



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

**Ιδιότητες συναρτήσεων μέτρησης πλήθους λύσεων
σε προβλήματα με εύκολη απόφαση ύπαρξης λύσης:
πληρότητα, προσεγγισιμότητα,
μαρκοβιανές αλυσίδες, αλλαγές φάσης**

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ
της
Ελένης Μπακάλη

Επιβλέπων: Ευστάθιος Ζάχος, καθηγητής

Αθήνα, Δεκέμβριος 2018



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

**Ιδιότητες συναρτήσεων μέτρησης πλήθους λύσεων
σε προβλήματα με εύκολη απόφαση ύπαρξης λύσης:
πληρότητα, προσεγγισιμότητα,
μαρκοβιανές αλυσίδες, αλλαγές φάσης**

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

της
Ελένης Μπακάλη

Επιβλέπων: Ευστάθιος Ζάχος, καθηγητής

Εγκρίθηκε από την επταμελή επιτροπή:

| ΟΝΟΜΑΤΕΠΩΝΥΜΟ | ΒΑΘΜΙΑ | ΥΠΟΓΡΑΦΗ |
|---------------------------|-----------------------|----------|
| 1. Αριστείδης Παγουρτζής | αναπληρωτής καθηγητής | |
| 2. Δημήτριος Φωτάκης | αναπληρωτής καθηγητής | |
| 3. Νικόλαος Παπασπύρου | αναπληρωτής καθηγητής | |
| 4. Αντώνιος Συμβώνης | καθηγητής | |
| 5. Βασίλειος Ζησιμόπουλος | καθηγητής | |
| 6. Αλέξανδρος Αρβανιτάκης | επίκουρος καθηγητής | |
| 7. Ευάγγελος Μαρκάκης | επίκουρος καθηγητής | |

Αθήνα, Δεκέμβριος 2018

On properties of counting functions with easy
decision version: completeness, approximability,
Markov chains, phase transitions

Eleni Bakali

PhD thesis
NTUA

Athens, December 2018

Ευχαριστίες

Θα ήθελα πρώτα από όλα να ευχαριστήσω την συμβουλευτική μου επιτροπή κ. Στάθη Ζάχο, κ. Άρη Παγουρτζή και κ. Δημήτρη Φωτάκη για όλα όσα με δίδαξαν, και για την σημαντική καθοδήγηση και πολλαπλή υποστήριξη που μου προσέφεραν κατά την διάρκεια των σπουδών μου. Επίσης θα ήθελα να ευχαριστήσω τους φίλους και συμφοιτητές μου Αντώνη Αντωνόπουλο και Αγγέλα Χαλκή για την ουσιαστική ώθηση που μου προσέφεραν ώστε να ασχοληθώ με το συγκεκριμένο θέμα, και την γενικότερη συνεργασία τους μαζί μου, τον Πέτρο Πανταβό και τον Αλέξανδρο Αγγελόπουλο για τις συνεργασίες μας, τον Μανώλη Ζαμπετάκη για τις πολύ χρήσιμες συζητήσεις σε θέματα σχετικά με την διατριβή μου, το Γεράσιμο Παλαιοπάνο, την Ελένη Χάμου και το Λευτέρη Καραλέκα για τη βοήθειά τους στην επιμέλεια του κειμένου και τις διορθώσεις τους, το Θανάση Λιανέα και το Δημήτρη Σακαβάλα για τη βοήθεια με τις συμβουλές και την εμπειρία τους. Επίσης ευχαριστώ την επταμελή μου επιτροπή για τα σχόλια και τις διορθώσεις τους. Ακόμη ευχαριστώ τις γραμματείς της σχολής και κυρίως την κ.Κάντα για την άριστη εξυπηρέτηση που μου προσέφεραν. Πάνω απ' όλους ευχαριστώ την οικογένειά μου και τους φίλους μου που πάντα μου συμπαραστέκονται και με υποστηρίζουν.

Περίληψη

Η κλάση πολυπλοκότητας #P είναι η κλάση συναρτήσεων που η τιμή τους αντιστοιχεί στο πλήθος των λύσεων σε προβλήματα των οποίων το αντίστοιχο πρόβλημα απόφασης ύπαρξης λύσης είναι στο NP, π.χ. η #SAT είναι η συνάρτηση που αντιστοιχίζει κάθε λογικό τύπο ϕ στον αριθμό των ικανοποιητικών αναθέσεων του ϕ . Το πλήθος των λύσεων για NP-πλήρη προβλήματα είναι δύσκολο να υπολογιστεί, αλλά υπάρχουν επίσης δύσκολα προβλήματα καταμέτρησης, για τα οποία το αντίστοιχο πρόβλημα απόφασης ύπαρξης λύσης είναι στο P, δηλαδή εύκολο. Η TotP είναι μια υποκλάση της #P που περιέχει όλα τα αυτοαναγωγίμα προβλήματα καταμέτρησης με εύκολη απόφαση ύπαρξης λύσης. Περιέχει πολλά ενδιαφέροντα προβλήματα από πολλές επιστημονικές περιοχές.

Οι Cook αναγωγές θολώνουν πολλές δομικές διαφορές μεταξύ των προβλημάτων καταμέτρησης, π.χ. η συνάρτηση PERMANENT είναι #P-πλήρης, αλλά ανήκει επίσης στην TotP. Επομένως απαιτούνται αυστηρότερες αναγωγές προκειμένου να χαρακτηριστεί πλήρως η πολυπλοκότητα ενός προβλήματος καταμέτρησης: οι λεγόμενες φειδωλές (parsimonious) αναγωγές, οι οποίες έχουν την ιδιότητα να διατηρούν ακριβώς τις τιμές των συναρτήσεων που ανάγεται η μία στην άλλη, ή αλλιώς διατηρούν το πλήθος των λύσεων των αντίστοιχων προβλημάτων. Η ύπαρξη TotP -πλήρων προβλημάτων κάτω από φειδωλές αναγωγές ήταν ένα ανοιχτό πρόβλημα εδώ και δέκα περίπου χρόνια. Ο πρώτος σκοπός αυτής της εργασίας είναι να παρουσιάσει τα πρώτα τέτοια προβλήματα (κεφάλαιο 2). Αυτά τα προβλήματα σχετίζονται με την ικανοποιησιμότητα Boolean κυκλωμάτων (συγκεκριμένα το #tree-monotone-circuit-SAT) και τύπων (συγκεκριμένα το #clustered-monotone-SAT ή #CM-SAT) και με το πρόβλημα της εκτίμησης του μεγέθους του δέντρου μιας backtracking διαδικασίας (συγκεκριμένα το Size-of-Subtree).

Ένα σημαντικό θεώρημα που αποδεικνύουμε στο κεφάλαιο 2 είναι ότι το #SAT ανάγεται στο #CM-SAT υπό αναγωγές που διατηρούν την προσεγγισιμότητα. Η δειγματοληψία και η προσεγγιστική μέτρηση πραγματοποιούνται συνήθως με τη χρήση μαρκοβιανών αλυσίδων, οι οποίες πρέπει να είναι εργοδικές (δηλαδή μη αναγώγιμες και απεριοδικές), προκειμένου να λειτουργούν σωστά οι αντίστοιχοι αλγόριθμοι. Ωστόσο, για το #SAT είναι γνωστό ότι δεν μπορούμε να σχεδιάσουμε μη αναγώγιμες μαρκοβιανές αλυσίδες, των οποίων ο χώρος καταστάσεων να είναι το σύνολο ικανοποιητικών αναθέσεων ενός τύπου που δίνεται ως είσοδος, εξαιτίας ενός φαινομένου διασκορπισμού του συνόλου των λύσεων. Αντίθετα, το σύνολο των λύσεων του #CM-SAT, καθώς και του Size-of-Subtree, συνδέεται με έναν συ-

γκεκριμένο τρόπο που επιτρέπει το σχεδιασμό μη αναγώγιμων μαρκοβιανών αλυσίδων.

Στο κεφάλαιο 4 σχεδιάζουμε και μελετάμε μερικές μαρκοβιανές αλυσίδες, των οποίων ο χώρος καταστάσεων είναι το σύνολο των λύσεων των παραπάνω προβλημάτων. Αναλύουμε το χρόνο σύγκλισης, τις στάσιμες κατανομές τους και την πολυπλοκότητα υπολογισμού των συντελεστών κανονικοποίησης, όπως και του μεγέθους του στηρίγματος των στάσιμων κατανομών. Τα κύρια αποτελέσματα της μελέτης μας είναι καταρχάς ότι το SAT ανάγεται στον υπολογισμό του συντελεστή κανονικοποίησης των στάσιμων κατανομών κάποιων μαρκοβιανών αλυσίδων, οι οποίες ανήκουν σε μια οικογένεια που σχεδιάζουμε. Με άλλα λόγια, ο υπολογισμός του συντελεστή κανονικοποίησης αυτών των κατανομών είναι δύσκολος εκτός αν $NP=P$. Δεύτερον, ο συντελεστής κανονικοποίησης αυτών των κατανομών μπορεί να προσεγγιστεί με FPRAS (δηλ. με ένα αυθαίρετα μικρό πολλαπλασιαστικό σφάλμα σε πολυωνυμικό χρόνο).

Παρατηρούμε στη συνέχεια ένα ενδιαφέρον φαινόμενο. Στο κεφάλαιο 4 για κάθε είσοδο σε ένα πρόβλημα στην TotP θεωρήσαμε δύο διαφορετικές μαρκοβιανές αλυσίδες που συγκλίνουν σε δύο διαφορετικές κατανομές P_1, P_2 , με συντελεστές κανονικοποίησης Z_1, Z_2 αντίστοιχα. Στο κεφάλαιο 5 δείχνουμε ότι μπορούμε να γενικεύσουμε τις δύο παραπάνω κατανομές πιθανότητας με ένα ενιαίο μοντέλο $P(\lambda)$, $\lambda \in \mathbb{R}_{>0}$, έτσι ώστε $P(1) = P_1$ και $P(2) = P_2$. Αυτό το μοντέλο παρουσιάζει εντελώς διαφορετική συμπεριφορά για $\lambda = 1$ και $\lambda = 2$: Και για τα δύο $\lambda = 1$ και $\lambda = 2$, ο υπολογισμός του Z_λ είναι δύσκολος ($\#P$ -πλήρης), αλλά για $\lambda = 1$ έχουμε

- εκθετικό χρόνο σύγκλισης της αντίστοιχης μαρκοβιανής αλυσίδας
- αδυναμία ύπαρξης FPRAS για το Z_1 εκτός $NP = RP$.

και για $\lambda = 2$ έχουμε

- πολυωνυμικό χρόνο σύγκλισης της αντίστοιχης μαρκοβιανής αλυσίδας
- FPRAS για το Z_2 .

Το ερώτημα που τίθεται είναι τι ισχύει για τις υπόλοιπες τιμές του $\lambda > 0$. Σχεδιάζουμε (στο κεφάλαιο 5) μια μαρκοβιανή αλυσίδα, παραμετροποιημένη από το λ , που γενικεύει τις δύο διαφορετικές μαρκοβιανές αλυσίδες που μελετήθηκαν στο κεφάλαιο 4. Αυτή η μαρκοβιανή αλυσίδα M_λ ακολουθεί τον κανόνα του Metropolis και συγκλίνει στην κατανομή $P(\lambda)$.

Δείχνουμε ότι υπάρχει αλλαγή φάσης ως προς τον χρόνο σύγκλισης της M_λ συναρτήσει του λ . Συγκεκριμένα, υπάρχει μια ασυνεχής μετάβαση από εκθετικό σε πολυωνυμικό χρόνο σύγκλισης για λ που εξαρτάται από το δέντρο. Για το πλήρες δέντρο, όπως και για τα δέντρα που αποτελούν δύσκολα στιγμιότυπα του προβλήματος Size-of-Subtree, η αλλαγή φάσης είναι στο $\lambda = 2$, ενώ για το μονοπάτι (το οποίο βρίσκεται στον αντίποδα του πλήρους δέντρου) η αλλαγή φάσης είναι στο $\lambda = 1$. Επίσης αποδεικνύουμε ότι υπάρχει αλλαγή φάσης για την πολυπλοκότητα

του προβλήματος από δύσκολα προσεγγίσιμο (NP-hard to approximate) σε προσεγγίσιμο με FPRAS για κάποιο $\lambda \in [1, 2]$.

Μια παράλληλη κατεύθυνση αυτής της διατριβής αφορά την προσέγγιση των συναρτήσεων στην TotP. Παρατηρούμε ότι FPRAS για όλα τα προβλήματα στην TotP είναι εφικτό αν και μόνο αν $NP = RP$. Το ίδιο είναι γνωστό ότι ισχύει και για τη #P. Ωστόσο, στο κεφάλαιο 3 δείχνουμε ότι μπορούμε να έχουμε κάποια καλύτερα αποτελέσματα προσέγγισης για την TotP σε σχέση με τα αντίστοιχα που ισχύουν για την #P. Πρώτον, για κάθε πρόβλημα στην TotP, αν ο αριθμός λύσεων είναι x , μπορούμε να υπολογίσουμε ακριβώς αυτόν τον αριθμό σε χρόνο $x \cdot poly(n)$, όπου n είναι το μέγεθος της εισόδου. Με άλλα λόγια, αν ο αριθμός των λύσεων είναι πολυωνυμικός (δηλαδή μικρός), μπορούμε να τις μετρήσουμε ακριβώς σε πολυωνυμικό χρόνο. Δεύτερον, αν ο αριθμός των λύσεων είναι $2^n/x$, μπορούμε να έχουμε RAS (δηλαδή αυθαίρετα μικρό πολλαπλασιαστικό σφάλμα) σε χρόνο $poly(n, x)$. Με άλλα λόγια, εάν ο αριθμός των λύσεων είναι $2^n/poly(n)$ (δηλαδή μεγάλος), μπορούμε να έχουμε FPRAS. Τρίτον, αν συνδυάσουμε τα παραπάνω αποτελέσματα με το γνωστό γεγονός ότι όλα τα προβλήματα στην #P επιδέχονται μια προσθετικού σφάλματος προσέγγιση, παίρνουμε καλύτερα εκθετικού χρόνου αλγοριθμικά αποτελέσματα για την TotP από τα αντίστοιχα γνωστά αποτελέσματα για την #P. Παραμένει ανοιχτό το ερώτημα εάν αυτά τα αποτελέσματα είναι βέλτιστα υπό μια fine-grained οπτική πολυπλοκότητας (δηλ. υπό κάποια παραδοχή ανάλογη με την SETH, η οποία δηλώνει χονδρικά ότι το SAT χρειάζεται για να λυθεί χρόνο $\Theta(2^n)$).

Επίσης αφού παρατηρούμε ότι το TotP-πλήρες πρόβλημα Size-of-Subtree είναι εύκολο να προσεγγιστεί σε πολλές περιπτώσεις, στο ίδιο κεφάλαιο προσδιορίζουμε μια οικογένεια δέντρων για την οποία αποδεικνύουμε ότι περιέχει δύσκολα στιγμιότυπα του προβλήματος.

Το τελευταίο θέμα που εξετάζει αυτή η διατριβή (στο κεφάλαιο 3) αφορά στη σχέση της TotP με την κλάση προβλημάτων που επιδέχονται FPRAS. Όπως αναφέραμε ήδη, $NP=RP$ αν και μόνο αν όλα τα προβλήματα στην TotP επιδέχονται FPRAS. Αφού το NP vs. RP είναι ένα από τα σημαντικότερα προβλήματα της θεωρητικής πληροφορικής, το ίδιο ισχύει άρα και για το TotP vs. FPRAS, για αυτό και το μελετούμε. Μια διαισθητική πεποίθηση πολλών επιστημόνων είναι ότι τα μόνα προβλήματα στην #P που μπορεί να έχουν FPRAS ανήκουν στην TotP, και δεν υπάρχουν ως τώρα γνωστά αντιπαραδείγματα σε αυτή την εικασία. Αποδεικνύουμε ότι αυτή η πεποίθηση είναι λάθος εκτός εάν $P = RP$. Προκειμένου να το δείξουμε αυτό, εισάγουμε δύο νέες κλάσεις πολυπλοκότητας #RP1 και #RP2 με τη βοήθεια των οποίων το αποτέλεσμα προκύπτει εύκολα. Δείχνουμε επίσης ότι η κλάση των προβλημάτων που επιδέχονται FPRAS βρίσκεται μεταξύ αυτών των δύο κλάσεων και ότι αυτές οι κλάσεις δεν συμπίπτουν εκτός αν $NP = RP$. Τέλος, για να αποκτήσουμε μια πιο ξεκάθαρη εικόνα των σχέσεων των παραπάνω κλάσεων με την #P και την TotP (και με μερικές άλλες σχετικές κλάσεις), μελετάμε τους εγκλεισμούς μεταξύ τους και παρουσιάζουμε τους τέσσερις δυνατούς κόσμους σε σχέση με τα προβλήματα NP vs. RP και RP vs. P .

Abstract

The complexity class $\#P$ is the class of functions that count the number of solutions to problems in NP, e.g. $\#SAT$ is the function that given as input a formula ϕ returns the number of satisfying assignments of ϕ . NP-complete problems are hard to count, but there exist hard counting problems with decision version in P. TotP is a subclass of $\#P$ that contains all self-reducible problems with easy decision version. It contains many interesting problems from many scientific areas.

Cook reductions blur structural differences between counting problems, e.g. the PERMANENT is $\#P$ complete, but it also belongs to TotP, thus stricter reductions are needed in order to fully characterize the complexity of a counting problem; the so called parsimonious reductions, which are those that preserve exactly the values of the functions. The existence of TotP-complete problems under parsimonious reductions (besides the generic one), was an open question. The first purpose of this thesis is to present the first such problems (chapter 2). These problems are related to satisfiability of Boolean circuits (namely $\#tree\text{-monotone-circuit-SAT}$) and formulas (namely the clustered monotone SAT, or $\#CM\text{-SAT}$), and to the problem of estimating the size of a backtracking tree (namely the Size-of-Subtree problem).

An important theorem that we prove is that $\#SAT$ reduces to $\#CMSAT$ under approximation preserving reductions. Sampling and approximate counting are usually performed with the use of Markov chains. However for $\#SAT$ it is known that we cannot design irreducible Markov chains whose state space is the set of satisfying assignments of an input formula, due to a shattering phenomenon of the set of solutions. On the contrary, the set of solutions of $\#CM\text{-SAT}$, as well as of Size-of-Subtree, is connected in a particular way that permits the design of irreducible Markov chains.

In chapter 4 we design and study some Markov chains whose state space is the set of solutions of the above problems. We analyse their mixing time, their stationary distributions, the complexity of computing the normalizing factors and the complexity of computing the size of the support of the stationary distributions. The main results of our study is firstly that $\#SAT$ is reduced to the computation of the normalizing factor of the stationary distribution of a family of Markov chains that we design. In other words, the computation of this normalizing factor is $\#P$ -complete. Secondly this normalizing factor can be approximated with FPRAS, (i.e. with an arbitrarily small multiplicative error in polynomial time). It remains an open

question whether this normalizing factor can be computed either exactly or with a small absolute error. However we show that the latter is impossible unless $\text{NP}=\text{RP}$.

We then observe an interesting phenomenon. For every input to a problem in TotP we considered two different Markov chains that converge to two different stationary distributions P_1, P_2 , with normalizing factors Z_1, Z_2 respectively. In chapter 5 we show that we can generalize the above two probability distributions by a single model $P(\lambda)$, $\lambda > 0$, so that $P(1) = P_1$ and $P(2) = P_2$. This model exhibits a completely different behaviour for $\lambda = 1$ and $\lambda = 2$: For both $\lambda = 1$ and $\lambda = 2$, the computation of Z_λ is hard ($\#P$ -complete), but for $\lambda = 1$ we have

- exponential mixing time of the respective Markov chain
- impossibility of FPRAS for Z_1 unless $\text{NP}=\text{RP}$.

and for $\lambda = 2$ we have

- polynomial mixing time of the respective Markov chain
- FPRAS for Z_2 .

The question that arises is what happens for the other values of $\lambda > 0$. We design (in chapter 5) a Markov chain, parametrized by λ , that generalizes the two different Markov chains studied in chapter 4. This Markov chain M_λ follows the Metropolis rule, and converges to the probability distribution $P(\lambda)$.

We show that a phase transition occurs to the running time of M_λ with respect to λ . In particular there is a discontinuous transition from polynomial to exponential mixing time for $\lambda \in [1, 2]$ that depends on the input tree. The complexity of computing Z_λ also exhibits a phase transition from NP-hard to approximate to approximable with FPRAS for $\lambda \in [1, 2]$.

A parallel direction of this thesis concerns the approximability of functions in TotP. It is known that FPRAS for all problems in TotP is possible if and only if $\text{NP}=\text{RP}$. The same holds for $\#P$. However in chapter 3 we show that we can have some better results for TotP than for $\#P$. Firstly, for any instance to any problem in TotP, if the number of solutions is x , we can exactly compute this number in time $x \cdot \text{poly}(n)$; where n is the size of the input. In other words, if the number of solutions is polynomial (i.e. small), we can count them exactly in polynomial time. Secondly if the number of solutions is $2^n/x$, we can have a RAS (i.e. arbitrarily small multiplicative error) in time $\text{poly}(n, x)$: In other words, if the number of solutions is $2^n/\text{poly}(n)$ (i.e. big), we can have an FPRAS. Thirdly if we combine the above results with the known fact that all problems in $\#P$ admit an additive approximation, we get better exponential time algorithmic results for TotP than the corresponding known results for $\#P$. It remains an open question whether these results are optimal under a fine grained complexity perspective (i.e. under some assumption analogous to the SETH, which roughly states that SAT needs $\Theta(2^n)$ time to be solved).

Also after observing that the TotP-complete problem Size-of-Subtree problem is easy to approximate on many instances, in the same chapter we identify a family of trees that we prove to contain difficult instances of the problem.

The last issue that this thesis deals with, (in chapter 3), concerns an intuitive belief of many scientists that the only problems in #P that can have an FPRAS belong to TotP, and no counterexamples to this conjecture are known. We prove that this is wrong unless $P=RP$. In order to show that, we introduced two new complexity classes #RP1 and #RP2, both being counting versions of RP. We also show that the class of problems that admit FPRAS lies between these two classes, and that these classes do not coincide unless $NP=RP$. Finally, in order to get a more clear picture of the relationships of the above classes with #P and TotP (and some other related classes), we study inclusions between them and present all four possible worlds with respect to the NP v.s. RP, and RP v.s. P questions.

