική της κατάσταση...

4.4.2 Markov Chain Monte Carlo Method

Χρησιμοποιώντας τις Μαρκοβιανές αλυσίδες μπορούμε να κατασκευάσουμε FPAUS για πολλά προβλήματα(Markov Chain Monte Carlo Method,MCMC). Η ιδέα είναι ότι κατασκευάζουμε μία εργοδική Μαρκοβιανή αλυσίδα η οποία έχει ως χώρο καταστάσεων το χώρο του προβλήματος και προσομοιώνουμε την λειτουργία της για ένα αρκετά μεγάλο αριθμό βημάτων.Μετά θεωρούμε ως αποτέλεσμα του sampling την τελική κατάσταση της αλυσίδας. Με δεδομένο οτι οι εργοδικές ΜΑ τείνουν προς την stationary κατανομή μετά από κάποιο χρονικό διάστημα προσομοίωσης μας εξασφαλίζει πως αν ορίσουμε κατάλληλα την ΜΑ έτσι ώστε να έχει μία επιθυμητή stationary κατανομή- π.χ ομοιόμορφη - μετά από κάποιο χρονικό διάστημα τα αποτελέσματα θα προκύπτουν με πιθανότητες πολύ κοντινές σε αυτή. Η κρίσιμη παράμετρος σε αυτή την διαδικασία είναι ο αριθμός των βημάτων που πρέπει να επιτρέψουμε στην προσομοίωση. Εμείς θέλουμε ο αριθμός αυτός να είναι μικρός σε σχέση με το μέγεθος του Ω,αλλιώς η διαδικασία δεν είναι αποδοτική. Αλλά, δεν μπορούμε να τον κάνουμε και πολύ μικρό γιατί τότε θα είμαστε αρκετά μακριά από την stationary κατανομή. Ο χρόνος - αριθμός βημάτων - που χρειάζεται μία ΜΑ για να φτάσει αρκετά κοντά στην stationary κατανομή τής ονομάζεται mixing time. Για την μελέτη και τον υπόλογισμό αυτού υπάρχουν διάφορες τεχνικές - coupling, canonical paths - πιο πολλές λεπτομέρειες για τα οποία μπορούν να βρεθούν στο [M.J96]. Αυτό στο οποίο εμείς θα περιοριστούμε μόνο να δούμε είναι ένα παράδειγμα ΜΑ για το πρόβλημα του #Matchings.

Παράδειγμα 4.4.1 *Έστω ένας γράφος G(V,E) και MA με Ω το σύνολο M(G) των ταιριασμάτων του G. Έστω μία αρχική κατάσταση $X_0 = M$. Τότε η επόμενη κατάσταση X_1 καθορίζεται ως εξής:*

1. *Με πιθανότητα 1/2 $X_1 = X_0$ και σταματάμε.*
2. *Διαφορετικά επιλέγουμε τυχαία μία ακμή από το σύνολο E και θεωρούμε το $M' = M \oplus \{e\}$ όπου $\oplus$ σημαίνει συμμετρική διαφορά.*
3. *Αν το M' είναι ταίριασμα τότε θέτουμε $X_1 = M'$ αλλιώς $X_1 = M$*

Κεφάλαιο 5

#PE και TotP

Όπως έχουμε ήδη δει υπάρχουν προβλήματα τα οποία είναι #P πλήρη υπό την Cook αναγωγή αλλά η αντίστοιχη εκδοχή τους σε πρόβλημα απόφασης είναι εύκολη. Έτσι μπορούμε να ορίσουμε μία υποκλάση του #P που να περιέχει αυτά ακριβώς τα προβλήματα. Έχουμε λοιπόν :

Ορισμός 5.0.4 *Η κλάση #PE είναι η κλάση που περιέχει όλες τις συναρτήσεις f για τις οποίες ισχύει :* $L_f = x|f(x) > 0$ *είναι στο P ενώ η f(x) είναι στο #P.*

Επίσης μπορούμε να ορίσουμε την κλάση TotP ως την κλάση των προβλημάτων για τα οποία υπάρχει NTM της οποίας ο συνολικός αριθμός μονοπατιών είναι ίσος με την τιμή της συνάρτησης. Δηλαδή :

Ορισμός 5.0.5 *Η κλάση TotP είναι η κλάση που περιέχει όλες τις συναρτήσεις f για τις οποίες υπάρχει πολυωνυμικού χρόνου NTM M τέτοια ώστε :* $f(x) = \#(pathsofMonx) - 1$.