Extended abstract

Introduction

In the field of Counting Complexity we study functions that count the number of solutions to a decision problem, i.e. their values on an instance that is given as input, is equal to the number of solutions for that instance. For example take the decision problem SAT, which is the problem that has as input a logical formula, and as output the decision of whether a satisfying assignment exists to that formula or not. The counting version of SAT is #SAT, which is the problem of counting the number of satisfying assignments to a given logical formula.

If a decision problem is in NP, then its counting version is in a class called #P. If a decision problem is hard, then its counting version is also hard. However, there exist #P-complete problems with decision version in P, e.g. #DNF: the function that counts the number of satisfying assignments to a formula in disjunctive normal form, #perfect matchings: the function that counts the number of perfect matchings of a bipartite graph. A less trivial example is the (0,1)-PERMANENT: the function that is equal to the permanent of a given matrix with entries 0 or 1. The latter has easy decision version since it is equivalent to #perfect matchings. Note that in this case the decision version corresponds to the problem of deciding whether the permanent of a given matrix is non-zero.

#P, #PE, TotP

In terms of Turing machines, #P is the class of functions whose value on any input equals the number of accepting paths of a non deterministic Turing machine of polynomial time (NPTM) on the same input. For example it contains #SAT and #k-colorings.

Another class, called TotP, is the class of functions whose values on an input equals the number of all paths of an NPTM – 1, on the same input, which equivalently equals the number of branchings of a binary NPTM on the same input. For example it contains #IS, which is the problem of counting the number of independent sets of all sizes of a graph given as input, and #perfect matchings.

#PE is the class of all functions in #P with decision version in P. For example it contains #Divisors, which is the problem of counting the number of divisors of a natural number given as input.

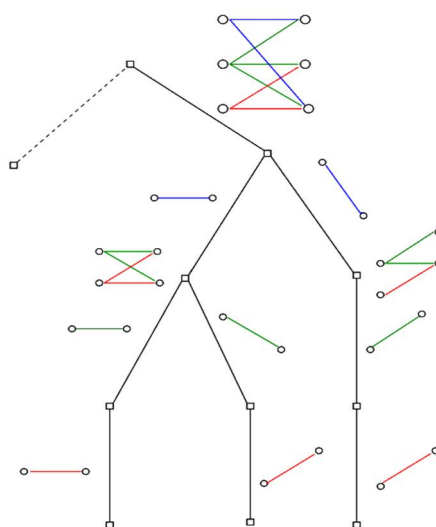
The important theorem about TotP is that it is exactly the Karp-closure of all self-reducible functions in #P with decision version in P [62]. This fact is important because #PE is a class with a semantic characterization, and this theorem provides a syntactic characterization to at least a large and important subclass of #PE, containing all self-reducible functions of it.

Many interesting problems from many scientific fields belong to #PE and TotP, e.g. counting matchings, computing the permanent as we already mentioned, computing the partition function of several models from statistical physics, like the Ising model, the hard-core model and the monomer-dimer model, counting k -colorings of a given graph when the number of colours is greater than the maximum degree of the graph, counting bases of a matroid, computing the volume of a convex body, counting independent sets of all sizes of a given graph, and many more.

Many complexity classes from the literature are subsets of #PE and TotP, e.g. classes of interval size functions: IF_t^{LN} , IF_t^{rmed} , $IF_p^<$, etc. [39, 13], descriptive complexity classes: # $\Sigma 1$, # $R\Sigma 2$, etc. [66, 8], logarithmic space classes: SpanL [6].

In order to better understand the definition of TotP, we give an example showing that #perfect matchings \in TotP.

Consider a bipartite graph G . We first construct an NPTM M such that its computational paths of M are in one to one correspondence with the perfect matchings of G . The NPTM starts with a node u and checks for every edge e incident to u whether a perfect matching exists that contains e . If the answer is positive for more than one incident edges, it proceeds non-deterministically by choosing one of them and then repeats the same procedure with the remaining graph. The important observation is that the existence check can be done in polynomial time. In the end there is exactly one computational path for every perfect matching. In order to satisfy the definition of TotP, we add a dummy path in the beginning of the computation.



Overview

We focus on the complexity class TotP. Our contribution is summarized in the following list.

- Completeness
 - first TotP-complete problems under parsimonious reductions
- Approximability
 - instances with too few or too many solutions are easy
 - family of hard instances
 - exponential time results for TotP, better than the corresponding results for #P
 - $\text{TotP} \subseteq \text{FPRAS}$ iff $\text{NP}=\text{RP}$
 - $\text{FPRAS} \not\subseteq \text{TotP}$ unless $\text{RP}=\text{P}$
- Markov Chains
 - design of rapidly mixing Markov chains for TotP-complete problems
 - stationary distribution $P_S(v) = \frac{w_S(v)}{Z_S}$, where S is the input tree, $v \in V(S)$, $w_S(v) = 2^{n-\text{depth}(v)}$ and $Z_S = \sum_{u \in S} w_S(u)$
 - complexity of Z_S
 - no exact computation unless $\text{NP}=\text{RP}$
 - FPRAS
- Phase transitions
 - Generalized model $Z_\lambda^S = \sum_{u \in S} w_\lambda^S(u)$, $P_\lambda^S(v) = \frac{w_\lambda^S(v)}{Z_\lambda^S}$, where S is the input tree, $\lambda > 0$, $v \in V(S)$ and $w_\lambda^S(v) = \lambda^{n-\text{depth}(v)}$
 - analysis of mixing time of Metropolis type Markov chain
 - phase transition at $\lambda \in [1, 2]$
 - complexity of Z_λ^S
 - exact computation is hard
 - approximability: phase transition at $\lambda \in [1, 2]$
 - sampling \Rightarrow FPRAS
 - modification of the model
 - hard to approximate for all $\lambda > 0$
 - sampling $\not\Rightarrow$ FPRAS

TotP-completeness

The problem

There are (at least) two types of reductions between counting problems, the Cook reductions, also called Turing reductions, and the Karp reductions, also called many-one or parsimonious reductions.

A function f is reduced to g under Cook/Turing reductions ($f \leq_T^p g$) if $f \in FP^g$. In other words, f can be computed in polynomial time using oracle calls to g .

A function f is reduced to g under Karp/many-one/parsimonious reductions ($f \leq_m^p g$) if $\exists h \in FP, \forall x \in \Sigma^* f(x) = g(h(x))$. In other words, parsimonious reductions preserve exactly the number of solutions between the two involved counting problems.

Cook reductions blur structural differences between counting classes. For example (0,1)-PERMANENT is #P-complete, but it is also TotP-complete under Cook reductions. So more strong reductions, like the parsimonious ones, are needed to fully classify a counting problem and to find a representative problem that characterizes the complexity of a counting class.

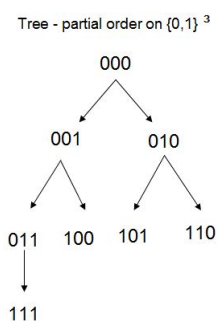
No TotP-complete problems under parsimonious reductions were known before this thesis.

Contribution

We present the first TotP-complete problems under parsimonious reductions. Those problems are #tree-monotone Circuit Sat, Size of maximum accepting down-set, Size-of-Subtree versions 1 and 2, and #Clustered monotone SAT.

#tree-monotone Circuit Sat

Consider the tree-partial-order (\leq_{tpo}) on $\{0, 1\}^n$. It is the partial order that results if we label the nodes of a full complete binary tree in the breadth first search order (bfs) and represent the labels by their n -bit binary representation.



A circuit C is monotone with respect to \leq_{tpo} if it reverses the inequality, i.e. if $x \leq_{tpo} y \Rightarrow C(x) \geq C(y)$.

- **Input:** C monotone with respect to \leq_{tpo}
- **Output:** the number of satisfying assignments

Size of Maximum Accepting Downset

Consider the tree-partial-order on $\{0, 1\}^n$, as described before.

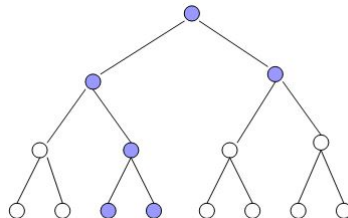
A downset of a partially ordered set is an upwards closed set. In other words if S is a set and \leq_p is a partial order on S , then D is a downset with respect to \leq_p if $\forall y, z \in S$ if $z \in D$ and $y \leq_p z$ then $y \in D$.

An accepting set for a circuit C is a subset of its satisfying assignments

- **Input:** arbitrary circuit C
- **Output:** the size of the maximum accepting downset with respect to \leq_{tpo} .

Size-of-Subtree - version 1

Consider the full complete binary tree T , of height n . Let $S \subseteq T$ be a subtree containing the root of T .

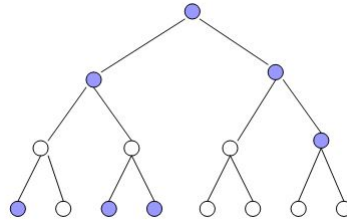


A succinct representation of S is a $poly(n)$ computable predicate $R : V(T) \rightarrow \{0, 1\}$ s.t. $R(v) = 1$ iff $v \in S$.

- **Input:** S in succinct representation
- **Output:** size of S

Size-of-Subtree - version 2

Consider the full complete binary tree T , of height n . Let S be an arbitrary subset of $V(T)$, not necessarily a tree, unlike version 1.

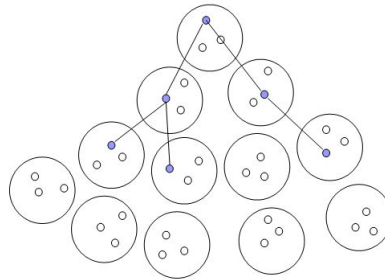


A succinct representation of S is a $poly(n)$ computable predicate $R : V(T) \rightarrow \{0, 1\}$ s.t. $R(v) = 1$ iff $v \in S$.

- **Input:** S in succinct representation
- **Output:** size of maximum connected subset of S containing the root of T .

#Clustered Monotone SAT (or #CM-SAT)

Consider the partition of $\{0, 1\}^n$ into clusters, such that each cluster contains all assignments with the first k variables fixed to specific values.



- **Input:** k , formula φ such that
 1. there is at most one solution (i.e. satisfying assignment) in each cluster
 2. There is a tree of $poly(n)$ height connecting the solutions such that it is
 - easy to find a solution if it exists
 - easy to find the neighbours of any solution
- **Output:** the number of solutions

In fact the tree connecting the solutions can be obtained if we consider the tree-partial-order on $\{0, 1\}^k$. Remember that each cluster contains all assignments that have their first k variables fixed to some particular values. If we label each cluster with the binary string formed by the concatenation of these k fixed values, then the tree-partial-order on the labels gives a tree connecting the clusters. See the full text of the thesis for an algorithm that finds the solution in each cluster (or reports that a solution does not exist).

Note To avoid misunderstanding, what we prove is that for any function f in TotP and every input x for f , we can construct in polynomial time a formula with the aforementioned properties. Therefore the problem #Clustered Monotone Sat is TotP-complete. Moreover the reduction is parsimonious.

The same comment holds for all of the problems that we presented in this section.

Implications

The problem Size-of-Subtree, also known as the backtracking tree estimation problem, is a well known problem studied from many perspectives, with good algorithms that succeed in practical cases and in special cases, see e.g. [51, 65, 21, 50, 15, 7]. However until now its worst case complexity was unknown (except for [71] where its complexity is studied under a model of computation not equivalent to the Turing machine). Since we prove Size-of-Subtree to be TotP-complete under Karp reductions, and since PERMANENT is #P-complete under Cook reductions, and #IS is #P-complete under approximation preserving reductions, and both these two problems belong to TotP, we get the following corollaries.

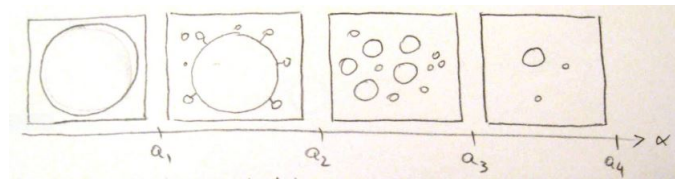
- **Corollary:** Size-of-Subtree is #P-complete under
 - Cook reductions (via PERMANENT)
 - Approximation preserving (or AP) reductions (via #IS)
- **Corollary:** Size-of-Subtree is not exactly computable in polynomial time unless PH=P, and it is inapproximable in polynomial time unless NP=RP.

Moreover it is known that Size-of-Subtree is average case easy to approximate if we consider certain probabilistic models of the problem [29, 75], which leads us to the following conclusion.

Conclusion: #SAT which is thought to be average case hard to approximate, is AP-reduced (via #IS) to a problem whose average case is easy to approximate. This means that the approximation preserving reductions do not preserve the probability mass between the instances of the two involved problems. In other words, the *many* hard instances of the first problem might be reduced to the *few* hard instances of the second one.

Another implication of our results is related to the study of random SAT and the reason of failure of algorithms for SAT based on Markov chains.

From the study of random SAT we know the following. If we consider typical random CNF formulas of density a (where $a = \text{\#clauses}/\text{\#variables}$), as we increase the density, we observe the following phenomenon.



First of all the number of solutions gradually decreases.

For $a > a_2$ the solution space shatters to a large number of clusters of fixed variables [53, 2], so that

- it is hard to find even one solution for the formula
- given any cluster it is hard to find any other

This shattering phenomenon is the reason of failure of the already known algorithms for SAT based on Markov chains, because this shattering translates to ergodicity breaking of these Markov chains [5], since the state space of these Markov chains is not connected.

Since we prove #CM-SAT to be TotP complete under parsimonious reductions, with the same reasoning as for Size-of-Subtree we conclude to the following corollaries.

- **Corollary:** #CM-SAT is #P-complete under
 - Cook reductions (via PERMANENT)
 - AP reductions (via #IS)
- **Corollary:** #CM-SAT is not exactly computable in polynomial time unless PH=P, and it is inapproximable in polynomial time unless NP=RP.

However #CM-SAT has a connected space of solutions, contrary to #SAT, which leads us to the the following conclusions.

Conclusion: #SAT whose typical hard instances have a disconnected space of solutions, thus not allowing the design of ergodic Markov chains, is reduced under AP-reductions to #CM-SAT, all formulas of which, have a connected space of solutions, permitting the design of ergodic Markov chains. This means that the current knowledge is not sufficient to explain the hardness of #SAT any more. We discovered a new topology under which ergodic Markov chains are possible. New Markov chains and algorithms are needed to be studied for #SAT through #CM-SAT. New hardness explanations are needed.

Approximability

Problem 1

It is known as a Corollary from [71] that $NP=RP \Leftrightarrow \#P \subseteq \text{FPRAS}$ and it is easy to see that the same holds for TotP, i.e. regarding FPRAS the following holds.

Theorem:(Corollary of [71]) $NP=RP \Leftrightarrow \#P \subseteq FPRAS \Leftrightarrow TotP \subseteq FPRAS$.

A question that concerns us is the approximability of problems in TotP in time more than polynomial, or with error greater than polynomial. Especially we are concerned with the exponential time complexity of approximating functions in TotP, and in particular we are interested in the comparison with the exhaustive search algorithm.

Contribution

We prove the following.

Theorem: for every $f \in TotP$

- Small instances are easy:
if $f(x) = s(|x|)$ then we have exact computation in time $s(n)poly(n)$.
Proof: traverse the tree exhaustively
- Large instances are easy:
if $f(x) = \frac{2^n}{s(n)}$ then we have RAS in time $s(n)poly(n, \epsilon^{-1})$.
Proof: simple sampling is unbiased estimator

In other words, if the value of the function (or equivalently the number of solutions) is polynomial, i.e small, we can compute it exactly in polynomial time. Also if the value of the functions is 2^n over some polynomial, i.e. large, we can approximate it in polynomial time.

Combining the above we get the following.

Theorem: For every $f \in TotP$ we have approximation algorithms

- with absolute error $2^{(\beta+1)n/2}$ in time $2^{(1-\beta)n}poly(n), \forall \beta \in (0, 1)$
- RAS in time $(2^{(\beta+1)n/2} + 2^{(1-\beta)n})poly(n), \forall \beta \in (0, 1)$
- RAS in time $O(2^{2n/3}\epsilon^{-2}poly(n))$

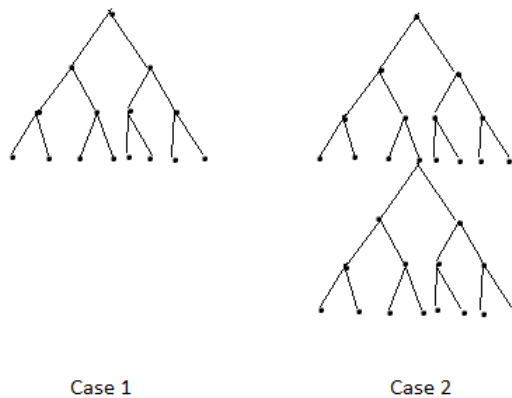
Conclusions: Every function in TotP can be approximated using algorithms that run faster than the exhaustive search algorithm, and also faster than the better algorithms that approximate functions in #P.

Problem 2

Since, as we already mentioned, the problem Size-of-Subtree can be approximated on many special instances, the question is whether we can characterize a family of hard instances.

Contribution

We identify a family of hard instances for the TotP-complete problem Size-of-Subtree: the so called Christmas-trees. This family of trees contains all full complete binary trees, and all trees that consist of a full complete binary tree of height n , from a leaf of which is hanging another full complete binary tree of the same height n , for all n .



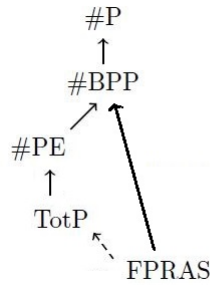
Theorem: If an upper bound of the height of the tree is given, we cannot approximate the size of Christmas-trees (given in succinct representation).

Proof sketch: We map unsatisfiable formulas to trees of case 1, and uniquely satisfiable formulas to trees of case 2. If we could approximate Christmas-trees, we could distinguish between case 1 and 2, and thus solve USAT.

Problem 3

Finally regarding the relationship between TotP and the class of counting problems that admit an FPRAS, there is an intuitive belief (conjecture) expressed in many texts (in words) that $\text{FPRAS} \subset \text{TotP}$ (e.g. in [9] chapter 17, [34] chapter 6.2, [8] pp. 7-8), and there are no known counterexamples to this conjecture. All problems for which an FPRAS is known belong to TotP and all subclasses of #P for which FPRAS is known to exist are subclasses of TotP.

The world of inclusions inside #P was thought to be as in the following figure, where the arrows denote set inclusions.



Contribution

We prove the following.

Theorem: The conjecture is wrong unless $RP=P$.

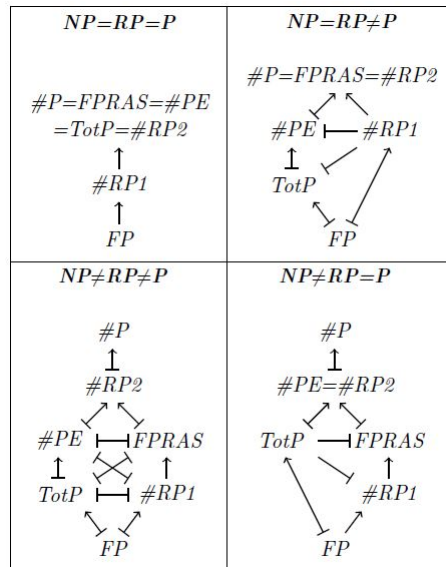
In order to prove that, we introduce a new class #RP1 which we proved to be a subset of FPRAS. For every problem $A \in RP$ there is a function $f_A \in \#RP1$ having as decision version the problem A . Thus if $FPRAS \subseteq TotP$ then $\#RP1 \subseteq TotP$ and thus A should be in P , since the decision version of any problem in $TotP$ is in P . Thus $RP=P$.

We also mention that in the course of proving the above, another class also occurred that we denote #RP2, because it also has functions with decision version in RP .

We prove that $\#R1 \subseteq FPRAS \subseteq \#R2$ and that $\#R1 \neq \#R2$ unless $NP=RP$.

Finally we present all four possible worlds inside #P, with respect to NP vs. RP and RP vs. P .

In the next figure $A \rightarrow B$ denotes $A \subseteq B$, $A \dashv B$ denotes $A \not\subseteq B$, and $A \mapsto B$ denotes $A \subsetneq B$.



Markov chains

A Markov chain over a set \mathcal{X} is a stochastic process $\{X_n\}_{n \in \mathbb{N}}$ such that $\forall x, y, v_0, \dots, v_{n-1} \in \mathcal{X} \Pr[X_{n+1} = y | X_0 = v_0, \dots, X_{n-1} = v_{n-1}, X_n = x] = \Pr[X_{n+1} = y | X_n = x]$.

If a Markov chain P is ergodic, i.e. irreducible and aperiodic, and \mathcal{X} is finite, then there is a unique stationary distribution π (i.e. a distribution π satisfying $\pi P = \pi$), and $\lim_{n \rightarrow \infty} \pi_0 P^n = \pi$.

Markov chains are often used for sampling and counting.

The problem

As we already discussed, the shattering phenomenon of random SAT explains the reason of failure of the current algorithmic approaches for SAT and #SAT that are based on Markov chains.

However we proved that #SAT is AP-reduced to #CM-SAT, the set of solutions of formulas of which, is connected. This tree-structure connecting the satisfying assignments of any formula for #CM-SAT, allows the design of ergodic Markov chains on this set of solutions.

We design Markov Chains for Size-of-Subtree, #CM-SAT, and any problem in TotP in general, and we study the following:

- stationary distribution $\pi(v) = w(v)/Z$
- mixing time with respect the height n of the tree
- complexity of $Z = \sum_{v \text{ solution}} w(v)$
- counting via these Markov chains

Contribution

The simple random walk on the full complete binary tree T converges to the uniform distribution over the nodes of T . The mixing time is polynomial with respect to the height n of the tree. An intuitive reason that the mixing time of the simple random walk is exponential is that the probability of going a level down equals $2 \times$ probability of going a level up, since every internal node has one parent but two children.

This lead us to the idea of the design of a Markov chain M_T such that the probability of going a level up equals probability of going a level down. We prove that the mixing time is polynomial for this Markov chain on the perfect binary tree.

We then generalize this Markov chain to M_S , having as state space the nodes of an arbitrary binary tree S of height n , as follows

$$p_S(i, j) = \begin{cases} 1/2 & \text{if } j \text{ is the parent of } i \\ 1/4 & \text{if } j \text{ is a child of } i \\ 0 & \text{for any other } j \neq i \\ 1 - \sum_{j \neq i} p_S(i, j) & \text{for } i = j \end{cases}$$

Theorem: For the generalized Markov chain M_S the following hold.

- Stationary distribution: $P_S(u) = \frac{w_S(u)}{Z_S}$, where $w_S(u) = 2^{n-\text{depth}(u)}$ and $Z_S = \sum_{u \in S} w_S(u)$
- Mixing time: polynomial
- Complexity of Z_S :
 - #P-complete (under Cook reductions)
 - admits FPRAS

Proof of stationary distribution

It is easy to check that $\forall j \sum_i \pi_S(i) p_S(i, j) = \pi_S(j)$.

Proof of mixing time

To bound the mixing time, we bound a quantity called conductance. The concept that conductance captures is the presence or absence of 'bottlenecks' in the state space of the Markov chain. In other words if (and only if) there is a subset of the state space from where it would be difficult to escape if you were trapped in, then the conductance of the Markov chain is small and the mixing time is big. Conversely if there is no subset from where it would be difficult to escape, then the conductance is big and the Markov chain mixes quickly to its stationary distribution.

Proof of hardness

The size of the tree S is reduced to the computation of Z_{S_i} , where S_i is the subtree of S containing all nodes up to depth i .

$$|S| = Z_{S_n} - \sum_{k=0}^{n-1} Z_{S_k}$$

Proof sketch: $|S| = r_0 + \dots + r_n$, where r_i is the number of nodes in depth i . We prove by induction that $r_k = Z_{S_k} - 2Z_{S_{k-1}}$.

Proof of FPRAS

Algorithm:

- Take m samples using M_S
- Compute $\hat{p} = \sum_i X_i / m$, where $X_i = 1$ iff the i -th sample is the root.
- Return $\hat{Z}_S = 2^n / \hat{p}$

Running time: The running time of the above algorithm is polynomial in the height n of the tree S . This holds because firstly the mixing time of M_S is polynomial. Secondly it holds that $P_S(\text{root}) = 2^n/Z_S$ and $P_S(\text{root}) \geq 1/(n+1)$, thus $m = \text{poly}(n)$ samples suffice to get a good estimate \hat{p} of $P_S(\text{root})$, and from \hat{p} to estimate Z_S .

Phase transitions

We introduce a model that generalizes the stationary distributions of the Markov chains studied in the previous section, and the respective normalizing factors, which are some weighted sums over the nodes of an input tree S given in succinct representation.

The tree-depth model:

$$w_\lambda^S(u) = \lambda^{n-\text{depth}(u)}$$

$$Z_\lambda^S = \sum_{u \in S} w_\lambda^S(u)$$

$$P_\lambda^S(u) = \frac{w_\lambda^S(u)}{Z_\lambda^S}$$

We assume that the exact height of the tree n is known.

The problem

We observe, in combination with the results of the previous section that

- for $\lambda = 1$: P_1^S is the uniform distribution over $V(S)$
 - the mixing time of the corresponding Markov chain is exponential
 - there is no FPRAS for Z_1^S unless NP=RP
- for $\lambda = 2$: $P_2^S = P_S$
 - we have polynomial mixing time of the corresponding Markov chain
 - there is an FPRAS for Z_2^S .

The question is what holds for the other values of $\lambda > 0$.

We design Markov chains M_λ^S that converge to P_λ^S using the Metropolis rule, and we study the mixing time for the various values of λ . We also study the complexity of computing and approximating Z_λ^S .

The Metropolis rule is a general method for designing a Markov chain that converges to some desirable probability distribution $\pi : \mathcal{X} \rightarrow [0, 1]$, where \mathcal{X} is a finite set.

The method is the following: first define a graph over \mathcal{X} . The transition probabilities are defined in two steps. From any state $u \in \mathcal{X}$ define an arbitrary probability distribution k over the neighbourhood of u (including u), and then for every $y \neq u$ in the neighbourhood, we go to y with probability $p(u, y) = k(u, y) * \max\{1, \frac{\pi(y)}{\pi(u)}\}$.

Contribution

We prove the following theorems.

Theorem: The mixing time of M_λ^S is

- for $0 < \lambda < 1$ exponential for all S
- for $\lambda \geq 2$ polynomial for all S
- for $\lambda \in [1, 2)$ it depends on the tree, e.g.
 - polynomial for the path
 - exponential for the perfect binary tree (T) and the Christmas-tree (CT)

For the proof we bound the conductance. The proofs differ for $\lambda < 1$ and $\lambda > 1$. This means that when we have slow mixing, it is caused by different reasons.

Corollary: The mixing time of M_λ^S undergoes a phase transition at $\lambda_c^S \in [1, 2]$ from exponential to polynomial. The exact value of the phase transition depends on the structure of the tree S .

Theorem: The complexity of Z_λ^S (in the worst case) is as follows.

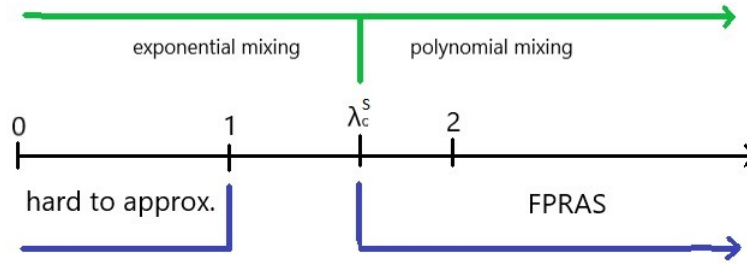
- $\forall \lambda > 0$ #P-hard under Cook reductions \rightarrow no exact computation (or with a small absolute error) is possible in polynomial time (unless NP=RP).
- $0 < \lambda \leq 1$ #P-hard under AP-reductions \rightarrow no FPRAS is possible (unless NP=RP).
 - Proof sketch: $Z_\lambda^{S_i} = \lambda Z_\lambda^{S_{i-1}} + m_i \Rightarrow |S| = Z_\lambda^S + (1 - \lambda) \sum_{i=0}^{n-1} Z_\lambda^{S_i}$, where S_i contains all nodes of S up to depth i , and m_i is the number of nodes in depth i .
- $\lambda \geq 2$ FPRAS exists, via sampling
 - Proof sketch: $Z_\lambda^S = \frac{2^n}{P_\lambda^S(\text{root})}$ and $P_\lambda^S(\text{root}) \geq 1/\text{poly}(n)$
- $\lambda \geq 1$ sampling \Rightarrow FPRAS

Note. we proved for $\lambda \geq 1$ that sampling \Rightarrow FPRAS. This holds even when sampling is not possible with the particular Markov chain that we studied here. In other words if it is possible to perform sampling according to P_λ^S in polynomial time with any algorithm (possibly different from ours), then FPRAS for Z_λ^S is also possible.

Corollary: The complexity of Z_λ^S undergoes a phase transition from inapproximable to approximable with FPRAS, at $\lambda_c \in [1, 2]$.

It is an open question whether λ_c coincides with λ_c^S for all S in some family of trees, where λ_c^S denotes the point of phase transition of the mixing time of M_λ^S .

Our results are summarized in the following figure.



In the previous results we assumed that the exact height n of the tree S is known. Now we study a modification of the problem, when n is not known, but only an upper bound of it is known. We prove the following.

Theorem: When an upper bound of the height of the tree is given

- The mixing times of M_λ^S are the same as before.
- Z_λ^S is hard to approximate for all λ
 - Proof sketch: for $\lambda \geq 1$ it holds $Z_\lambda^{CT} = Z_\lambda^T + \lambda^n(Z_\lambda^T - 1) \Rightarrow Z_\lambda^{CT} \geq 2Z_\lambda^T - 1$, where the height of T is n , the height of CT is $2n$ and we are given $2n$ as an upper bound for the height of the tree. If we could estimate Z_λ^S we could distinguish between case 1 and 2 of Christmas-trees, and thus solve USAT (as in the proof of hardness of Christmas-trees in the respective section presented previously).

Note. The FPRAS for Z_λ^S for $\lambda \geq 2$ fails in this modification of the problem. This is explained because, as we saw, $Z_\lambda^S = \frac{\lambda^n}{P_\lambda^S(\text{root})}$ but we can't find n just by knowing an upper bound of it.

Corollary: In the version of the problem where an upper bound of the height of the tree is given, weighted sampling $\not\Rightarrow$ weighted counting.

Remember that uniform sampling \Leftrightarrow unweighted counting [69], but it was not known whether an analogous result holds for weighted sums. Our result gives a counterexample, where sampling is possible in polynomial time, but the estimation of the weighted sum is hard.

Summary

- first completeness results for TotP
- #SAT, which is hard on average to approximate, is AP-reduced to Size-of-Subtree which is easy on average to approximate: AP-reductions don't preserve probability mass
- #SAT, which has a shattered set of solutions, is AP-reduced to #CM-SAT, which has a connected set of solutions: new algorithms must be studied, new hardness explanations are needed
- study of Markov chains for #CM-SAT, and other ToP-complete problems
- discovery of phase transitions
- weighted sampling $\not\Rightarrow$ weighted counting (unlike unweighted)
- better exponential time results for TotP than those for #P
- $\text{FPRAS} \not\subseteq \text{TotP}$ unless $\text{RP}=\text{P}$
- Instances with too few or too many solutions are easy
- Christmas-trees are hard

Open Problems

- Fine grained complexity of #CM-SAT, Size-of-Subtree etc.
- Relationships of Interval-Function classes and descriptive complexity classes with #RP1, #RP2.
- Descriptive complexity of TotP.
- Design and study of other Markov chains for #CM-SAT.
- FPTAS for Z_S . Note this would imply AC0-CAPE in polynomial time.
- Complexity of Z_λ^S $\lambda \in (1, \lambda_c^S)$ for the tree-depth model.
- Characterization of FPRAS, FPTAS in terms of path counting/ Interval-Function/ descriptive complexity.
- Is #IS TotP-complete under Karp reductions?
- For which class is PERMANENT complete under Karp reductions?
- (NP vs. RP) via (FPRAS vs. TotP).

Γλωσσάριο - Glossary

| | |
|-----------------------------------|-------------------------------|
| αγωγιμότητα | conductance |
| αλλαγή φάσης | phase transition |
| αμερόληπτη εκτιμήτρια | unbiased estimator |
| αναγωγή | reduction |
| ανεξάρτητο σύνολο | independent set |
| απλός τυχαίος περίπατος | simple random walk |
| αποκωδικοποίηση | decoding |
| απόλυτο σφάλμα | absolute error |
| αυτοαναγώγιμο (πρόβλημα) | self reducible (problem) |
| δειγματοληψία | sampling |
| διαζευκτική κανονική μορφή | disjunctive normal form (DNF) |
| διακλάδωση | branching |
| διαμόρφωση | configuration |
| δομικός | structural |
| δυαδικός | binary |
| είσοδος | input |
| έξοδος | output |
| ικανοποιητική ανάθεση | satisfying assignment |
| κλάση | class |
| κλήση μαντείου | oracle call |
| κύκλωμα | circuit |
| κωδικοποίηση | encoding |
| λογικός τύπος | logical formula |
| μαρκοβιανή αλυσίδα | Markov chain |
| μερική διάταξη | partial order |
| μερικώς διατεταγμένο σύνολο | partially ordered set |
| μετρητική πολυπλοκότητα | counting complexity |
| μη αναγώγιμη (μαρκοβιανή αλυσίδα) | irreducible (Markov chain) |

| | |
|----------------------------------|----------------------------------|
| μονοπάτι αποδοχής | accepting path |
| οριακή κατανομή | limiting distribution |
| περιοδική (μαρκοβιανή αλυσίδα) | periodic (Markov chain) |
| πίνακας μεταβάσεων | transition matrix |
| πλειάδα | tuple |
| πλήρης | complete |
| πληρότητα | completeness |
| πολλαπλασιαστικό σφάλμα | multiplicative error |
| πολυπλοκότητα | complexity |
| πρόβλημα απόφαση ύπαρξης λύσης | decision problem |
| πρόβλημα καταμέτρησης ή μέτρησης | counting problem |
| προσέγγιση | approximation |
| προσθετικό σφάλμα | additive error |
| πύλη | gate |
| σταθμισμένη μέτρηση | weighted counting |
| στάσιμη κατανομή | stationary distribution |
| στατιστική απόσταση | statistical/variational distance |
| στήριγμα (κατανομής) | support |
| στιγμιότυπο | instance |
| στοχαστική διαδικασία | stochastic process |
| συζευκτική κανονική μορφή | conjunctive normal form (CNF) |
| συμβολοσειρά | string |
| συντελεστής κανονικοποίησης | normalizing factor |
| ταίριασμα | matching |
| υπολογίσιμος | computations |
| φειδωλή αναγωγή | parsimonious reduction |
| χρόνος σύγκλισης | mixing time |
| χώρος καταστάσεων | state space |

Περιεχόμενα

| | | |
|----------|---|-----------|
| 1 | Εισαγωγικά | 41 |
| 1.1 | Η #P και η TotP | 41 |
| 1.2 | Είδη αναγωγών | 44 |
| 1.3 | Είδη προσεγγίσεων | 46 |
| 1.4 | Βασικά θεωρήματα σχετικά με προσεγγισιμότητα | 47 |
| 1.4.1 | Σχετικά με προσθετικό σφάλμα | 47 |
| 1.4.2 | Σχετικά με FPRAS | 47 |
| 1.4.3 | Δειγματοληψία και καταμέτρηση | 48 |
| 1.5 | Μαρκοβιανές αλυσίδες-Αλλαγές φάσης | 50 |
| 1.5.1 | Σταθμισμένη μέτρηση | 50 |
| 1.5.2 | Βασικές στοιχεία για Μαρκοβιανές αλυσίδες | 52 |
| 1.5.3 | Δειγματοληψία με τη μέθοδο Markov Chain Monte Carlo | 54 |
| 1.5.4 | Ο κανόνας του Metropolis | 55 |
| 1.5.5 | Αλλαγές φάσης | 56 |
| 1.5.6 | Ένα φαινόμενο διασκορπισμού λύσεων για το τυχαίο SAT | 57 |
| 2 | TotP-Πληρότητα | 61 |
| 2.1 | Εισαγωγή | 61 |
| 2.1.1 | Σχετικές εργασίες | 63 |
| 2.1.2 | Συνεισφορά και βασικές ιδέες | 64 |
| 2.1.3 | Συνέπειες | 65 |
| 2.2 | Προκαταρκτικά | 67 |
| 2.3 | Το #MONOTONE CIRCUIT SAT είναι TotP-πλήρες υπό Karp αναγωγές | 70 |
| 2.3.1 | Το #MONOTONE CIRCUIT SAT είναι TotP-hard | 71 |
| 2.3.2 | Το #MONOTONE CIRCUIT SAT ανήκει στην TotP | 72 |
| 2.3.3 | Συζήτηση σχετικά με την επιλογή της κωδικοποίησης και τη μερική διάταξη | 74 |
| 2.4 | Άλλα TotP-πλήρη προβλήματα | 75 |
| 2.5 | Επιπτώσεις | 80 |
| 2.5.1 | Σχετικά με την πολυπλοκότητα του Size-of-Subtree | 80 |
| 2.5.2 | Σχετικά με την προσεγγισιμότητα της TotP | 81 |
| 2.5.3 | Σχετικά με την προσέγγιση στη #P, και το τυχαίο SAT | 83 |

| | | |
|----------|---|------------|
| 2.6 | Συμπεράσματα και ανοιχτά προβλήματα | 84 |
| 3 | Προσεγγισιμότητα | 87 |
| 3.1 | Εκθετικού χρόνου πολυπλοκότητα προσέγγισης | 87 |
| 3.1.1 | Εισαγωγή | 87 |
| 3.1.2 | Συνεισφορά | 88 |
| 3.1.3 | Σχετικές εργασίες και ανοιχτά προβλήματα | 88 |
| 3.1.4 | Προαπαιτούμενα | 90 |
| 3.1.5 | Αποτελέσματα | 90 |
| 3.2 | FPRAS vs. TotP | 92 |
| 3.2.1 | Εισαγωγή | 93 |
| 3.2.2 | Προαπαιτούμενα | 95 |
| 3.2.3 | Αποτελέσματα | 95 |
| 3.2.4 | Αποδείξεις | 96 |
| 3.2.5 | Συζήτηση και ανοιχτά προβλήματα | 99 |
| 3.2.6 | Σχετικές εργασίες | 99 |
| 3.2.7 | Συμπεράσματα | 100 |
| 3.3 | Τα δύσκολα στιγμιότυπα του Size-of-Subtree | 100 |
| 3.3.1 | Δέντρα με δύσκολα προσεγγίσιμο μέγεθος | 101 |
| 4 | Μαρκοβιανές αλυσίδες για TotP-πλήρη προβλήματα | 103 |
| 4.1 | Εισαγωγή | 104 |
| 4.1.1 | Πρώτες απόπειρες και αναδυόμενα ερωτήματα | 105 |
| 4.1.2 | Κύρια αποτελέσματα και συζήτηση | 106 |
| 4.2 | Ο απλός τυχαίος περίπατος στο τέλειο δυαδικό δέντρο | 107 |
| 4.3 | Μια ταχέως συγκλίνουσα μαρκοβιανή αλυσίδα στο τέλειο δυαδικό δέντρο | 108 |
| 4.4 | Μια γενίκευση για αυθαίρετο δυαδικό δέντρο | 109 |
| 4.4.1 | Στάσιμη κατανομή και χρόνος σύγκλισης | 109 |
| 4.4.2 | Η πολυπλοκότητα υπολογισμού του συντελεστή κανονικοποίησης | 111 |
| 4.4.3 | Η πολυπλοκότητα υπολογισμού του μεγέθους του στηρίγματος | 115 |
| 4.5 | Παρατηρήσεις και ανοιχτά ερωτήματα | 118 |
| 4.6 | Σχετικές εργασίες | 119 |
| 5 | Αλλαγές φάσης για το tree-depth μοντέλο | 121 |
| 5.1 | Εισαγωγή | 121 |
| 5.1.1 | Σύνδεση με τα προηγούμενα | 122 |
| 5.2 | Το tree-depth μοντέλο | 123 |
| 5.3 | Αποτελέσματα | 124 |
| 5.4 | Η μαρκοβιανή αλυσίδα | 125 |
| 5.5 | Ο χρόνος σύγκλισης | 126 |
| 5.6 | Η πολυπλοκότητα υπολογισμού του συντελεστή κανονικοποίησης | 130 |

| | | |
|-------|-------------------------------|-----|
| 5.6.1 | Όταν το ύψος είναι γνωστό | 130 |
| 5.6.2 | Όταν το ύψος δεν είναι γνωστό | 133 |
| 5.7 | Συζήτηση | 136 |
| 5.7.1 | Ανοιχτά προβλήματα | 137 |
| 5.7.2 | Σχετικές εργασίες | 137 |

Κεφάλαιο 1

Εισαγωγικά

1.1 Η #P και η TotP

Η κλάση πολυπλοκότητας #P [76] είναι η κλάση συναρτήσεων που μετρούν το πλήθος των μονοπατιών αποδοχής μιας NPTM (μη ντετερμινιστική πολυωνυμικού χρόνου μηχανή Turing). Ισοδύναμα, η #P είναι η κλάση των συναρτήσεων που μετρούν τον αριθμό λύσεων ενός προβλήματος απόφασης που ανήκει στην NP. Συχνά χρησιμοποιούμε τον όρο «πρόβλημα καταμέτρησης» για τέτοιες συναρτήσεις.

Το πλήθος των λύσεων για τα NP-πλήρη προβλήματα είναι δύσκολο να μετρηθεί σε πολυωνυμικό χρόνο, αλλά υπάρχουν #P-πλήρη προβλήματα, που έχουν το αντίστοιχο πρόβλημα απόφασης στο P, π.χ. #DNF. Επιπλέον, μερικά από αυτά μπορούν να προσεγγιστούν, π.χ. το PERMANENT [43] και το #DNF [46], ενώ άλλα δεν μπορούν, π.χ. #IS [25].

Με τον όρο «αντίστοιχο πρόβλημα απόφασης» ενός προβλήματος καταμέτρησης, εννοούμε το πρόβλημα όπου πρέπει να αποφασίσουμε εάν η τιμή της αντίστοιχης συνάρτησης σε μια είσοδο είναι μηδενική. Αντίστοιχα, το πρόβλημα απόφασης εξετάζει αν υπάρχουν λύσεις ή ισοδύναμα, αν υπάρχει μονοπάτι αποδοχής για την αντίστοιχη NPTM. Θα χρησιμοποιούμε συχνά την έκφραση "απόφαση" αντί για "πρόβλημα απόφασης ύπαρξης λύσης".

Η κλάση των προβλημάτων στη #P με απόφαση στο P ονομάζεται #PE. Το σύνολο όλων των προβλημάτων καταμέτρησης που είναι αυτοαναγώγιμα (self reducible) και ανήκουν στη #P έχοντας απόφαση στην P, περιέχεται σε μια κλάση πολυπλοκότητας που ονομάζεται TotP [62]. Η TotP είναι γνήσια υποκλάση της #P εκτός αν $P = NP$ [62].

Συμβολισμοί Σε όλη την παρούσα εργασία, χρησιμοποιούμε ως μοντέλο υπολογισμού τη μη ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου (NPTM). Για κάθε NPTM M υπάρχει ένα πολύνυμο p_M που φράσσει το χρόνο λειτουργίας της. Όταν μια NPTM M επιστρέφει *yes* ή *no*, δηλώνουμε με $acc_M(x)$ τη συνάρτηση που η τιμή της στο x ισούται με τον αριθμό των αποδεκτών υπολογιστικών μονοπατιών της M με είσοδο $x \in \Sigma^*$, όπου Σ είναι κάποιο αλφάβητο.

Ορισμός 1. [76] Η $\#P$ είναι η κλάση συναρτήσεων f για τις οποίες υπάρχει μια υπολογίσιμη σε πολωνυμικό χρόνο σχέση R και ένα πολώνυμο p τέτοιο ώστε $\forall x \in \Sigma^*$, $f(x) = |\{y \in \{0, 1\}^* \mid |y| = p(|x|) \wedge R(x, y)\}|$. Ισοδύναμα, $\#P = \{acc_M : \Sigma^* \rightarrow \mathbb{N} \mid M \text{ is a NPTM}\}$

Ορισμός 2. Η FP είναι η κλάση συναρτήσεων στη $\#P$ που υπολογίζονται σε πολωνυμικό χρόνο.