Για τις κλάσεις αυτές ισχύει ότι $FP \subseteq TotP \subseteq PE \subseteq \#P$ όπου οι σχέσεις υποσυνόλου είναι γνήσιες εκτός και αν NP = P. Συνεπώς οι κλάσεις αυτές δεν είναι ισοδύναμες κατά Karp αν και είναι ισοδύναμες κατά Cook [AP06].

Όπως μπορούμε να δούμε αναλυτικά στο παραπάνω paper ένα πλήρες πρόβλημα για την κλάση TotP είναι το #PerfectMatchings (ή ισοδύναμα το πρόβλημα του permanent). Ακόμη μπορεί να αποδειχθεί ότι το TotP περιέχει ακριβώς τα προβλήματα του #PE τα οποία έχουν την παρακάτω ιδιότητα :

Ορισμός 5.0.6 *Μία συνάρτηση f λέγεται πολυωνυμικού χρόνου self-reducible εάν υπάρχουν πολυώνυμα r και q και υπολογίσιμες σε πολυωνυμικό χρόνο συναρτήσεις h, g και t τέτοιες ώστε για όλα τα* $x \in \{0,1\}$ *:*

$$f(x) = t(x) + \sum_{i=0}^{r(|x|} g(x,i)f(h(x,i))$$

, δηλαδή η f μπορεί να υπολογιστεί αναδρομικά με αναγωγή του x στο h(x,i) $(0 \leq i \leq r(|x|))$. *Βέβαια αυτή η αναδρομή θα πρέπει να τερματίζει μετά από έναν αριθμό το πολύ πολυωνυμικών βημάτων.*

Βέβαια, έννοια self-reducibility έχουμε ορίσει ξανά στο 4ο κεφάλαιο για σχέσεις. Το ζήτημα το οποίο προκύπτει είναι αν οι δύο έννοιες είναι ισοδύναμες. Είναι εύκολο να δούμε ότι αν μία σχέση είναι self-reducible με τον τρόπο που το ορίσαμε σε εκείνο το σημείο ορίζει τότε η αντίστοιχη $N_R(x)$ είναι self-reducible σύμφωνα με τον παραπάνω ορισμό. Το αντίστροφο δεν είναι τόσο απλό να δειχθεί ή να καταρριφθεί....

Βιβλιογραφία

[AP06] Stathis Zachos Aris Pagourtzis. The complexity of counting functions with easy decision version. *MFCS*, pages 741–752, 2006.

[C.H83] S.Zachos C.H.Papadimitriou. Two remarks on the power of counting. *Lecture Notes in Computer Science*, 145:269, 1983.

[D.Z96] D.Zuckerman. On unapproximable versions of np-complete problems. *SIAM Journal on Computing*, 25, 1996.

[J.K89] S.Toda J.Toran J.Köbler, U.Schöning. Turing machines with few accepting computationsand low sets for pp. *Proc. 4th IEEE Conference on Structure in Complexity Theory*, pages 208–215, 1989.

[J.S77] J.Simon. On the difference between one and many. *Lecture Notes in Computer Science*, 52:480–491, 1977.

[L.J77] L.J.Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

[LV86] V.V. Vazirani L.G. Valiant. Np is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

[MD04] Catherine Greenhill Mark Jerrum Martin Dyer, Leslie Ann Goldberg. The relative complexity of approximate counting. *Algorithmica*, 38:471–500, 2004.

[MJ86] Vijay Vazirani Mark Jerrum, Leslie Valiant. Random generation of combinatorial structures from a uniform distribution. *Theoretical Computer Science*, 43:169–188, 1986.

[M.J96] A. Sinclair M.Jerrum. The markov chain monte carlo method: an approach to approximate counting and integration. *Approximation Algorithms for NP-hard problems*, pages 482–520, 1996.

[ST92] Osamu Waranabe Seinosuke Toda. Polynomial-time 1-turing reductions from #ph yo #p. *Theoretical Computer Science*, 100:205–221, 1992.

[Sto85] Larry Stockmeyer. On approximation algorithms for #p. *SIAM Computing*, 14(4), November 1985.

[Tod91] Seinosuke Toda. Pp is as hard as the polynomial-time hierarchy. *SIAM Journal*, 20(5):865–877, October 1991.

[U.S89] U.Schöning. Probabilistic complexity classes and lowness. *J.Comput. System Sci.*, 39:84, 1989.

[Val] L.G. Valiant. The relative complexity of enumeration and reliability problems. *SIAM Journal of Computing*.

[Val79] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

Document powered by LaTeX