Ορισμός 3. Η απόφαση (*decision version*), ή αλλιώς το πρόβλημα απόφασης, μιας συνάρτησης στην $\#P$ είναι η γλώσσα $L_f = \{x \in \Sigma^* \mid f(x) > 0\}$.

Ορισμός 4. [61] $\#PE = \{f : \Sigma^* \rightarrow \mathbb{N} \mid f \in \#P \text{ and } L_f \in P\}$.

Ορισμός 5. [47] $TotP = \{tot_M : \Sigma^* \rightarrow \mathbb{N} \mid M \text{ is a NPTM}\}$, όπου $tot_M(x) = \#(\text{όλα τα υπολογιστικά μονοπάτια της } M \text{ με είσοδο } x) - 1$.

Το πιο σημαντικό θεώρημα για την $TotP$ είναι ότι περιέχει όλα τα αυτοαναγωγίσιμα προβλήματα στην $\#P$ με απόφαση στην P .

Διασθητικά, μια συνάρτηση είναι αυτοαναγωγίσιμη αν μπορούμε να ανάγουμε τον υπολογισμό της τιμής της σε κάποια είσοδο, στον αναδρομικό υπολογισμό της τιμής της αναδρομικά σε ένα πολωνυμικό πλήθος άλλων εισόδων, αρκεί το βάθος της αναγωγής να είναι επίσης πολωνυμικό.

Για παράδειγμα το $\#SAT$ είναι αυτοαναγωγίσιμο, αφού το πλήθος των ικανοποιητικών αναθέσεων για έναν λογικό τύπο ϕ ισούται με το άθροισμα των ικανοποιητικών αναθέσεων των δύο τύπων ϕ_0 και ϕ_1 , όπου ϕ_0 , (αντίστοιχα ϕ_1) είναι ο ϕ με την πρώτη του μεταβλητή σταθεροποιημένη στην τιμή 0 (αντίστοιχα 1).

Ο πιο γενικός ορισμός αυτοαναγωγιμότητας που καλύπτει η $TotP$ είναι ο εξής.

Ορισμός 6. Μια συνάρτηση $f : \Sigma^* \rightarrow \mathbb{N}$ λέγεται πολωνυμικά αυτοαναγωγίσιμη αν υπάρχουν πολώνυμα r και q , και υπολογίσιμες σε πολωνυμικό χρόνο συναρτήσεις $h : \Sigma^* \times \mathbb{N} \rightarrow \Sigma^*$, $g : \Sigma^* \times \mathbb{N} \rightarrow \mathbb{N}$, και $t : \Sigma^* \rightarrow \mathbb{N}$ έτσι ώστε για κάθε $x \in \Sigma^*$:

1. η f μπορεί να υπολογιστεί αναδρομικά, ανάγοντας το x σε ένα πολωνυμικό πλήθος άλλων στιγμοτύπων (δλδ εισόδων) $h(x, i)$ ($0 \leq i \leq r(|x|)$), και συγκεκριμένα μπορεί να γραφτεί ως εξής:

$$\forall x \in \Sigma^* \quad f(x) = t(x) + \sum_{i=0}^{r(|x|)} g(x, i) f(h(x, i))$$
2. η αναδρομή έχει πολωνυμικό βάθος, δλδ τυπικά: το βάθος της αναδρομής είναι $q(|x|)$, και $\forall x \in \Sigma^*$

$$\forall j_1, j_2, \dots, j_{q(|x|)} \in \{0, \dots, r(|x|)\} \quad \eta \quad f(h(\dots h(h(x, j_1), j_2) \dots, j_{q(|x|)}))$$

 μπορεί να υπολογιστεί σε πολωνυμικό χρόνο.
3. κάθε στιγμότυπο που εμπλέκεται στην αναδρομή έχει μέγεθος $poly(|x|)$, δλδ τυπικά:

$$\forall x \in \Sigma^* \quad \forall k \leq q(|x|) \quad \forall j_1, j_2, \dots, j_k \in \{0, \dots, r(|x|)\}$$

$$|h(\dots h(h(x, j_1), j_2) \dots, j_k)| \in \mathcal{O}(poly(|x|)).$$

Παρατηρήστε ότι αν η h μειώνει το μήκος της εισόδου, δηλ $|h(x, i)| < |x|$ για κάθε $x \in \Sigma^*$ και i ($0 \leq i \leq r(|x|)$), το οποίο σημαίνει ότι τα υπο-στιγμιότυπα $h(x, i)$ είναι μικρότερου μεγέθους από το x , τότε η απαίτηση (b) ισχύει τετριμμένα. Επιπλέον το (c) απαιτεί όλα τα στιγμιότυπα στα οποία η f θα υπολογιστεί να είναι πολωνυμικού μεγέθους σε σχέση με το $|x|$, το οποίο επίσης ισχύει τετριμμένα αν η h μειώνει το μήκος της εισόδου.

Επίσης παρατηρήστε ότι στον ορισμό της αναγωγής επιτρέπεται μόνο πρόσθεση, με θετικούς συντελεστές $g(\cdot)$, των τιμών των $r(\cdot)$ στιγμιότυπων (και όχι αφαίρεση ή αρνητικοί συντελεστές).

Για τις προαναφερθείσες κλάσεις ισχύει το παρακάτω θεώρημα. Ιδιαίτερα το (b) είναι πολύ σημαντικό, διότι δίνει έναν συντακτικό χαρακτηρισμό για την κλάση όλων των αυτοαναγωγίμων μετρητικών προβλημάτων με εύκολη απόφαση, ενώ ο χαρακτηρισμός "με εύκολη απόφαση" δεν είναι συντακτικός, αλλά εννοιολογικός.

Για να είναι κατανοητός ο ορισμός πρέπει να αναφέρουμε ότι Karp-closure μίας κλάσης πολυπλοκότητας είναι η ένωση της κλάσης με το σύνολο όλων των προβλημάτων που ανάγονται κατά Karp σε κάποιο πρόβλημα της κλάσης. Περισσότερα για τα είδη αναγωγών θα δούμε παρακάτω στην υποενότητα 1.2.

Θεώρημα 1. [62] (a) $FP \subseteq TotP \subseteq \#PE \subseteq \#P$. Οι εγκλεισμοί είναι γνήσιοι εκτός αν $P=NP$.

(b) Η $TotP$ είναι το Karp-closure των πολωνυμικά αυτοαναγωγίμων συναρτήσεων στην $\#PE$.

Για να γίνουν οι ορισμοί πιο κατανοητοί, θα δώσουμε ένα παράδειγμα ενός προβλήματος στην $TotP$, θα δείξουμε ότι είναι αυτοαναγωγίμο, και θα δώσουμε την αντίστοιχη NPTM, της οποίας το πλήθος των μονοπατιών με είσοδο x ισούται με $f(x) + 1$.

Το πρόβλημα είναι το $\#IS$: δεδομένου ενός γραφήματος G με n κόμβους, $f(G)$ είναι το πλήθος των ανεξαρτήτων συνόλων του G , όλων των μεγεθών. Υπενθυμίζουμε ότι ένα υποσύνολο των κόμβων ενός γραφήματος είναι ανεξάρτητο, εάν δεν υπάρχουν ακμές μεταξύ των κόμβων αυτού του συνόλου.

Θεώρημα 2. $\#IS \in TotP$.

Απόδειξη. Το πρόβλημα απόφασης ύπαρξης λύσης για το $\#IS$, δηλαδή ύπαρξης ανεξάρτητου συνόλου οποιουδήποτε μεγέθους, είναι στο P , αφού ένας μεμονωμένος κόμβος αποτελεί πάντα ανεξάρτητο σύνολο.

Το αντίστοιχο δέντρο της αυτοαναγωγιμότητας μπορεί να οριστεί ως εξής. Οι κόμβοι του δέντρου αυτοαναγωγιμότητας είναι τα υπογραφήματα που εμφανίζονται στην αναγωγή.

Η $f(G)$ ισούται με το πλήθος των ανεξαρτήτων συνόλων που περιέχουν τον κόμβο 1 συν το πλήθος αυτών που δεν τον περιέχουν, οπότε η $f(G)$ ανάγεται στο $f(G_0) + f(G_1)$, όπου G_0 είναι το G έχοντας αφαιρέσει τον κόμβο 1 και τους γείτονές του, και G_1 είναι το G έχοντας αφαιρέσει τον κόμβο 1.

Επαναλαμβάνουμε το ίδιο αναδρομικά για όλα τα υποστιγμιότυπα που εμφανίζονται. Οπότε το ύψος του δέντρου αυτοαναγωγιμότητας είναι n . Η αντίστοιχη

NPTM λειτουργεί ως εξής. Σε κάθε βήμα i ελέγχει για τα αντίστοιχα υποστιγμιότυπα αν τα $f(G_0^i)$ και $f(G_1^i)$ είναι μη μηδενικά, και αν και τα δύο είναι μη μηδενικά, τότε διακλαδώνεται σε ένα από τα δύο υποστιγμιότυπα (δηλαδή προχωράει μη ντετερμινιστικά), αλλιώς προχωράει ντετερμινιστικά σε εκείνο το υποστιγμιότυπο G_b^i για το οποίο $f(G_b^i) > 0$, εφόσον υπάρχει τέτοιο υποστιγμιότυπο, αλλιώς τερματίζει. Τέλος, προκειμένου να έχουμε τελικά συνολικά $f(G) + 1$ φύλλα (ή, ισοδύναμα, $f(G) + 1$ υπολογιστικά μονοπάτια), στο τέλος όλου του υπολογισμού κάνει άλλη μία διακλάδωση στο αριστερότερο μονοπάτι (αυτό δλδ στο οποίο δεν έχει γίνει καμία "δεξιά" επιλογή σε κανένα υπολογιστικό βήμα). \square

Παρατηρήστε ότι σε αυτή την περίπτωση το δέντρο υπολογισμού ταυτίζεται ακριβώς με το δέντρο της αυτοαναγωγιμότητας έχοντας προσθέσει μια επιπλέον διακλάδωση στο αριστερότερο φύλλο. Και προφανώς το πλήθος των μη ντετερμινιστικών bits που χρησιμοποιούνται από την NPTM είναι το πολύ όσο και το ύψος του δέντρου αυτοαναγωγιμότητας συν ένα. Αυτό συμβαίνει επειδή η $f(x)$ προκύπτει από μια απλή πρόσθεση τιμών της f για δύο υποστιγμιότυπα. Αλλά δεν συμβαίνει το ίδιο για όλα τα προβλήματα της TotP, μιας και ο ορισμός της αυτοαναγωγιμότητας είναι πιο γενικός. Από την άλλη αυτό συμβαίνει για πολλά ενδιαφέροντα προβλήματα που ορίζονται σε γράφους και κυκλώματα, όπως είναι η μέτρηση ικανοποιητικών αναθέσεων μονότονων κυκλωμάτων και DNF τύπων.

1.2 Είδη αναγωγών

Αναγωγές μεταξύ συνατήσεων μέτρησης μπορούν να οριστούν με ανάλογο τρόπο όπως οι Cook/Turing και οι Karp/many-one αναγωγές μεταξύ γλωσσών. Στην παρούσα διατριβή θα μας απασχολήσουν τρία είδη αναγωγών: οι Cook ή Turing, οι Karp ή parsimonious, και οι approximation preserving.

Έστω $f, g \in \#P$.

Ορισμός 7. Cook-reductions. Η f ανάγεται στην g με Cook αναγωγές (συμβολικά $f \leq_T^p g$) αν $f \in FP^g$. Δλδ. η f μπορεί να υπολογιστεί σε πολυωνυμικό χρόνο με μια μηχανή Turing, η οποία χρησιμοποιεί κλήσεις μαντείου στην g .

Ορισμός 8. Parsimonious reductions. Η f ανάγεται στην g με φειδωλές αναγωγές (συμβολικά $f \leq_m^p g$) if αν $\exists h \in FP, \forall x \in \Sigma^* f(x) = g(h(x))$.

Ορισμός 9. Approximation preserving reductions [27]. Η f ανάγεται στην g με αναγωγές που διατηρούν την προσέγγιση (συμβολικά $f \leq_{AP} g$) αν ισχύει το εξής: Αν υπάρχει FPRAS (ορ. [3]) για την g , τότε υπάρχει FPRAS για την f , το οποίο χρησιμοποιεί κλήσεις μαντείου στην g .

Παρατήρηση Οι φειδωλές αναγωγές είναι επίσης Cook και διατηρούν την προσέγγιση. Όμως οι Cook και αυτές που διατηρούν την προσέγγιση είναι μη συγκρίσιμες μεταξύ τους. Για παράδειγμα το πρόβλημα μέτρησης ανεξαρτήτων συνόλων

όλων των μεγεθών ενός γραφήματος που δίνεται ως είσοδος, δηλ το #IS, είναι #P-complete με αναγωγές που διατηρούν την προσέγγιση [27], αλλά δεν είναι #P-complete με αναγωγές Cook. Αντιθέτως το πρόβλημα υπολογισμού της permanent ενός πίνακα με στοιχεία 0,1 είναι #P-complete με Cook αναγωγές [76], αλλά δεν μπορεί να είναι #P-complete με αναγωγές που διατηρούν την προσέγγιση εκτός αν NP=RP, επειδή ο υπολογισμός της permanent επιδέχεται FPRAS [43], οπότε μια τέτοια αναγωγή θα συνεπαγόταν ύπαρξη FPRAS για το #SAT και συνεπώς το NP θα ήταν ίσο με το RP. Υπενθυμίζουμε ότι αν το #SAT επιδέχεται FPRAS, τότε υπολογίζοντάς το με πολλαπλασιαστικό σφάλμα μικρότερο από 0.5 μπορούμε να ξεχωρίσουμε μια μη ικανοποιήσιμη από μια ικανοποιήσιμη φόρμουλα με μεγάλη πιθανότητα (οπότε NP=RP).

Παρατηρήσεις

- Οι Karp αναγωγές είναι και Cook, και AP.
- Οι Karp αναγωγές διατηρούν την ύπαρξη λύσης, οι Cook και οι AP δεν τη διατηρούν.
- Οι Cook αναγωγές δεν είναι απαραίτητα AP, οι AP δεν είναι απαραίτητα Cook.
- Αν A είναι NP-complete κατά Karp, τότε το #A είναι #P-complete κατά AP [27] (ενώ δεν έχουμε απόδειξη ότι είναι #P-complete κατά Karp ή Cook)!!!
- Αν $A \in \#P\text{-complete}$ κατά
 - Cook \Rightarrow ακριβής υπολογισμός δύσκολος (λύνει το #SAT)
προσέγγιση όχι απαραίτητα δύσκολη (πχ. το PERMANENT έχει FPRAS).
 - AP \Rightarrow προσέγγιση δύσκολη (προσεγγίζει το #SAT)
ακριβής λύση πάλι απλώς προσεγγίζει (δε λύνει) το #SAT.
 - Karp \Rightarrow ακριβής λύση δύσκολη (λύνει το #SAT)
προσέγγιση δύσκολη (προσεγγίζει το #SAT).
- Προσέγγιση του #SAT \Rightarrow λύση του SAT \Rightarrow NP=P.
Λύση του #SAT \Rightarrow PH=P [73]!!!
- Αν $A \in \text{TotP-complete}$ κατά
 - Cook \Rightarrow $A \in \#P\text{-complete}$ κατά Cook (μέσω PERMANENT).
 - AP \Rightarrow $A \in \#P\text{-complete}$ κατά AP (μέσω #IS).
 - Karp \Rightarrow $A \notin \#P\text{-complete}$ κατά Karp (εκτός αν P=NP).
Αλλά $A \in \#P\text{-complete}$ κατά Cook (μέσω PERMANENT)
και $A \in \#P\text{-complete}$ κατά AP (μέσω #IS).

- Άρα οι Cook αναγωγές είναι πιο ισχυρές από τις AP αναγωγές, υπό την έννοια ότι η ακριβής λύση ενός πλήρους προβλήματος είναι τόσο δύσκολη όσο η πολυωνυμική ιεραρχία (PH), όμως η προσέγγισή του επιτρέπεται. Οι AP αναγωγές είναι πιο ισχυρές από τις Cook υπό την έννοια ότι απαγορεύουν και την ακριβή λύση αλλά και την προσέγγιση του πλήρους προβλήματος, όμως σε αυτή την περίπτωση η ακριβής λύση είναι τόσο δύσκολη μόνο όσο το NP. Οι Karp αναγωγές είναι οι πιο ισχυρές από όλες από κάθε άποψη. Επιπλέον οι Karp είναι οι μόνες που διαχωρίζουν την #P από την TotP, αφού είναι οι μόνες που διατηρούν την ύπαρξη λύσης.

Στα παραπάνω, σύμφωνα με το σύνηθες στη βιβλιογραφία, ο όρος Karp είναι ισοδύναμος με τον όρο parsimonious. Όμως πρέπει να αναφέρουμε ότι σε κάποιες σπάνιες περιπτώσεις στη βιβλιογραφία ο όρος έχει χρησιμοποιηθεί και με λίγο διαφορετικό ορισμό, ο οποίος φυσικά δίνεται στα αντίστοιχα κείμενα, κι έτσι δημιουργείται σύγχυση.

1.3 Είδη προσεγγίσεων

Θα μας απασχολήσουν τρία είδη σφαλμάτων προσέγγισης: το προσθετικό, το πολλαπλασιαστικό και το απόλυτο. Το προσθετικό αφορά στον υπολογισμό πιθανοτήτων, ενώ το πολλαπλασιαστικό και το απόλυτο αφορούν σε οποιαδήποτε πραγματική ποσότητα που θέλουμε να υπολογίσουμε.

Ορισμός 10. Καλούμε ξ -*additive-error approximation* για μία ποσότητα $p \in [0, 1]$ (πχ. το p συνήθως είναι ποσοστό ή πιθανότητα), έναν αριθμό $\hat{p} = p \pm \xi$, για κάποιο $\xi \in (0, 1)$.

Για παράδειγμα, για το #SAT ένα προσθετικό σφάλμα αφορά στην ποσότητα $p(\phi) = (\# \text{ satisfying assignments of } \phi) / 2^n$, όπου ϕ είναι μια φόρμουλα με n μεταβλητές, δοσμένη ως είσοδος.

Ορισμός 11. Έστω $x, \in \mathbb{R}, \epsilon > 0$. Καλούμε ϵ -*multiplicative-error approximation* για το x έναν αριθμό $\hat{x} = x(1 \pm \epsilon)$.

Ορισμός 12. Έστω $x, \in \mathbb{R}, \epsilon > 0$. Καλούμε ϵ -*absolute-error approximation* για το x έναν αριθμό $\hat{x} = x \pm \epsilon$.

Καλούμε FPRAS έναν αλγόριθμο πολυωνυμικού χρόνου, που επιτυγχάνει όσο μικρό πολλαπλασιαστικό σφάλμα θέλουμε.

Ορισμός 13. Καλούμε *FPRAS* για μια συνάρτηση $f : \Sigma^* \rightarrow \mathbb{R}$ έναν πιθανοτικό αλγόριθμο A τέτοιο ώστε για κάθε $x \in \Sigma^*$, και για κάθε $\epsilon > 0$ υπολογίζει μια ποσότητα $A(x)$ σε χρόνο $\text{poly}(|x|, \epsilon^{-1})$ έτσι ώστε

$$\Pr[(1 - \epsilon)f(x) \leq A(x) \leq (1 + \epsilon)f(x)] \geq \frac{3}{4}$$

1.4 Βασικά θεωρήματα σχετικά με προσεγγισιμότητα

1.4.1 Σχετικά με προσθετικό σφάλμα

Κάθε συνάρτηση στη $\#P$ επιδέχεται αλγόριθμο με προσθετικό σφάλμα σε πολυωνυμικό χρόνο.

Έστω $f \in \#P$, $x \in \Sigma^*$, $\xi \in (0, 1)$. Έστω M η αντίστοιχη NPTM, δλδ. μια NPTM τέτοια ώστε $\forall x \text{ acc}_M(x) = f(x)$, και έστω m το ύψος του υπολογιστικού δέντρου της M με είσοδο x . Παρατηρήστε ότι $m = \text{poly}(n)$, όπου n είναι το μέγεθος της εισόδου x . Έστω $p_f(x) = f(x)/2^m$.

Θεώρημα 3. Για κάθε $f \in \#P$, $x \in \Sigma^*$, $\xi \in (0, 1)$ υπάρχει αλγόριθμος που επιστρέφει σε χρόνο $\text{poly}(n, \xi^{-1})$ έναν αριθμό $\hat{p} = p_f(x) \pm \xi$.

Απόδειξη. Μπορούμε να πραγματοποιήσουμε μια απλή διαδικασία δειγματοληψίας κατά την οποία διαλέγουμε $r = \text{poly}(m)$ μη ντετερμινιστικά υπολογιστικά μονοπάτια της M με είσοδο x , με ομοιόμορφη πιθανότητα, και να πάρουμε ως προσέγγιση της $p_f(x)$ το ποσοστό αυτών των r δειγμάτων που είναι μονοπάτια αποδοχής. Για μια πλήρη απόδειξη αυτού δείτε π.χ. [34] κεφάλαιο 6.2.2. \square

Ακόμα και για προβλήματα που επιδέχονται πολλαπλασιαστικού σφάλματος προσέγγιση, ένας αλγόριθμος προσθετικού σφάλματος δεν είναι συγκρίσιμος, με την έννοια ότι μπορεί να δώσει είτε καλύτερο είτε χειρότερο αποτέλεσμα από τον αλγόριθμο πολλαπλασιαστικού σφάλματος, ανάλογα με την είσοδο. Το προσθετικό σφάλμα είναι καλύτερο από το πολλαπλασιαστικό όταν η ποσότητα που θέλουμε να υπολογίσουμε είναι μεγάλη, ενώ είναι χειρότερο όταν η ποσότητα είναι πολύ μικρή.

1.4.2 Σχετικά με FPRAS

Και $\#P$ και η TotP επιδέχονται FPRAS αν και μόνον αν $NP=RP$. Η αντίστροφη κατεύθυνση αυτής της ισοδυναμίας προκύπτει από ένα θεώρημα του Stockmeyer, αλλά επειδή δεν την έχουμε δει πουθενά γραμμένη ρητά, δίνουμε ένα σκιαγράφημα απόδειξης, για λόγους πληρότητας του παρόντος κειμένου.

Θεώρημα 4. Για κάθε $f \in \#P$ υπάρχει FPRAS αν $NP=RP$.

Απόδειξη. (σκιαγράφημα)

Αν $NP=RP$ τότε όλα τα προβλήματα στην $\#P$ επιδέχονται FPRAS.

Απόδειξη: Στο [71] ο Stockmeyer αποδεικνύει ότι ένα FPRAS, με πρόσβαση σε ένα Σ_2^P μαντείο, υπάρχει για κάθε πρόβλημα στην $\#P$. Οπότε αν $NP=RP$ τότε $\Sigma_2^P = NP^{NP} = RP^{RP} \subseteq BPP$. Τέλος είναι εύκολο να δει κανείς ότι ένα FPRAS με πρόσβαση σε ένα BPP μαντείο, μπορεί να αντικατασταθεί από ένα άλλο FPRAS, που προσομοιώνει το ίδιο τις κλήσεις στο μαντείο.

Αν $NP \neq RP$ τότε είναι αδύνατη η ύπαρξη FPRAS για κάθε πρόβλημα στην $\#P$, αυτό π.χ. προκύπτει από το [27]. \square

Να παρατηρήσουμε ότι το ίδιο ισχύει και για την TotP, δηλ

Θεώρημα 5. Για κάθε $f \in \text{TotP}$ υπάρχει FPRAS αν $\text{NP}=\text{RP}$.

Απόδειξη. Η απόδειξη είναι η ίδια με πριν, αρκεί να παρατηρήσουμε επιπλέον ότι το #IS ανήκει στην TotP και δεν επιδέχεται FPRAS εκτός αν $\text{NP}=\text{RP}$ [27]. \square

Υπάρχουν δύο πολύ σημαντικά θεωρήματα σχετικά με το πολλαπλασιαστικό σφάλμα για αυτοαναγώγιμα (*self-reducible*) προβλήματα στην #P. Το πρώτο λέει ότι κάθε αυτοαναγώγιμη συνάρτηση στην #P είτε επιδέχεται FPRAS, είτε δεν μπορεί να υπολογιστεί ούτε καν με ένα πολυωνυμικά μεγάλο πολλαπλασιαστικό σφάλμα σε πολυωνυμικό χρόνο. Το δεύτερο λέει ότι η ύπαρξη FPRAS είναι ισοδύναμη με τη δυνατότητα σχεδόν ομοιόμορφης δειγματοληψίας από το σύνολο των λύσεων του εκάστοτε προβλήματος.

Θεώρημα 6. [69] Έστω μία $f \in \#P$ αυτοαναγώγιμη. Ένας αλγόριθμος πολυωνυμικού χρόνου με πολυωνυμικό πολλαπλασιαστικό σφάλμα για την f μπορεί να μετατραπεί σε FPRAS.

Θεώρημα 7. [69] Έστω $A \in \text{NP}$, έστω $\#A \in \#P$ η μετρητική του εκδοχή, και ας υποθέσουμε ότι το $\#A$ είναι αυτοαναγώγιμο. Έστω $S_A(x)$ το σύνολο των λύσεων του A με είσοδο x . Το $\#A$ επιδέχεται FPRAS αν και μόνο αν για κάθε $x \in \Sigma^*$ μπορούμε να πραγματοποιήσουμε σε πολυωνυμικό χρόνο σχεδόν ομοιόμορφη δειγματοληψία από το σύνολο S_A .

Τέλος, υπάρχουν τρεις κατηγορίες προβλημάτων στη #P σε σχέση με την δυνατότητα προσέγγισης [27]. Η πρώτη κλάση περιέχει εκείνα τα προβλήματα που είναι αλληλοαναγόμενα με το #SAT κάτω από αναγωγές που διατηρούν την προσέγγιση και επομένως είναι μη προσεγγίσιμα εκτός αν $\text{NP} = \text{RP}$. Η δεύτερη κλάση περιέχει τα προβλήματα που επιδέχονται FPRAS. Η τρίτη κλάση περιέχει τα προβλήματα που είναι αλληλοαναγόμενα με το πρόβλημα της καταμέτρησης ανεξάρτητων συνόλων όλων των μεγεθών ενός διμερούς γραφήματος, δηλαδή το #BIS. Η δυνατότητα προσέγγισης του τελευταίου εξακολουθεί να είναι ανοιχτό πρόβλημα.

Υπάρχει ένας μεγάλος αριθμός ερευνητικών άρθρων σχετικά με τους αλγόριθμους προσέγγισης και τη δυσκολία προσέγγισης για μεμονωμένα προβλήματα στη #P. Η βιβλιογραφία είναι τεράστια. Αναφέρουμε ενδεικτικά τα [30, 33, 76, 36, 46, 77, 25, 57, 29].

1.4.3 Δειγματοληψία και καταμέτρηση

Έστω ένα πεπερασμένο σύνολο A και ένα υποσύνολό του B . Εάν γνωρίζουμε το μέγεθος του A και μπορούμε να πραγματοποιήσουμε ομοιόμορφη δειγματοληψία από αυτό, τότε μπορούμε να προσεγγίσουμε το μέγεθος του B , λαμβάνοντας ένα ικανό πλήθος από δείγματα, δηλαδή στοιχεία του A , και υπολογίζοντας τι ποσοστό αυτών είναι στοιχεία του B . Το πλήθος των δειγμάτων που θα χρειαστούμε εξαρτάται από το μέγεθος του B . Όσο πιο μικρό είναι το μέγεθος του B τόσο περισσότερα δείγματα από το A θα χρειαστούμε προκειμένου να το προσεγγίσουμε.

Αυτή η μέθοδος λέγεται και απλή (naive) Monte Carlo.

Θεώρημα 8. [unbiased estimator lemma] Έστω A ένα πεπερασμένο σύνολο, $B \subseteq A$, και $p = \frac{|B|}{|A|}$.

Μπορούμε να προσεγγίσουμε το p παίρνοντας m δείγματα ομοιόμορφα από το A . Έστω t το πλήθος των δειγμάτων που ανήκουν και στο B . Ορίζουμε $\hat{p} = t/m$.

Αρκούν $m = \text{poly}(p^{-1}, \epsilon^{-1})$ δείγματα προκειμένου να λάβουμε μια προσέγγιση $\hat{p} = p(1 \pm \epsilon)$ με πιθανότητα τουλάχιστον $\frac{3}{4}$.

Απόδειξη.

$$\Pr[|\hat{p} - p| \geq \epsilon p] = \Pr[|\hat{p} - p|^2 \geq \epsilon^2 p^2] \leq \frac{E[|\hat{p} - p|^2]}{\epsilon^2 p^2} = \frac{\text{Var}[\hat{p}]}{\epsilon^2 p^2} \quad (1.1)$$

Το \hat{p} μπορεί να γραφτεί ως $\hat{p} = \frac{1}{m} \sum_{i=1}^m X_i$, όπου για κάθε i $X_i = 1$ αν το i -οστό δείγμα ανήκει στο B , αλλιώς $X_i = 0$. Τα X_i είναι ανεξάρτητα και ισόνομα, οπότε

$$\text{Var}[\hat{p}] = \text{Var}\left[\frac{1}{m} \sum_{i=1}^m X_i\right] = \frac{1}{m^2} \text{Var}\left[\sum_{i=1}^m X_i\right] = \frac{1}{m^2} \sum_{i=1}^m \text{Var}[X_i] = \frac{1}{m} \text{Var}[X_i] \quad (1.2)$$

όπου η προτελευταία ισότητα προκύπτει επειδή οι X_i είναι ανεξάρτητες, οπότε για κάθε $i \neq j$ $\text{Cov}[X_i, X_j] = 0$. Επίσης

$$\text{Var}[X_i] = E[X_i^2] - E[X_i]^2 = p - p^2. \quad (1.3)$$

Οπότε βάζοντας τις [1.2](#) και [1.3](#) στην [1.1](#) παίρνουμε

$$\Pr[|\hat{p} - p| \geq \epsilon p] \leq \frac{p - p^2}{m \epsilon^2 p^2} \leq \frac{1}{m \epsilon^2 p}$$

Για να είναι η τελευταία πιθανότητα το πολύ $\frac{1}{4}$, αρκεί να πάρουμε $m = \frac{4}{\epsilon^2 p}$ δείγματα.

Τέλος, σημειώνουμε ότι μπορούμε να μειώσουμε την πιθανότητα αποτυχίας από $1/4$ σε αυθαίρετα μικρό $\delta > 0$ επαναλαμβάνοντας την παραπάνω διαδικασία δειγματοληψίας ανεξάρτητα s φορές (όπου s μονός αριθμός δλδ $s = 2r + 1$ για κάποιο $r \in \mathbb{N}$) και παίρνοντας ως τελική εκτίμηση τη διάμεσο των s διαφορετικών εκτιμήσεων. Αρκούν $s = O(\log \delta)$ επαναλήψεις για να έχουμε πιθανότητα αποτυχίας δ .

Απόδειξη του τελευταίου ισχυρισμού: Έστω Y το πλήθος των επιτυχημένων εκτιμήσεων. Η Y ακολουθεί την διωνυμική $\text{Bin}(\frac{3}{4}, s)$. Η διάμεσος είναι αποτυχημένη εκτίμηση εάν έχουμε το πολύ r επιτυχημένες εκτιμήσεις.

$$\begin{aligned} \Pr[Y \leq r] &= \sum_{i=1}^r \binom{s}{i} \left(\frac{3}{4}\right)^i \left(\frac{1}{4}\right)^{s-i} = \\ &= \sum_{i=1}^r \binom{s}{i} \frac{3^i}{4^s} \leq \frac{3^r}{4^s} \sum_{i=1}^r \binom{s}{i} < \frac{3^r 2^s}{4^s} = \left(\frac{3}{4}\right)^r \frac{1}{2} \end{aligned}$$

□

Επομένως εάν το μέγεθος του A είναι εκθετικά μεγαλύτερο από το μέγεθος του B τότε χρειαζόμαστε εκθετικά πολλά δείγματα προκειμένου να προσεγγίσουμε το μέγεθος του B .

Ένα τέχνασμα που χρησιμοποιείται για να υπολογίσουμε προσεγγιστικά το μέγεθος ενός συνόλου B που μπορεί να είναι εκθετικά μικρό σε σχέση με το A , είναι να σπάσουμε το λόγο $\frac{|B|}{|A|}$ σε διαδοχικούς λόγους

$$\frac{|B|}{|A|} = \frac{|B|}{|A_k|} \cdot \frac{|A_k|}{|A_{k-1}|} \cdot \dots \cdot \frac{|A_1|}{|A|}$$

τέτοιους ώστε ο καθένας από αυτούς να είναι αρκετά μεγάλος, κι έτσι να χρειάζονται λίγα δείγματα για να προσεγγιστεί.

Αν το πλήθος k των υποσυνόλων που λαμβάνουν χώρα στην παραπάνω ισότητα είναι πολυωνυμικό, και κάθε υποσύνολο είναι πολυωνυμικά μεγαλύτερο από το προηγούμενό του, τότε συνολικά χρειάζεται πολυωνυμικός χρόνος για να προσεγγίσουμε τον αρχικό λόγο $\frac{|B|}{|A|}$ με σφάλμα $(1 \pm \epsilon)^{k+1}$.

Οπότε αυτό που απομένει είναι να πραγματοποιηθεί ομοιόμορφη δειγματοληψία από κάθε υποσύνολο A, A_1, \dots, A_k . Αυτή η δειγματοληψία συνήθως δεν είναι κάτι το τετριμμένο, και πραγματοποιείται με μια γενικότερη μέθοδο που λέγεται Markov Chain Monte Carlo, την οποία περιγράφουμε αναλυτικά παρακάτω.

1.5 Μαρκοβιανές αλυσίδες-Αλλαγές φάσης

1.5.1 Σταθμισμένη μέτρηση

Μια γενίκευση της καταμέτρησης στη #P είναι αυτή της σταθμισμένης ή σταθμισμένης μέτρησης, όπου δίνεται ένα πραγματικό βάρος σε κάθε λύση του εξεταζόμενου προβλήματος και ο στόχος είναι να υπολογιστεί το άθροισμα των βαρών όλων των λύσεων. Φυσικά, αυτά τα προβλήματα είναι συχνά εκτός της #P, αφού τα βάρη μπορεί να μην είναι φυσικοί αριθμοί.

Ορισμός 14. (σταθμισμένη μέτρηση) Έστω ένα πεπερασμένο σύνολο και έστω $w : A \rightarrow \mathbb{R}$ μια συνάρτηση βάρους. Το ζητούμενο είναι να υπολογιστεί το άθροισμα $Z = \sum_{a \in A} w(a)$.

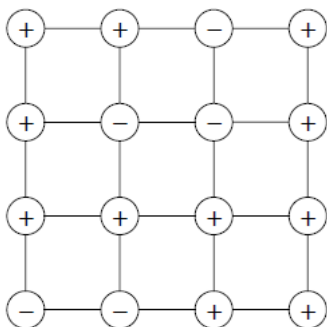
Είναι σαφές ότι κάθε πρόβλημα καταμέτρησης στην #P εμπίπτει στον παραπάνω ορισμό, όπου δίνεται βάρος 1 σε κάθε μονοπάτι αποδοχής της αντίστοιχης μηχανής Turing, και βάρος 0 σε κάθε μονοπάτι απόρριψης.

Πολλά προβλήματα από τη στατιστική φυσική ή από τη θεωρία πιθανοτήτων εμπίπτουν επίσης σε αυτή την τυποποίηση, π.χ. το μοντέλο Ising το οποίο περιγράφουμε παρακάτω, το hard-sphere μοντέλο, το hard-core μοντέλο το οποίο αντιστοιχεί σε σταθμισμένα ανεξάρτητα σύνολα ενός γραφήματος, το monomer-dimer μοντέλο το οποίο αντιστοιχεί σε σταθμισμένα ταιριάσματα ενός γραφήματος, το μοντέλο Potts το οποίο αντιστοιχεί σε σταθμισμένους χρωματισμούς ενός γραφήματος, κλπ. [16, 14, 18, 70, 80, 83], όπως επίσης προβλήματα υπολογισμών μέσων τιμών και περιθωρίων κατανομών πιθανότητας.

Βάρη αποδίδονται στα στοιχεία ενός (πιθανώς εκθετικά μεγάλου) συνόλου και ορίζεται μια κατανομή πιθανότητας πάνω σε αυτό το σύνολο, όπου οι πιθανότητες είναι ανάλογες προς τα βάρη, π.χ. η κατανομή Boltzmann για μοντέλα στατιστικής φυσικής. Ο στόχος είναι να υπολογιστεί ο συντελεστής κανονικοποίησης αυτής της κατανομής, γνωστή και ως *partition function*.

Πιο συγκεκριμένα αν έχουμε όπως πριν μια συνάρτηση βάρους $w : A \rightarrow \mathbb{R}$, και $Z = \sum_{a \in A} w(a)$, τότε μπορούμε να ορίσουμε μια κατανομή πιθανότητας $P : A \rightarrow \{0, 1\}$ ως εξής $P(a) = w(a)/Z$. Το Z καλείται συντελεστής κανονικοποίησης ή και συνάρτηση διαμερισμού (*partition function*), όρος που προέρχεται από τη στατιστική φυσική.

Παράδειγμα. Ising Model [42] Έχουμε ένα πλέγμα όπου κάθε κόμβος i παίρνει ένα spin $\sigma_i \in \{+, -\}$.



Η ενέργεια του συστήματος είναι $E(\sigma) = -\sum_{i \sim j} \sigma_i \sigma_j$, όπου $i \sim j$ συμβολίζει ζεύγος γειτονικών κόμβων.

Η *Boltzmann Distribution* είναι μία κατανομή πιθανότητας πάνω σε όλες τις διαμορφώσεις του συστήματος. Ορίζεται ως εξής.

$$\mu_\beta(\sigma) = \frac{1}{Z_\beta} e^{-\beta E(\sigma)}$$

Ο συντελεστής κανονικοποίησης $Z_\beta = \sum_{\sigma} e^{-\beta E(\sigma)}$ λέγεται και συνάρτηση διαμερισμού (*partition function*) του μοντέλου Ising.

Η πιο κοινή μέθοδος για την επίτευξη εκτιμήσεων συντελεστών κανονικοποίησης, καθώς και σταθμισμένων αθροισμάτων γενικά, είναι η αποκαλούμενη μέθοδος MCMC [38]. Η μέθοδος περιλαμβάνει το σχεδιασμό μιας μαρκοβιανής αλυσίδας που συγκλίνει στην επιθυμητή κατανομή. Στη συνέχεια, αυτή η μαρκοβιανή αλυσίδα χρησιμοποιείται για δειγματοληψία από αυτή την κατανομή.

Ο γνωστός κανόνας του Metropolis, τον οποίο θα περιγράψουμε πιο κάτω, μας παρέχει έναν ενιαίο τρόπο σχεδιασμού μαρκοβιανών αλυσίδων που συγκλίνουν σε μια επιθυμητή κατάσταση (αν και αυτός ο κανόνας δεν είναι ο μοναδικός τρόπος να σχεδιαστούν τέτοιες αλυσίδες). Παραδείγματα εφαρμογών του κανόνα του

Metropolis είναι η δειγματοληψία Gibbs, η προσομοιωμένη απόπτωση (simulated annealing), ο Glauber dynamics αλγόριθμος κλπ. [32, 59, 38].

Ο χρόνος σύγκλισης των μαρκοβιανών αλυσίδων τύπου Metropolis δεν είναι πάντοτε πολυωνυμικός. Γενικά, είναι ερώτημα ανεξάρτητου ενδιαφέροντος να προσδιοριστεί ο χρόνος σύγκλισης μιας μαρκοβιανής αλυσίδας.

Εκτός από τις μαρκοβιανές αλυσίδες που χρησιμοποιούνται για σχεδιασμό FPRAS, ένας δεύτερος βασικός τύπος αλγορίθμων που χρησιμοποιείται για την προσέγγιση των σταθμισμένων αθροισμάτων - με FPTAS, δηλ. ντετερμινιστικά, - είναι η οικογένεια των αλγορίθμων ανταλλαγής μηνυμάτων (message passing). Παραδείγματα τέτοιων αλγορίθμων είναι γνωστοί ως belief-propagation, sum-product algorithm, Viterbi algorithm, the cavity method, the correlation decay method. Για περισσότερες αναφορές δείτε το εξαιρετικό άρθρο [54].

Όλοι αυτοί οι αλγόριθμοι, αν και ανακαλύφθηκαν ανεξάρτητα από επιστήμονες διαφορετικών επιστημονικών περιοχών και για διαφορετικούς σκοπούς, ακολουθούν μια αναδρομή του ίδιου τύπου, και μπορούν να θεωρηθούν ως δυναμικός προγραμματισμός με κύκλους. Η πειραματική τους απόδοση είναι πέρα από κάθε προσδοκία. Κάποιες εργασίες έχουν γίνει προς την κατεύθυνση της θεωρητικής αιτιολόγησής τους, αλλά η πλήρης κατανόηση του λόγου της επιτυχίας ή της αποτυχίας τους και των συνθηκών υπό τις οποίες επιτυγχάνουν εξακολουθεί να είναι ανοικτό ερώτημα. Δεν θα ασχοληθούμε με αυτό το ζήτημα σε αυτή τη διατριβή, αλλά το αναφέρουμε για λόγους πληρότητας.

1.5.2 Βασικές στοιχεία για Μαρκοβιανές αλυσίδες

Θα μας απασχολήσουν μόνο μαρκοβιανές αλυσίδες σε πεπερασμένο χώρο καταστάσεων.

Έστω \mathcal{X} ένα πεπερασμένο σύνολο (το οποίο θα καλούμε χώρο καταστάσεων της μαρκοβιανής αλυσίδας), και έστω μια στοχαστική διαδικασία, δηλαδή μια οικογένεια τυχαίων μεταβλητών $\{X_n\}_{n \in \mathbb{N}}$ από ένα χώρο πιθανότητας Ω στο \mathcal{X} , (δηλαδή $\forall i \in \mathbb{N} X_i : \Omega \rightarrow \mathcal{X}$).

Ορισμός 15 (Markov Chain). *Μαρκοβιανή αλυσίδα καλείται μία στοχαστική διαδικασία $\{X_n\}_{n \in \mathbb{N}}$ με την ιδιότητα $\forall x, y, v_0, \dots, v_{n-1} \in \mathcal{X}$*

$$\Pr[X_{n+1} = y | X_0 = v_0, \dots, X_{n-1} = v_{n-1}, X_n = x] = \Pr[X_{n+1} = y | X_n = x]$$

Όταν μια μαρκοβιανή αλυσίδα σε πεπερασμένο χώρο καταστάσεων είναι ομογενής στο χρόνο, τότε μπορεί να οριστεί μέσω ενός πίνακα P , οποίος καλείται *πίνακας μεταβάσεων (transition matrix)*, ως εξής $P_{ij} = \Pr[X_{n+1} = j | X_n = i]$.

Στάσιμη κατανομή (stationary distribution) μιας μαρκοβιανής αλυσίδας καλείται μια κατανομή πιθανότητας π πάνω στο χώρο καταστάσεων, με την ιδιότητα $\pi P = \pi$.

Μια μαρκοβιανή αλυσίδα καλείται *μη αναγώγιμη (irreducible)* όταν το γράφημα που αντιστοιχεί στον πίνακα μεταβάσεων είναι ισχυρά συνεκτικό, δηλ $\forall x, y \in \mathcal{X} \exists t \geq 0 P_{xy}^t > 0$.

Μια μη αναγώγιμη μαρκοβιανή αλυσίδα καλείται *απεριοδική* (*aperiodic*) όταν δεν είναι περιοδική. Μια μη αναγώγιμη αλυσίδα είναι περιοδική με περίοδο δ όταν ο χώρος καταστάσεων μπορεί να χωριστεί σε δ ομάδες έτσι ώστε σε κάθε βήμα να μεταβαίνει από τις καταστάσεις μιας ομάδα σε καταστάσεις μόνο μίας άλλης ομάδας, κάνοντας τελικά κύκλο μεταξύ των ομάδων. Πχ αν το γράφημα που αντιστοιχεί στον πίνακα μεταβάσεων είναι διμερές, τότε η αλυσίδα έχει περίοδο 2. Για να γίνει μια αλυσίδα απεριοδική, αρκεί να υπάρχει ένα self loop. Τυπικά, για κάθε αλυσίδα, αναγώγιμη ή μη, ορίζεται η περίοδος k μίας κατάστασης x ως εξής $k = \gcd\{n > 0 : \Pr[X_n = x | X_0 = x] > 0\}$, όπου \gcd συμβολίζει το μέγιστο κοινό διαιρέτη. Κάθε συνεκτική συνιστώσα του γραφήματος της αλυσίδας έχει καταστάσεις με την ίδια περίοδο. Αν η αλυσίδα είναι μη αναγώγιμη, όλες οι καταστάσεις έχουν την ίδια περίοδο δ . Η αλυσίδα καλείται απεριοδική αν υπάρχει έστω και μια κατάσταση με περίοδο 1.

Θεώρημα 9. *Αν μία μαρκοβιανή αλυσίδα είναι μη αναγώγιμη και απεριοδική, τότε έχει μοναδική στάσιμη κατανομή. Επιπλέον για κάθε κατανομή π_0 πάνω στο χώρο καταστάσεων, ισχύει $\pi_0 P^t \rightarrow \pi$ καθώς $t \rightarrow \infty$, δηλαδή η στάσιμη κατανομή είναι επίσης και οριακή κατανομή της αλυσίδας.*

Καλείται *χρόνος σύγκλισης* (*mixing time*) $\tau(\epsilon)$ μιας μαρκοβιανής αλυσίδας, το ελάχιστο πλήθος βημάτων που χρειάζονται για να φτάσουμε ϵ κοντά στην οριακή κατανομή ξεκινώντας από οποιαδήποτε αρχική κατανομή π_0 πάνω στο χώρο καταστάσεων. Δηλαδή αν $\pi_t = \pi_0 P^t$ τότε $\tau_{\pi_0}(\epsilon) = \min_t \{\|\pi_t - \pi\| \leq \epsilon\}$, όπου η νόρμα $\|\cdot\|$ εδώ συμβολίζει την στατιστική απόσταση δύο κατανομών, ή πιο συγκεκριμένα $\|p_1 - p_2\| = \frac{1}{2} \sum_{x \in \mathcal{X}} |p_1(x) - p_2(x)|$. Οπότε $\tau(\epsilon) = \max_{\pi_0} \{\tau_{\pi_0}(\epsilon)\}$, όπου το μέγιστο λαμβάνεται μεταξύ όλων των δυνατών κατανομών πάνω στο χώρο των καταστάσεων. Συχνά ως χρόνος σύγκλισης τ_{mix} μιας αλυσίδας καλείται το $\tau(1/4)$.

Υπάρχουν πολλά λήμματα και μέθοδοι απόδειξης για να φράξει κανείς το χρόνο σύγκλισης μιας μαρκοβιανής αλυσίδας.

Σε αυτή τη διατριβή διαπιστώσαμε ότι τα πιο κατάλληλα λήμματα για να φράξουμε το χρόνο σύγκλισης των μαρκοβιανών αλυσίδων που μελετούμε, είναι δύο λήμματα που σχετίζονται με την αγωγιμότητα μιας μαρκοβιανής αλυσίδας. Η διαισθητική ιδέα αυτών των λημμάτων είναι ότι μια μαρκοβιανή αλυσίδα συγκλίνει γρήγορα εάν και μόνο εάν δεν υπάρχουν "σημεία συμφόρησης" στο γράφημα του χώρου καταστάσεων.

Έστω $\{X_t\}_{t \geq 0}$ μια μαρκοβιανή αλυσίδα σε ένα πεπερασμένο χώρο καταστάσεων \mathcal{X} με πιθανότητες μετάβασης p_{ij} .

Έστω $p_x^{(t)}$ η κατανομή της X_t ξεκινώντας από την κατάσταση x , δηλαδή την κατανομή που δίνει όλη τη μάζα πιθανότητας στο x .

Έστω π η στάσιμη κατανομή, και έστω $\tau_x(\epsilon) = \min\{t : \|p_x^{(t)} - \pi\| \leq \epsilon\}$ ο χρόνος σύγκλισης ξεκινώντας από την κατάσταση x .

Μια εργοδική μαρκοβιανή αλυσίδα (δλδ μη αναγώγιμη και απεριοδική) λέγεται χρονικά αναστρέψιμη αν $\forall i, j \in \mathcal{X}, p_{ij}\pi_i = p_{ji}\pi_j$.

Έστω H ο υποκείμενος γράφος της αλυσίδας, στου οποίου τις ακμές δίνουμε βάρος $w_{ij} = p_{ij}\pi_i = p_{ji}\pi_j$ για κάθε $i, j \in \mathcal{X}$.

Μια μαρκοβιανή αλυσίδα λέγεται τεμπέλικη αν $\forall i \in \mathcal{X}, p_{ii} \geq \frac{1}{2}$.

Στο [69] ορίζεται η αγωγιμότητα μια χρονικά αναστρέψιμης μαρκοβιανής αλυσίδας, ως εξής.

Ορισμός 16. Έστω $Y \subseteq \mathcal{X}$. Ορίζουμε

$$\Phi(Y) = \frac{\sum_{i \in Y, j \notin Y} w_{ij}}{\sum_{i \in Y} \pi_i}$$

Η αγωγιμότητα (conductance) της μαρκοβιανής αλυσίδας είναι

$$\Phi(H) = \min \Phi(Y)$$

όπου το ελάχιστο λαμβάνεται μεταξύ όλων των $Y \subseteq \mathcal{X}$ για τα οποία $0 < \sum_{i \in Y} \pi_i \leq \frac{1}{2}$.

Παρατηρήστε ότι η αγωγιμότητα μιας μαρκοβιανής αλυσίδας είναι μεγάλη όταν ο υποκείμενος γράφος είναι καλά συνδεδεμένος, χωρίς σημεία συμφόρησης. Τα παρακάτω λήμματα δηλώνουν ότι μια μαρκοβιανή αλυσίδα συγκλίνει γρήγορα όταν η αγωγιμότητα είναι μεγάλη, και συγκλίνει αργά όταν η αγωγιμότητα είναι μικρή.

Λήμμα 1. [69] Για κάθε τεμπέλικη, χρονικά αναστρέψιμη μαρκοβιανή αλυσίδα

$$\tau_x(\epsilon) \leq \text{const} \times \left[\frac{1}{\Phi(H)^2} (\log \pi_x^{-1} + \log \epsilon^{-1}) \right].$$

Λήμμα 2. Για κάθε μαρκοβιανή αλυσίδα και κάθε $Y \subseteq \mathcal{X}$ με $\pi(Y) \leq \frac{1}{2}$

$$\tau_{mix} \geq \frac{1}{4\Phi(Y)}$$

1.5.3 Δειγματοληψία με τη μέθοδο Markov Chain Monte Carlo

Έστω π μια κατανομή πιθανότητας πάνω σε ένα πεπερασμένο σύνολο \mathcal{X} . Το ζητούμενο είναι να λάβουμε ένα στοιχείο του \mathcal{X} ακολουθώντας την κατανομή π . Η μέθοδος Markov Chain Monte Carlo το επιτυγχάνει αυτό χρησιμοποιώντας μια μαρκοβιανή αλυσίδα με στάσιμη κατανομή τη ζητούμενη. Η μέθοδος συνοψίζεται ως εξής.

1. Βρες μια μαρκοβιανή αλυσίδα P με στάσιμη κατανομή π .
2. Ξεκίνα από μια αυθαίρετη κατάσταση $x \in \mathcal{X}$.
3. Πήγαινε στην κατάσταση $y \in \mathcal{X}$ με πιθανότητα P_{xy} .
4. Επανάλαβε το προηγούμενο βήμα για τ_{mix} βήματα.
5. Επίστρεψε το στοιχείο στο οποίο βρίσκεσαι σε αυτό το βήμα, δηλ το $X_{\tau_{mix}}$.

Υπάρχουν πολλές εφαρμογές της δειγματοληψίας με τη μέθοδο Markov Chain Monte Carlo (και γενικά της υπολογιστικής δειγματοληψίας), όπως για παράδειγμα είναι (α) η δημιουργία τυχαίων συνδυαστικών αντικειμένων για έλεγχο αλγορίθμων και έλεγχο εικασιών, (β) πιθανοτικές κατασκευές όπως οι LDPC (low density parity check) κώδικες διόρθωσης λαθών, (γ) η προσομοίωση φυσικών συστημάτων για τη στατιστική φυσική, (δ) ο υπολογισμός περιθωρίων κατανομών, αναμενόμενων τιμών, συναρτήσεων καταμερισμού (partition functions), (ε) στατιστική συμπερασματολογία (statistical inference), πρόβλεψη (prediction), σύγκριση μοντέλων (model comparison), (ζ) καταμέτρηση στην #P μέσω ομοιόμορφης δειγματοληψίας, όπως αναφέραμε στο θεώρημα 1.7.

Έστω, όπως προηγουμένως, $w : A \rightarrow \mathbb{R}$, $Z = \sum_{a \in A} w(a)$, και κατανομή $P : A \rightarrow \{0, 1\}$ τέτοια ώστε $P(a) = w(a)/Z$, σύμφωνα με την οποία επιθυμούμε να πραγματοποιήσουμε δειγματοληψία.

Μερικά ερωτήματα που αφορούν στην θεωρία πολυπλοκότητας είναι τα εξής.

- Μπορούμε να πραγματοποιήσουμε δειγματοληψία σύμφωνα με την P με τη μέθοδο MCMC αποδοτικά; Με άλλα λόγια, υπάρχει μαρκοβιανή αλυσίδα που να συγκλίνει γρήγορα στην P ;
- Μπορούμε να υπολογίσουμε τον συντελεστή κανονικοποίησης αποδοτικά;
- Είναι ο υπολογισμός του Z #P-hard, και υπό ποιές αναγωγές;
- Δεδομένης μιας μαρκοβιανής αλυσίδας, ποιός είναι ο χρόνος σύγκλισης της στην οριακή της κατανομή; Ποιά η οριακή της κατανομή;

1.5.4 Ο κανόνας του Metropolis

Ο Metropolis πρότεινε μια μέθοδο σχεδιασμού μαρκοβιανών αλυσίδων που συγκλίνουν σε μια επιθυμητή κατανομή πιθανότητας.

Η Metropolis-Hastings [59][38] μέθοδος είναι η εξής.

Έστω \mathcal{X} ένα πεπερασμένο σύνολο, και έστω $\pi : \mathcal{X} \rightarrow \mathbb{R}$ μια κατανομή πιθανότητας πάνω στο \mathcal{X} . Το \mathcal{X} θα είναι ο χώρος καταστάσεων της μαρκοβιανής μας αλυσίδας.

1. Ορίζουμε αυθαίρετα ένα γράφημα του οποίου κόμβοι είναι τα στοιχεία του \mathcal{X} . Αυτό θα λέγεται γράφημα των διαμορφώσεων (configuration graph).
2. Έστω ότι είμαστε στην κατάσταση i . Διαλέγουμε ένα γείτονα j του i με πιθανότητα $k(i, j) > 0$. Οι αριθμοί k θα πρέπει να ικανοποιούν $\sum_j k(i, j) \leq 1$.
3. Αν η j είναι καλύτερη διαμόρφωση από την i , δλδ. αν $\pi(j) > \pi(i)$, τότε πάμε στην j με πιθανότητα $p = 1$. Αλλιώς πάμε στην j με πιθανότητα $p = \frac{\pi(j)}{\pi(i)}$, και με πιθανότητα $1 - p$ παραμένουμε στην i .

Παρατηρήσεις

- Η στάσιμη κατανομή της παραπάνω μαρκοβιανής αλυσίδας είναι η π .
- Το μη τετριμμένο κομμάτι του αλγορίθμου είναι ο σχεδιασμός της δομής γειτονιάς, η οποία δίνει τον κανόνα επιλογής της κάθε επόμενης κατάστασης. Αυτή η δομή είναι διαφορετική για κάθε πρόβλημα, και υπάρχουν φυσικά πολλές δυνατές. Κάποιες συνήθεις στρατηγικές σχεδιασμού, όταν ο χώρος των καταστάσεων αποτελείται από το σύνολο όλων των αναθέσεων τιμών σε ένα σύνολο μεταβλητών (όπως συμβαίνει π.χ. με το SAT και το coloring), είναι να αλλάζουμε την τιμή σε μία μεταβλητή τη φορά, ή σε ένα block μεταβλητών τη φορά.
- Αποδεικτικά το δύσκολο κομμάτι είναι να φράξει κανείς το χρόνο σύγκλισης της αλυσίδας.
- Ο χρόνος σύγκλισης εξαρτάται από τα ενεργειακά φράγματα που ενδεχομένως να υπάρχουν, όπως επίσης και από τη δομή του γραφήματος διαμορφώσεων που θα επιλέξουμε.
- Ο κανόνας στο βήμα 3 που λέει ότι αν η καινούρια διαμόρφωση είναι χειρότερη από την παλιά, πηγαίνουμε σε αυτή με κάποια πιθανότητα, χρησιμεύει στο να δραπετεύσουμε από τυχόντα τοπικά ελάχιστα.

1.5.5 Αλλαγές φάσης

Μια αλλαγή φάσης είναι ένα σημείο όπου μια πραγματική (ή μιγαδική) συνάρτηση δεν είναι αναλυτική, π.χ. ένα σημείο όπου μια συνάρτηση είναι ασυνεχής (αλλαγή φάσης πρώτης τάξης), ή όπου εμφανίζεται κάποια κορυφή (αλλαγή φάσης δεύτερης τάξης).

Οι αλλαγές φάσης συνήθως υποδηλώνουν την ύπαρξη κάποιου φαινομένου, όπως η μετάβαση του νερού από την υγρή κατάσταση στον πάγο σε θερμοκρασία 0°C [31].

Όσον αφορά τις ποσότητες όπως οι partition functions και τα σταθμισμένα αθροίσματα γενικά, αν εξαρτήσουμε τα βάρη από μια παράμετρο, συμβαίνει συχνά η τιμή αυτού του αθροίσματος, ή η πολυπλοκότητα του υπολογισμού του ή ο χρόνος λειτουργίας μιας αντίστοιχης μαρκοβιανής αλυσίδας πάνω στο σύνολο των στοιχείων του οποίου τα βάρη αθροίζουμε, να εμφανίζουν αλλαγή φάσης σε κάποια τιμή της παραμέτρου.

Παράδειγμα. Ο Glauber dynamics για το Ising Model, και αλλαγές φάσης. Υπενθυμίζουμε το μοντέλο: έχουμε ένα πλέγμα όπου κάθε κόμβος i παίρνει ένα spin $\sigma_i \in \{+, -\}$. Η ενέργεια του συστήματος είναι $E(\sigma) = -\sum_{i \sim j} \sigma_i \sigma_j$. Η Boltzmann distribution για το μοντέλο Ising ορίζεται ως εξής.

$$\mu_\beta(\sigma) = \frac{1}{Z_\beta} e^{-\beta E(\sigma)}$$

Ο συντελεστής κανονικοποίησης Z_β λέγεται partition function του Ising model.

Παρατηρήστε ότι όταν $\beta \rightarrow 0$, τότε η μ τείνει να είναι ομοιόμορφη σε όλες τις καταστάσεις, και όταν $\beta \rightarrow \infty$ η μ τείνει να δώσει όλη τη μάζα πιθανότητας στις καταστάσεις ελάχιστης ενέργειας. Το β λέγεται επίσης και αντίστροφη θερμοκρασία ($\beta = \frac{1}{k_B T}$, όπου k_B η σταθερά Boltzmann).

Σε χαμηλή θερμοκρασία T έχουμε μια τακτική (*ordered*) φάση, όπου όλα τα spin τείνουν να είναι ίδια. Σε υψηλή T έχουμε μια άτακτη (*disordered*) φάση, όπου όλες οι διαμορφώσεις είναι σχεδόν ισοπίθανες. Η μετάβαση από την τακτική στην άτακτη φάση δεν συμβαίνει ομαλά. Η partition function παρουσιάζει αλλαγή φάσης σε ένα σημείο β_c [64]. (Σε αντίθεση όταν το πλέγμα είναι μονοδιάστατο αποδεικνύεται ότι δεν υπάρχει αλλαγή φάσης και η μετάβαση από την τακτική στην άτακτη φάση γίνεται ομαλά.)

Ο αλγόριθμος Glauber dynamics (ο οποίος είναι μαρκοβιανή αλυσίδα τύπου Metropolis) ορίζεται ως εξής:

- Διάλεξε $u \in V$ ομοιόμορφα τυχαία
- Θέσε $u = +$ με πιθανότητα $Pr[u = +] = \frac{e^{\beta(a-\theta)}}{e^{\beta(a-\theta)} + e^{\beta(\theta-a)}}$

όπου a και θ είναι το πλήθος των γειτόνων του u με spin '-' και '+' αντίστοιχα.

Αποδεικνύεται στο [58] ότι ο χρόνος σύγκλισης αυτής της μαρκοβιανής αλυσίδας είναι

- $O(\log n)$ if $\beta < \beta_c$
- $e^{\Omega(\sqrt{n})}$ if $\beta > \beta_c$

Οπότε παρατηρούμε ότι η φυσική αλλαγή φάσης ταυτίζεται με την αλλαγή φάσης ως προς την πολυπλοκότητα του αλγορίθμου Glauber dynamics! (αλλά δεν συμβαίνει με όλα τα προβλήματα αυτό).

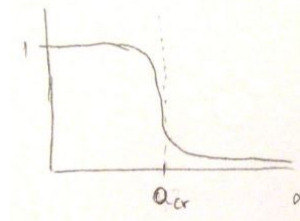
Όπως στη φυσική, η ύπαρξη μιας αλλαγής φάσης υποδεικνύει την ύπαρξη κάποιου φυσικού φαινομένου, στη θεωρητική πληροφορική είναι ένα ενδιαφέρον θέμα να κατανοήσουμε το νόημα και τη φύση μιας αλλαγής φάσης. Υπάρχει μια τέτοια αλλαγή φάσης για λόγους που εξηγούνται από τη θεωρία πληροφορίας, για υπολογιστικούς λόγους, για λόγους διακοπής της εργοδικότητας, σπάσιμο συμμετρίας ή για άλλους λόγους; Μπορούν αυτές οι μεταβάσεις φάσεων να μας βοηθήσουν να κατανοήσουμε την υπολογιστική δυσκολία των προβλημάτων;

Τέτοια μακροπρόθεσμα ζητήματα δεν έχουν ακόμη επιλυθεί. Προς το παρόν το κύριο ενδιαφέρον των περισσότερων επιστημόνων είναι να ανακαλύψουν πειραματικά και να αποδείξουν αυστηρά τέτοια φαινόμενα.

1.5.6 Ένα φαινόμενο διασκορπισμού λύσεων για το τυχαίο SAT

Ορισμένες αλλαγές φάσεων έχουν ανακαλυφθεί και έχουν αποδειχθεί αυστηρά για το random SAT. Έστω n ο αριθμός των μεταβλητών ενός τύπου boolean σε συζευκτική κανονική μορφή (CNF) και έστω m ο αριθμός των παρενθέσεων του

(clauses). Ας καλέσουμε πυκνότητα μιας φόρμουλας την ποσότητα $a = m/n$. Μερικοί επιστήμονες που χρησιμοποιούν τις μεθόδους που έχουμε ήδη αναφέρει από τη στατιστική φυσική (δηλαδή MCMC και την cavity μέθοδο) μελέτησαν τη συμπεριφορά μιας τυχαίας φόρμουλας με πυκνότητα a . Για το 3-SAT ανακάλυψαν την ακόλουθη αλλαγή φάσης στο $a_{cr} = 4.2$ [20, 60].

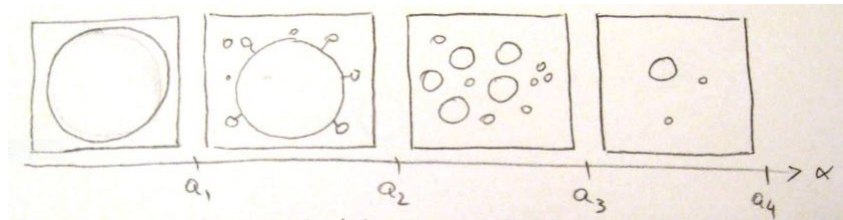


Για μια τυχαία φόρμουλα ϕ , για κάποιο μικρό $\epsilon > 0$ ισχύει με μεγάλη πιθανότητα

- αν $a < 4.2 - \epsilon$ τότε η ϕ είναι ικανοποιήσιμη
- αν $a > 4.2 - \epsilon$ τότε η ϕ είναι μη ικανοποιήσιμη

Αργότερα αποδείχθηκε αυστηρά για το k -SAT ότι $a_{cr} = 2^{k-1} \ln 2 - 2$ [3].

Επιπλέον, ανακαλύφθηκε η ακόλουθη εικόνα σχετικά με το χώρο των λύσεων σε μια τυπική τυχαία φόρμουλα, καθώς μεταβάλλουμε την παράμετρο της πυκνότητας



Καθώς αυξάνουμε την πυκνότητα, το σύνολο ικανοποιητικών αναθέσεων μιας τυπικής τυχαίας φόρμουλας, διαχωρίζεται σε ομάδες που είναι ευρέως διάσπαρτες στο χώρο όλων των δυνατών αναθέσεων.

Πριν το a_1 σχεδόν όλες οι αναθέσεις είναι ικανοποιητικές.

Στο a_2 ο χώρος των λύσεων, δηλαδή των ικανοποιητικών αναθέσεων, διαχωρίζεται σε ένα εκθετικά μεγάλο πλήθος από ομάδες οι οποίες είναι διάσπαρτες στο χώρο όλων των αναθέσεων. Σε αυτή την περιοχή οι μέχρι τώρα γνωστοί αλγόριθμοι που βασίζονται σε μαρκοβιανές αλυσίδες, αποτυγχάνουν.

Ο λόγος της αποτυχίας τους είναι καταρχάς ότι για μια φόρμουλα στην περιοχή $a > a_2$ δεν μπορούμε να βρούμε ούτε μία ικανοποιητική ανάθεση σε πολυωνυμικό χρόνο, αλλά ακόμα κι αν μας δοθεί κάποια λύση μέσα σε κάποια ομάδα λύσεων, οι ομάδες φαίνονται ασυσχέτιστες μεταξύ τους και δεν μπορούμε να βρούμε άλλες ομάδες σε πολυωνυμικό χρόνο. Με άλλα λόγια, δεν γνωρίζουμε πώς μπορεί να

γίνει σχεδίαση μη αναγώγιμων μαρκοβιανών αλυσίδων που να έχουν σαν χώρο καταστάσεων το σύνολο ικανοποιητικών αναθέσεων μιας φόρμουλας με πυκνότητα σε αυτή την περιοχή του a .

Αποτελεί έκπληξη το γεγονός ότι η cavity method λειτουργεί σωστά μέχρι και το a_3 . Αυτό συμβαίνει επειδή η λεγόμενη "replica symmetry ansatz" ισχύει μέχρι και το a_3 , δηλαδή $\lim_{n \rightarrow \infty} E[\ln Z/n] = \lim_{n \rightarrow \infty} \ln E[Z]/n$, και η cavity method μπορεί να υπολογίζει το $E[Z]$, (όπου εδώ η partition function Z ισούται με το πλήθος των ικανοποιητικών αναθέσεων της φόρμουλας εισόδου). Δεν θα επεκταθούμε σε αυτό το θέμα. Το αναφέρουμε για λόγους πληρότητας αυτής της ενότητας.

Στο a_3 το σύνολο ικανοποιητικών αναθέσεων αρχίζει να κυριαρχείται από ένα μικρό αριθμό ομάδων. Όλες οι μέθοδοι αποτυγχάνουν σε αυτήν την περιοχή, και οι φόρμουλες με πυκνότητα σε αυτή την περιοχή του a θεωρούνται ως τα πιο δύσκολα στιγμιότυπα του SAT.

Τέλος στο a_4 έχουμε το προαναφερθέν όριο ικανοποιησιμότητας.

Για περισσότερα πάνω σε αυτό το θέμα δείτε π.χ. τα [2, 1, 4].

Συμπέρασμα Αυτό που θέλουμε ο αναγνώστης να θυμάται από αυτήν την υποενότητα είναι ότι η διάσπαση του χώρου των λύσεων μιας τυχαίας φόρμουλας εξηγεί το λόγο της αποτυχίας των μέχρι τώρα γνωστών αλγορίθμων για το SAT που βασίζονται σε μαρκοβιανές αλυσίδες.

Κεφάλαιο 2

TotP-Πληρότητα

Η TotP είναι μια υποκλάση της #P που περιέχει όλα τα αυτοαναγώγιμα προβλήματα με εύκολη απόφαση ύπαρξης λύσης. Περιέχει πολλά ενδιαφέροντα προβλήματα από πολλές επιστημονικές περιοχές.

Οι Cook αναγωγές θολώνουν τις δομικές διαφορές μεταξύ των προβλημάτων καταμέτρησης, π.χ. το PERMANENT είναι #P-πλήρες, αλλά ανήκει επίσης στην TotP, επομένως απαιτούνται αυστηρότερες αναγωγές προκειμένου να χαρακτηριστεί πλήρως η πολυπλοκότητα ενός προβλήματος μέτρησης: οι λεγόμενες φειδωλές (parsimonious) αναγωγές, οι οποίες είναι εκείνες που διατηρούν ακριβώς τις τιμές των συναρτήσεων.

Η ύπαρξη TotP-πλήρων προβλημάτων κάτω από φειδωλές αναγωγές ήταν ένα ανοιχτό πρόβλημα εδώ και δέκα περίπου χρόνια. Ο πρώτος σκοπός αυτής της εργασίας είναι να παρουσιάσει τα πρώτα τέτοια προβλήματα (κεφάλαιο 2). Αυτά τα προβλήματα σχετίζονται με την ικανοποίηση Boolean κυκλωμάτων (συγκεκριμένα το #tree-monotone-circuit-SAT) και τύπων (δηλαδή το #clustered-monotone-SAT ή #CM-SAT) και με το πρόβλημα της εκτίμησης του μεγέθους του δέντρου μιας backtracking διαδικασίας (συγκεκριμένα το Size-Of-Subtree).

Συζητάμε κάποιες συνεπαγωγές των αποτελεσμάτων μας σε σχέση με την πολυπλοκότητα και προσεγγισιμότητα των μετρητικών προβλημάτων γενικότερα. ¹

2.1 Εισαγωγή

Από τη στιγμή που ο Valiant εισήγαγε την #P [76], την κλάση των συναρτήσεων που μετράει τον αριθμό των μονοπατιών αποδοχής μιας NPTM (Nondeterministic Polynomial Time Turing Machine), ένα πλήθος από κλάσεις προβλημάτων καταμέτρησης προέκυψαν στη βιβλιογραφία. Στο [61] ορίστηκε η κλάση #PE, ως η υποκλάση της #P που περιέχει όλες τις συναρτήσεις της #P με εύκολη απόφαση ύπαρξης λύσης, δηλαδή, για μια συνάρτηση $f \in \#PE$ το πρόβλημα “είναι το $f(x)$ μη μηδενικό;” είναι στο P. Η #PE περιέχει σημαντικά προβλήματα όπως το PERMANENT [76], μια ειδική περίπτωση του οποίου ισοδυναμεί με την καταμέτρηση

¹Μέρος του κεφαλαίου αυτού εμφανίστηκε στο [11]

των τέλειων ταιριασμάτων σε διμερή γραφήματα. Ένα άλλο γνωστό μέλος της #PE είναι το #DNF-SAT, δηλαδή το πρόβλημα της καταμέτρησης ικανοποιητικών αναθέσεων σε boolean DNF φόρμουλες. Για περισσότερα τέτοια προβλήματα βλέπε [77]. Συγκεκριμένα δείχθηκε στο [76, 77] ότι το PERMANENT, το #DNF-SAT, καθώς και διάφορα άλλα προβλήματα που παρουσιάζονται στο [77] είναι #P-πλήρη, δείχνοντας ότι η μέτρηση του πλήθους των λύσεων είναι δυσκολότερη από την απόφαση ύπαρξης λύσης για όλα αυτά τα προβλήματα.

Μια υποκλάση της #PE, η TotP, ορίστηκε ως η κλάση των συναρτήσεων που υπολογίζουν τον συνολικό αριθμό μονοπατιών του δέντρου υπολογισμού μιάς δυαδικής NPTM μείον ένα [47]. Αντιστοίχως, για $f \in \text{TotP}$, το $f(x)$ είναι ο αριθμός διακλαδώσεων του δέντρου υπολογισμού μιας δυαδικής NPTM. Η TotP περιέχει το PERMANENT και το #DNF-SAT, καθώς και όλα τα αυτοαναγωγίμα προβλήματα της #PE υπό μια φυσιολογική έννοια αυτοαναγωγιμότητας για προβλήματα καταμέτρησης. Είναι ενδιαφέρον το γεγονός ότι τα προβλήματα στην TotP έχουν διαφορετική κατάσταση προσεγγισιμότητας. Συγκεκριμένα, η TotP περιέχει προσεγγίσιμα προβλήματα (π.χ. #DNF-SAT), προβλήματα που είναι #P-πλήρη υπό αναγωγές που διατηρούν την προσέγγιση, και επομένως δεν είναι προσεγγίσιμα εκτός αν $\text{NP}=\text{RP}$ (π.χ. το πρόβλημα υπολογισμού του πλήθους ανεξαρτήτων συνόλων όλων των μεγεθών ενός γραφήματος), το οποίο συμβολίζεται #IS), καθώς και προβλήματα άγνωστης προσεγγισιμότητας, που εικάζεται ότι είναι "ενδιάμεσα", δηλαδή δεν είναι προσεγγίσιμα αλλά ούτε και πλήρη υπό αναγωγές που διατηρούν την προσέγγιση (π.χ. # (ανεξάρτητα σύνολα όλων των μεγεθών διμερών γραφημάτων), συμβολικά #Bis).

Είναι γνωστό ότι η #PE περιέχει την TotP [47] και επιπλέον ότι η TotP είναι ακριβώς το κλείσιμο κατά Karp των αυτοαναγωγίμων συναρτήσεων της #PE [62]. Σημειώστε ότι τα αυτοαναγωγίμα προβλήματα που μετριοούνται με προσέγγιση ενός πολυωνυμικού παράγοντα επιδέχονται και FPRAS και το πρόβλημα απόφασης τους ανήκει στην RP. Ομοίως, η καταμέτρηση των προβλημάτων με ένα PTAS έχουν αντίστοιχο πρόβλημα απόφασης στο P. Τα περισσότερα (αν όχι όλα) γνωστά προσεγγίσιμα προβλήματα είναι στην #PE [62].

Υπάρχει ένας μεγάλος αριθμός αυτοαναγωγίμων προβλημάτων με εύκολη απόφαση που είναι επομένως (από το [62]) στην TotP: μέτρηση ταιριασμάτων σε γραφήματα, ο υπολογισμός των permanent και determinant ενός πίνακα, ο υπολογισμός της partition function διαφόρων μοντέλων από τη στατιστική φυσική, όπως το μοντέλο Ising και το hard core model όταν τα βάρη είναι ακέραια, η μέτρηση των χρωματισμών ενός γραφήματος με αριθμό χρωμάτων μεγαλύτερο από τον μέγιστο βαθμό του γραφήματος, η μέτρηση του πλήθους των βάσεων ενός matroid, ο υπολογισμός του όγκου ενός κυρτού σώματος, η μέτρηση του πλήθους ανεξαρτήτων συνόλων και πολλά άλλα. Τα αποτελέσματα για TotP-πληρότητα μπορούν να ρίξουν φως στην πολυπλοκότητα και την προσεγγισιμότητα όλων αυτών των προβλημάτων και να βοηθήσουν να αντιμετωπιστούν όλα αυτά τα προβλήματα με ενιαίο τρόπο.

Όσον αφορά αποτελέσματα πληρότητας, όπως αναφέρθηκε παραπάνω, η TotP περιέχει κάποια #P-πλήρη προβλήματα που είναι συνεπώς και TotP-πλήρη. Αυτό

το παράδοξο οφείλεται στις αναγωγές Cook που χρησιμοποιούνται για αυτά τα αποτελέσματα, διότι η TotP και η #P είναι ισοδύναμες κάτω από Cook αναγωγές [49, 47].

Από την άλλη πλευρά, η κατάσταση είναι διαφορετική όταν εξετάζεται η πληρότητα υπό αναγωγές Karp (parsimonious). Συγκεκριμένα, δεν υπάρχει #P-πλήρες πρόβλημα υπό Karp αναγωγές στην TotP, εκτός αν $P = NP$. Για παράδειγμα, το PERMANENT δεν μπορεί να είναι #P-πλήρες υπό Karp αναγωγές εκτός αν $P = NP$. Επιπλέον, φαίνεται επίσης απίθανο ότι το PERMANENT είναι TotP-πλήρες υπό Karp αναγωγές, διότι τότε θα ίσχυε $NP=RP$. Αυτό συμβαίνει επειδή τέτοιες αναγωγές διατηρούν την προσέγγιση και το PERMANENT επιδέχεται FPRAS, ενώ άλλα προβλήματα που βρίσκονται στην TotP, όπως το #IS είναι AP-αλληλοαναγόμενα με το #SAT [27] (δηλαδή το ένα ανάγεται στο άλλο και αντιστρόφως), οπότε αν το PERMANENT ήταν TotP-πλήρες υπό Karp αναγωγές, το #SAT θα επιδεχόταν FPRAS, πράγμα που είναι αδύνατο, εκτός αν $NP=RP$. Από αυτή την άποψη αποτελέσματα για TotP-πληρότητα θα μπορούσαν να ρίξουν φως στην προσεγγισιμότητα πολλών προβλημάτων μέτρησης.

Σε αυτή την εργασία, παρουσιάζουμε ένα πρώτο TotP-πλήρες πρόβλημα κάτω από φειδωλές αναγωγές, το #MONOTONE CIRCUIT SAT: δεδομένης της κωδικοποίησης ενός μονότονου κυκλώματος σε σχέση με μια συγκεκριμένη μερική διάταξη (που θα οριστεί αργότερα), ζητείται να υπολογιστεί ο αριθμός των εισόδων τις οποίες το κύκλωμα αποδέχεται. Στη συνέχεια, ανάγουμε το παραπάνω πρόβλημα σε άλλα, αποδεικνύοντας ότι κι αυτά είναι επίσης TotP-πλήρη κάτω από φειδωλές αναγωγές. Τέλος, συζητούμε κάποιες επιπτώσεις των αποτελεσμάτων μας στην θεωρία μετρητικής πολυπλοκότητας γενικότερα.

2.1.1 Σχετικές εργασίες

Τα τελευταία χρόνια, υπήρξε μεγάλο ενδιαφέρον για την ταξινόμηση της πολυπλοκότητας προσέγγισης σε προβλήματα καταμέτρησης. Το ενδιαφέρον αυτό απορρέει από το γεγονός ότι πολύ λίγα μετρητικά προβλήματα έχουν αποδειχθεί να είναι στην FP. Την ίδια στιγμή τα προβλήματα καταμέτρησης στην #P με NP-πλήρη απόφαση ύπαρξης λύσης δεν μπορεί να έχουν πολυωνυμικού χρόνου προσέγγιση, εκτός εάν $P = NP$. Επιπλέον, στο [27] αποδείχθηκε ότι αυτά τα προβλήματα είναι πλήρη για την #P υπό αναγωγές που διατηρούν την προσέγγιση. Επομένως, δεν υπάρχει FPRAS για κανένα από αυτά, εκτός εάν $NP = RP$. Υποθέτοντας ότι $NP \neq RP$, υπάρχουν άπειρα επίπεδα πολυπλοκότητας μεταξύ της αποδοτικής προσέγγισης και της δυσκολίας του #SAT [17]. Εντούτοις, μας ενδιαφέρει κυρίως η αποτελεσματική προσέγγιση των προβλημάτων καταμέτρησης. Έτσι επικεντρωνόμαστε καταρχάς στην καταμέτρηση των προβλημάτων με εύκολη απόφαση ύπαρξης λύσης. Με τον όρο αποτελεσματικός αλγόριθμος προσέγγισης εννοούμε FPRAS ή FPTAS. Τέτοιοι αλγόριθμοι για κάποια προβλήματα καταμέτρησης μπορούν να βρεθούν στα [36, 24, 46, 43]. Ειδικά, η σταθερή πρόοδος στον προσδιορισμό της πολυπλοκότητας μέτρησης ομομορφισμών γραφημάτων συνέβαλαν στη μελέτη της πολυπλοκότητας προσεγγιστικής μέτρησης. Επίσης, η σύν-

δεση των προβλημάτων καταμέτρησης με τη στατιστική φυσική έχει οδηγήσει σε σημαντικά αποτελέσματα σε αυτόν τον τομέα [30, 33, 1, 2, 4].

Όσον αφορά υποκλάσεις της #P, μετρητικές κλάσεις όπως η #L, SpanL [6], #PE [61] TotP [47], #RΣ₂ [66], #RHΠ₁ [27] έχουν οριστεί. Μια σημαντική ανοικτή ερώτηση αφορά τη σχέση μεταξύ καθεμιάς από αυτές τις κλάσεις και τα προβλήματα που επιδέχονται FPRAS. Μας ενδιαφέρει ιδιαίτερα η κλάση TotP. Άλλες παρόμοιες κατηγορίες που μετράνε την τάξη του δεξιότερου, αριστερότερου, και μεσαίου μονοπατιού αποδοχής ενός δέντρου υπολογισμού μιας NPTM εισήχθησαν και μελετήθηκαν στο [47]. Η TotP ισούται με την IF_t^{LN} , την κλάση των συναρτήσεων μέτρησης μεγέθους διαστήματος σε ολικώς διατεταγμένα σύνολα συμβολοσειρών, με εύκολα υπολογίσιμη τη λεξικογραφικά πλησιέστερη λέξη σε δεδομένη συμβολοσειρά [13]. Το τελευταίο βασίζεται στο [39], όπου οι Hemaspaandra et al. όρισαν τις κλάσεις των συναρτήσεων μέτρησης μεγέθους διαστημάτων μερικώς ή ολικώς διατεταγμένων συνόλων, και χαρακτήρισαν τη #P σε όρους τέτοιων συναρτήσεων.

Μια υποκλάση της #P που περιέχει δύσκολες μετρητικές συναρτήσεις με εύκολη απόφαση ύπαρξης λύσης, είναι η κλάση λογαριθμικού χώρου SpanL [6]. Είναι ενδιαφέρον ότι η TotP βρίσκεται μεταξύ της SpanL και της #P (οι εγκλεισμοί είναι αυστηροί κάτω από λογικές υποθέσεις [62]). Έτσι, έχουμε την ακόλουθη αλυσίδα για τις υποκλάσεις της #P:

$$FP \subseteq \text{SpanL} \subseteq \text{TotP} \subseteq \#PE \subseteq \#P.$$

Ενώ SpanL-πλήρη προβλήματα κάτω από φειδωλές αναγωγές είναι γνωστά, πχ. η συνάρτηση ranking για NFA [6], κανένα πρόβλημα πλήρες υπό φειδωλές αναγωγές δεν ήταν γνωστό για την TotP μέχρι τώρα. Σε αυτή την εργασία αντιμετωπίζουμε αυτή την κατάσταση παρέχοντας μερικά πρώτα TotP-πλήρη προβλήματα κάτω από φειδωλές αναγωγές. Ελπίζουμε ότι αυτή η συνεισφορά θα βοηθήσει μεταξύ άλλων και στην καλύτερη κατανόηση των ιδιοτήτων της TotP, και των σχέσεών της με τις προαναφερθείσες κλάσεις, όπως και με άλλες ενδιαφέρουσες υποκλάσεις της #P.

2.1.2 Συνεισφορά και βασικές ιδέες

Σε αυτή την εργασία, παρουσιάζουμε κατ' αρχάς ένα πρώτο TotP-πλήρες πρόβλημα υπό φειδωλές αναγωγές, το #MONOTONE CIRCUIT SAT: δεδομένης της κωδικοποίησης ενός μονότονου κυκλώματος ως προς μια συγκεκριμένη μερική διάταξη, ζητείται να υπολογιστεί ο αριθμός των εισόδων τις οποίες το κύκλωμα αποδέχεται. Στη συνέχεια, ανάγουμε αυτό σε άλλα προβλήματα, αποδεικνύοντας ότι είναι επίσης TotP-πλήρη κάτω από φειδωλές αναγωγές.

Για να κατασκευάσουμε το πρώτο TotP-πλήρες πρόβλημα, αντιστοιχούμε την είσοδο x μιας συνάρτησης f της TotP σε ένα κύκλωμα C έτσι ώστε ο αριθμός των εισόδων που αποδέχεται το C ισούται με $f(x) + 1$. Η γνωστή αναγωγή που χρησιμοποιείται για να αποδείξει κανείς ότι κάθε πρόβλημα στην NP ανάγεται στο

CIRCUIT-SAT (βλ. π.χ. [9]), δεν είναι κατάλληλη για εμάς, αφού το πρόβλημα καταμέτρησης για το προκύπτον κύκλωμα δεν είναι στην TotP. Διότι παρόλο που είναι αυτοαναγώγιμο, η απόφαση ύπαρξης λύσης είναι NP-πλήρης.

Οι βασικές παρατηρήσεις για την κατασκευή μας είναι οι εξής: (1) Για μια συνάρτηση f στην TotP, η f μετράει τις διακλαδώσεις του δυαδικού δέντρου υπολογισμού μιας NPTM, οι οποίες είναι ίσες με τον αριθμό των φύλλων μείον ένα. Αυτό μπορεί να γίνει επειδή η μη ντετερμινιστική μηχανή Turing που θεωρούμε, έχει δύο μη ντετερμινιστικές επιλογές σε κάθε βήμα. (2) Αν θεωρήσουμε αυτό το δέντρο υπολογισμού $T_{M(x)}$ ως υποδέντρο ενός τέλει δυαδικού δέντρου $S_{M(x)}$, τότε στο τέλει δυαδικό δέντρο μπορεί να θεωρηθεί ότι παρουσιάζει κάποιο είδος μονοτονίας: οι απόγονοι των τερματικών κόμβων χαρακτηρίζονται επίσης ως “τερματικοί”. Έτσι, η ιδέα είναι να κατασκευάσουμε ένα κύκλωμα C , για το οποίο κάθε είσοδος να αντιστοιχεί σε έναν κόμβο του τέλει δυαδικού δέντρου $S_{M(x)}$, και η έξοδος να είναι ‘1’ αν ο αντίστοιχος κόμβος δεν φέρει την ένδειξη ‘τερματικός’. Το πρόβλημα της μέτρησης των αποδεκτών εισόδων από το C (δηλαδή των εισόδων με έξοδο “1”) έχει εύκολη απόφαση ύπαρξης λύσης, αφού αρκεί να ελέγξει κανείς την τιμή που επιστρέφει το κύκλωμα στην είσοδο που αντιστοιχεί στη ρίζα.

Μια άλλη δυσκολία προκύπτει τώρα, όσον αφορά στην αυτοαναγωγιμότητα: το προκύπτον κύκλωμα είναι μονότονο σε σχέση με τη μονοτονία που ορίζεται από το τέλει δυαδικό δέντρο. Αλλά για να είναι το πρόβλημα της καταμέτρησης αυτοαναγώγιμο, οι υποπεριπτώσεις στις οποίες ανάγεται, πρέπει επίσης να ικανοποιούν την ίδια ιδιότητα μονοτονίας. Για να επιτευχθεί αυτό, πρέπει να επιλεγεί μια κατάλληλη κωδικοποίηση για τους κόμβους του τέλει δυαδικού δέντρου. Συζητάμε τις επιθυμητές ιδιότητες μιας τέτοιας κωδικοποίησης στην ενότητα 3.2.5. Αν και για τις αποδείξεις μας έχουμε χρησιμοποιήσει μια συγκεκριμένη κωδικοποίηση που είναι απλή και φυσιολογική, κάθε κωδικοποίηση με αυτές τις ιδιότητες θα ήταν επίσης κατάλληλη, και τότε θα προέκυπτε ένα κύκλωμα που είναι μονότονο σε σχέση με μια διαφορετική μερική διάταξη, που σχετίζεται με την εκάστοτε κωδικοποίηση. Το αντίστοιχο πρόβλημα της μέτρησης των λύσεων ενός τέτοιου κυκλώματος, θα ήταν επίσης TotP-πλήρες.

2.1.3 Συνέπειες

Αποδεικνύεται ότι το πρόβλημα SIZE-OF-SUBTREE (βλ. Ορισμός 27) είναι επίσης TotP-πλήρες.

Αυτό το πρόβλημα είναι επίσης γνωστό και ως το backtracking tree estimation πρόβλημα, δηλαδή το πρόβλημα του υπολογισμού του μεγέθους ενός backtracking δέντρου, χωρίς να το διατρέξει κανείς εξαντλητικά, το οποίο έχει αρχικά μελετηθεί από τον Knuth [51]. Υπάρχει μια πληθώρα εργασιών πάνω σε αυτό το πρόβλημα που το ξεετάζουν από διάφορες οπτικές γωνίες, και προτείνουν αλγόριθμους που επιτυγχάνουν σε πολλές ειδικές περιπτώσεις, και περιπτώσεις που προκύπτουν στην πράξη, βλ. [51, 65, 21, 50, 15, 7].

Παρ’ όλα αυτά η πολυπλοκότητα χειρότερης περίπτωσης για αυτό το πρόβλημα

ήταν μέχρι τώρα άγνωστη (αν εξαιρέσουμε το [71] όπου η πολυπλοκότητά του μελετάται για ένα μοντέλο υπολογισμού που όμως δεν είναι ισοδύναμο με μηχανή Turing.) Εφόσον αποδεικνύουμε ότι το SIZE-OF-SUBTREE είναι TotP-πλήρες υπό φειδωλές αναγωγές, και εφόσον ως γνωστό, το PERMANENT είναι #P-πλήρες υπό αναγωγές Cook, το #IS είναι #P-πλήρες υπό αναγωγές που διατηρούν την προσέγγιση και τα δύο αυτά προβλήματα ανήκουν την TotP, προκύπτουν τα ακόλουθα πορίσματα.

- **Πόρισμα:** Το SIZE-OF-SUBTREE είναι #P-πλήρες υπό
 - αναγωγές Cook (μέσω του PERMANENT)
 - Approximation preserving (ή αλλιώς AP) αναγωγές (μέσω του #IS)
- **Πόρισμα:** Το SIZE-OF-SUBTREE δεν υπολογίζεται ακριβώς σε πολυωνυμικό χρόνο εκτός αν $PH=P$, και δεν προσεγγίζεται σε πολυωνυμικό χρόνο εκτός αν $NP=RP$.

Από την άλλη πλευρά είναι γνωστό ότι το SIZE-OF-SUBTREE είναι εύκολο να προσεγγιστεί στη μέση περίπτωση, κάτω από συγκεκριμένες κατανομές πιθανότητας πάνω στα στιγμιότυπα [29, 75], πράγμα που μας οδηγεί στο ακόλουθο συμπέρασμα.

Συμπέρασμα: Το #SAT που θεωρείται δύσκολο στη μέση περίπτωση να προσεγγιστεί, ανάγεται με αναγωγές που διατηρούν την προσέγγιση σε ένα πρόβλημα που είναι εύκολα προσεγγίσιμο στη μέση περίπτωση. Αυτό σημαίνει ότι οι αναγωγές που διατηρούν την προσέγγιση δεν διατηρούν απαραίτητα και τη μάζα πιθανότητας πάνω στα στιγμιότυπα. Με άλλα λόγια, τα πολλά δύσκολα στιγμιότυπα του πρώτου προβλήματος μπορεί να αντιστοιχούν μέσω της αναγωγής στα λίγα δύσκολα στιγμιότυπα του δεύτερου προβλήματος.

Τέλος, ένας πολύ απλός πιθανοτικός αλγόριθμος δόθηκε από τον Knuth, η μέση τιμή του οποίου είναι ακριβώς το μέγεθος του δέντρου. Από την άλλη πλευρά, η διασπορά της εξόδου αυτού του αλγορίθμου είναι εκθετική στη χειρότερη περίπτωση.

Το αποτέλεσμά μας συνεπάγεται ότι αυτός ο απλός αλγόριθμος είναι ουσιαστικά το καλύτερο που μπορούμε να ελπίζουμε, εκτός αν $NP = RP$, επειδή το #IS ανήκει στην TotP, και είναι γνωστό ότι δεν προσεγγίζεται εκτός αν $NP = RP$ [27].

Μια άλλη ενδιαφέρουσα συνέπεια των αποτελεσμάτων μας προέρχεται από την TotP-πληρότητα του προβλήματος #CLUSTERED-MONOTONE-SAT (Definition 30), δηλαδή του προβλήματος της καταμέτρησης του αριθμού ικανοποιητικών αναθέσεων σε λογικές φόρμουλες με τις εξής ιδιότητες: (α) μια λύση μπορεί εύκολα να βρεθεί εάν υπάρχει, και (β) το σύνολο των λύσεων κάθε τέτοιας φόρμουλας συνδέεται με συγκεκριμένο τρόπο όπως περιγράφεται παρακάτω στο θεώρημα 12. Συνδυάζοντας την πληρότά του προβλήματος αυτού με το γεγονός ότι το #SAT μπορεί να αναχθεί στο #IS, με αναγωγή που διατηρεί την προσέγγιση [27], παίρνουμε ότι η προσέγγιση του πλήθους ικανοποιητικών αναθέσεων μιας αυθαίρετης

φόρμουλας είναι τόσο δύσκολη όσο η προσέγγιση του πλήθους ικανοποιητικών αναθέσεων μιας φόρμουλας με τις παραπάνω ιδιότητες.

Αυτό είναι ενδιαφέρον, καθώς υπάρχει μια σειρά εργασιών που συσχετίζουν την θεωρία πολυπλοκότητας με φαινόμενα αλλαγής φάσης [1, 2, 4], από τις οποίες γνωρίζουμε ότι, για τα “δύσκολα” στιγμιότυπα του SAT, το σύνολο ικανοποιητικών αναθέσεων είναι ευρέως διεσπαρμένο στο χώρο όλων των αναθέσεων (δλδ στον boolean υπερκύβο n διαστάσεων), και αυτή η σκέδαση μπορεί να είναι υπεύθυνη για την υπολογιστική δυσκολία του SAT. Μάλιστα αυτή η σκέδαση αποδεδειγμένα δικαιολογεί την αποτυχία γνωστών αλγορίθμων που βασίζονται σε Μαρκοβιανές αλυσίδες [5]. Τα αποτελέσματά μας δείχνουν ότι μπορούμε να ανάγουμε μια αυθαίρετη φόρμουλα με ένα διεσπαρμένο σύνολο λύσεων, σε μια άλλη φόρμουλα με ένα σύνολο λύσεων που συνδέονται με ένα τρόπο που περιγράφουμε ρητά.

Συμπέρασμα: Αυτό μπορεί να εκληφθεί με δύο τρόπους: Για έναν αισιόδοξο δείχνει ότι η προσέγγιση του #SAT μπορεί να μην είναι τόσο δύσκολη τελικά (π.χ. ίσως $NP = RP$). Από την άλλη πλευρά, ένας απαισιόδοξος μπορεί να καταλήξει στο συμπέρασμα ότι το #SAT δεν είναι μόνο δύσκολο γενικά, αλλά ακόμη και για φαινομενικά πιο εύκολα (δλδ πολύ πιο δομημένα και με περισσότερη πληροφορία) στιγμιότυπα, θα είχε την ίδια δυσκολία.

Επιπλέον σημαίνει ότι η γνώση που είχαμε μέχρι τώρα δεν επαρκεί για να δικαιολογήσει την αποτυχία αλγορίθμων που βασίζονται σε μαρκοβιανές αλυσίδες για το #SAT. Καταφέραμε να ανάγουμε το #SAT σε ένα πρόβλημα του οποίου ο χώρος λύσεων δεν είναι διασκορπισμένος όπως συμβαίνει για μια τυπική δύσκολη φόρμουλα του #SAT. Έτσι νέες εργοδικές μαρκοβιανές αλυσίδες μπορούν να οριστούν με φυσιολογικό τρόπο και να μελετηθούν. Νέοι αλγόριθμοι πρέπει να αναλυθούν, και νέες ερμηνείες χρειάζονται που να δικαιολογούν την δυσκολία αυτού του προβλήματος.

2.2 Προκαταρκτικά

Παραπέμπουμε στο κεφάλαιο 1 για τους ορισμούς των κλάσεων και των τύπων αναγωγών.

Το μοντέλο υπολογισμού είναι η μη ντετερμινιστική μηχανή Turing πολυωνυμικού χρόνου. Υπάρχει δηλαδή ένα πολυώνυμο p τέτοιο ώστε για κάθε x από ένα αλφάβητο Σ^* , όλα τα υπολογιστικά μονοπάτια έχουν μήκος το πολύ $p(|x|)$, όπου $|x|$ είναι το μήκος της εισόδου.

Θα χρησιμοποιούμε τους όρους, Cook και Karp, σαν συντομεύσεις για “poly-time Turing” και “poly-time many-one” αντίστοιχα.

Παρόλο που η TotP, η #PE και η #P είναι ισοδύναμες κατά Cook, δεν είναι ισοδύναμες κατά Karp εκτός αν $P = NP$. Αυτό σημαίνει ότι:

- Υπό τις Karp αναγωγές, τα #P-πλήρη, τα #PE-πλήρη και τα TotP-πλήρη προβλήματα αποτελούν ξένες κλάσεις, εκτός αν $P = NP$.
- Υπό τις Cook αναγωγές τα TotP-πλήρη προβλήματα περιέχονται στα #PE-πλήρη

προβλήματα, που περιέχονται στα #P-πλήρη προβλήματα.

Προκειμένου να κατατάξουμε πλήρως ένα πρόβλημα, χρειάζεται να αποδείξουμε ότι είναι πλήρες για μια κλάση υπό Karp αναγωγές. Το γεγονός ότι ένα πρόβλημα είναι #P-πλήρες υπό Cook αναγωγές, δεν δίνει αρκετή πληροφορία για την πολυπλοκότητά του, αφού θα μπορούσε να ανήκει στην TotP.

Οι Cook αναγωγές θολώνουν τις δομικές διαφορές μεταξύ των μετρητικών κλάσεων [49], οπότε προκειμένου να κατανοήσουμε αυτές τις διαφορές θα θέλαμε να έχουμε πλήρη προβλήματα για αυτές τις κλάσεις κάτω από Karp (parsimonious) αναγωγές. Το #SAT είναι #P-πλήρες υπό Karp αναγωγές. Για την TotP, το μόνο πλήρες πρόβλημα υπό Karp αναγωγές που είναι μέχρι τώρα γνωστό είναι το generic πρόβλημα της κλάσης, δηλ το πρόβλημα όπου δεδομένης μιας NPTM M και μιας εισόδου x , το ζητούμενο είναι να μετρηθούν όλα τα υπολογιστικά μονοπάτια της μηχανής μείον ένα. Πιο συγκεκριμένα:

Ορισμός 17. (To generic TotP-πλήρες πρόβλημα) f_{gen} .

Είσοδος: $(M, x, 1^t)$, όπου M είναι μια (δυναδική) TM, $x \in \{0, 1\}^*$, και $t \in \mathbb{N}$.

Εξοδος: $f_{gen}(M, x, 1^t) :=$ (το συνολικό πλήθος υπολογιστικών μονοπατιών της M σε είσοδο x , με μήκος το πολύ t) - 1.

Στο υπόλοιπο αυτής της ενότητας, παρουσιάζουμε ορισμούς και παρατηρήσεις χρήσιμες για την βασική απόδειξη αυτού του κεφαλαίου.

Ένα δέντρο λέγεται (a) binary (δυναδικό) αν κάθε κόμβος έχει το πολύ δύο παιδιά, (b) full binary (πλήρως δυναδικό) αν κάθε κόμβος έχει είτε κανένα είτε δύο ακριβώς παιδιά, (c) perfect binary (τέλειο δυναδικό) αν είναι δυναδικό, όλοι οι εσωτερικοί κόμβοι έχουν δύο παιδιά, και όλα τα φύλλα βρίσκονται στο ίδιο επίπεδο.

Έστω M μια NPTM. Μπορούμε να υποθέσουμε ότι η M έχει σε κάθε βήμα (το πολύ) δύο μη ντετερμινιστικές επιλογές. Αυτό συμβαίνει επειδή αν υπάρχουν επιλογές $m > 2$ για κάποιο συνδυασμό κατάστασης-συμβόλου, αλλάζουμε τη M προσθέτοντας $m - 2$ νέες καταστάσεις, έτσι ώστε να επιτυγχάνεται το ίδιο αποτέλεσμα από τη λειτουργία της μηχανής. Επιπλέον, ο συνολικός αριθμός υπολογιστικών μονοπατιών στην τροποποιημένη μηχανή Turing είναι ο ίδιος με την αρχική μηχανή M . Επομένως, ο υπολογισμός της M στην είσοδο x μπορεί να θεωρηθεί ως δυναδικό δέντρο $T_{M(x)}$, όπου δημιουργείται μία διακλάδωση στο υπολογιστικό δέντρο κάθε φορά που η M πρέπει να επιλέξει μεταξύ δύο επιλογών. Εάν υπάρχει μόνο μία επιλογή για κάποιον συνδυασμό κατάστασης-συμβόλου, θεωρούμε ότι το δέντρο δεν έχει διακλάδωση σε αυτό το σημείο. Καταλήγουμε στο συμπέρασμα ότι μπορούμε να περιορίσουμε τη μελέτη μας σε πλήρη δένδρα υπολογισμών. Έτσι, δεν είναι δύσκολο να δούμε ότι

$$tot_M(x) = \#(\text{all paths of } M \text{ on input } x) - 1 = \#(\text{branchings of } T_{M(x)}).$$

Σημειώστε ότι όταν εξετάζουμε μια συνάρτηση στην TotP, για την αντίστοιχη NPTM M δεν μπορούμε να μετατρέψουμε το δέντρο υπολογισμού $T_{M(x)}$ σε ένα τέλειο δυναδικό δέντρο χωρίς να αλλάξουμε τον αριθμό των μονοπατιών της M (για αυτό και δεν το κάνουμε).

Επιπλέον οι μη ντετερμινιστικές επιλογές του υπολογισμού της M μπορούν να αναπαρασταθούν σαν μια δυαδική συμβολοσειρά y , όπου κάθε αριστερό κλαδί αντιστοιχεί στο 0 και κάθε δεξιό στο 1. Όταν γράφουμε $M(x, y)$ αναφερόμαστε στην έξοδο της μηχανής Turing M με είσοδο x και με μη ντετερμινιστικές επιλογές y . Πιο συγκεκριμένα, $M(x, y) = 1$ αν η M αποδέχεται το x με μη ντετερμινιστικές επιλογές y , και $M(x, y) = 0$ αλλιώς.

Στις ερχόμενες παραγράφους θα χρησιμοποιήσουμε δύο αντιστοιχίες από φυσικούς αριθμούς σε δυαδικές συμβολοσειρές, όπως επίσης και μια συγκεκριμένη μερική διάταξη πάνω στους φυσικούς αριθμούς.

Ορισμός 18. *Ορίζουμε την tree partial order, συμβολιζόμενη ως \leq_{tree} , πάνω στο \mathbb{N} ως εξής. Είναι ανακλαστική και μεταβατική και, αν $y = 2x + 1$ ή $y = 2x + 2$ τότε $x \leq_{tree} y$.*

Σημειώστε ότι η γραφική παράσταση αυτής της μερικής διάταξης είναι ένα άπειρο τέλει δυαδικό δέντρο που συμβολίζεται με $T_{\mathbb{N}}$, οι κόμβοι του οποίου φέρουν ως ετικέτες τους φυσικούς αριθμούς, με τρόπο που η αριστερά προς τα δεξιά διάσχιση αυτού του δέντρου (η γνωστή BFS) να δίνει τη φυσική διάταξη του \mathbb{N} (υποθέτοντας ότι το αριστερό παιδί του x είναι $2x + 1$ και το δεξί είναι $2x + 2$). Η ρίζα του $T_{\mathbb{N}}$ έχει ως ετικέτα το 0, και ισχύει $x \leq_{tree} y$ αν και μόνο αν το y είναι κάποιος απόγονος του x σε αυτό το δέντρο. Έστω ότι το $d_{T_{\mathbb{N}}}(u, v)$ συμβολίζει το μήκος της διαδρομής που συνδέει τα u και v στο $T_{\mathbb{N}}$. Διατηρούμε στο μυαλό μας την $T_{\mathbb{N}}$ για να ορίσουμε κάποιες χρήσιμες αντιστοιχίες.

Ορισμός 19. *Οι παρακάτω συναρτήσεις ορίζονται:*

1. $path : \mathbb{N} \rightarrow \{0, 1\}^*$. Αντιστοιχεί το n στη δυαδική συμβολοσειρά που περιγράφει το μονοπάτι που ξεκινάει από τη ρίζα του $T_{\mathbb{N}}$ και τελειώνει στον κόμβο με ετικέτα n . Για παράδειγμα, $path(3) = 00$, $path(9) = 010$, $path(0) = \varepsilon$, όπου ε είναι η κενή συμβολοσειρά.
2. $num : \{0, 1\}^* \rightarrow \mathbb{N}$. Ορίζεται ως η αντίστροφη συνάρτηση της $path$.
3. $bin_k : \{0, 1, \dots, 2^k - 1\} \rightarrow \{0, 1\}^k$. Αντιστοιχίζει ένα κόμβο $n \in \{0, 1, \dots, 2^k - 1\}$ του $T_{\mathbb{N}}$ στη δυαδική του αναπαράσταση στην οποία έχουμε προσθέσει στην αρχή όσα μηδενικά χρειάζεται ώστε να έχει μήκος k . Για παράδειγμα, $bin_6(3) = 000011$, $bin_4(9) = 1001$, και $bin_3(9)$ δεν ορίζεται.

Επιπλέον, η bin_k^{-1} είναι η αντίστροφη της bin_k . Για απλότητα θα παραβιάζουμε το συμβολισμό και θα χρησιμοποιούμε bin και bin^{-1} όταν το μήκος της δυαδικής αναπαράστασης θα είναι ξεκάθαρο από τα συμφραζόμενα. Οι συναρτήσεις $path$, num , bin_k και bin_k^{-1} είναι υπολογίσιμες σε πολυωνυμικό χρόνο. Αυτό φαίνεται ξεκάθαρα από τους παρακάτω ισοδύναμους ορισμούς τους.

Ορισμός 20. (a) *Ορίζουμε τη συνάρτηση $num : \{0, 1\}^* \rightarrow \mathbb{N}$: Έστω για μια δυαδική συμβολοσειρά s , το $number(s)$ να είναι η τιμή του s στο \mathbb{N} .*

$$num(s) = number(1||s) - 1,$$

όπου ‘ \parallel ’ συμβολίζει την παράθεση συμβολοσειρών.

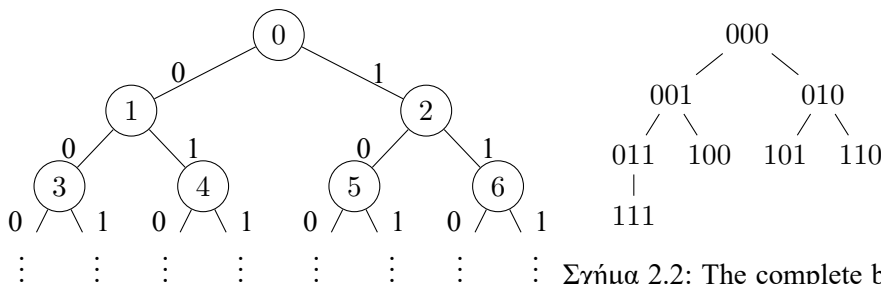
(b) Ορίζουμε τη συνάρτηση $\text{path} : \mathbb{N} \rightarrow \{0, 1\}^*$ αναδρομικά:

- $\text{path}(0) = \varepsilon$
- $\text{path}(k) = \text{path}(\lceil \frac{k}{2} \rceil - 1) \parallel \overline{\text{parity}(k)}$

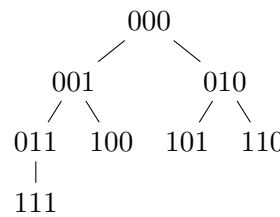
όπου $\overline{\text{parity}(k)} = \begin{cases} 1 & , \text{if } k \text{ even} \\ 0 & , \text{if } k \text{ odd} \end{cases}$, και ‘ \parallel ’ συμβολίζει την παράθεση συμβολοσειρών.

Για ένα κόμβο u της $T_{\mathbb{N}}$, $\text{path}(u)$ είναι η παράθεση των ταμπελών των ακμών που ενώνουν το 0 με το u (βλ. σχήμαΣ 2.1). Παρατηρήστε ότι αν θεωρήσουμε τη φυσική διάταξη του \mathbb{N} , η path δημιουργεί την λεξικογραφική διάταξη των δυαδικών συμβολοσειρών: $\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots$

Ορισμός 21. Αν περιορίσουμε την \leq_{tree} στο $\{0, 1, \dots, 2^k - 1\}$ και εφαρμόσουμε την bin_k , παίρνουμε μια μερική διάταξη στο $\{0, 1\}^k$, την οποία, παραβιάζοντας το συμβολισμό, θα συμβολίζουμε επίσης με \leq_{tree} . Το T_k συμβολίζει το δυαδικό δέντρο που αναπαριστά την \leq_{tree} στο $\{0, 1\}^k$.



Σχήμα 2.1: The infinite perfect binary tree $T_{\mathbb{N}}$.



Σχήμα 2.2: The complete binary tree T_3 .

2.3 Το #MONOTONE CIRCUIT SAT είναι TotP-πλήρες υπό Karp αναγωγές

Σε αυτή την ενότητα ορίζουμε ένα νέο μετρητικό πρόβλημα και αποδεικνύουμε ότι είναι TotP-πλήρες.

Έστω C_n ένα Boolean κύκλωμα (βλ. [9]) με n πύλες εισόδου, και έστω $C_n(z)$ η έξοδος του C_n με είσοδο $z \in \{0, 1\}^n$.

Ορισμός 22. Καλούμε ένα Boolean κύκλωμα C_n μη-αύξον ως προς την \leq_{tree} αν για κάθε $x, y \in \{0, 1\}^n$, $x \leq_{\text{tree}} y$ συνεπάγεται ότι $C_n(x) \geq C_n(y)$.

Ορισμός 23. #MONOTONE CIRCUIT SAT, που θα το συμβολίζουμε και ως $f_{\#MC}$ Είσοδος: Ένα Boolean κύκλωμα C_n μη-αύξον ως προς την \leq_{tree} .

Έξοδος: $f_{\#MC}(C_n) := |\{y \in \{0, 1\}^n : C_n(y) = 1\}|$, δηλ. το πλήθος των ικανοποιητικών αναθέσεων για το C_n .

2.3.1 Το #MONOTONE CIRCUIT SAT είναι TotP-hard

Αποδεικνύουμε ότι η συνάρτηση $f_{\#MC}$ είναι TotP-hard ανάγοντας τον υπολογισμό κάθε συνάρτησης $h \in \text{TotP}$ στην $f_{\#MC}$.

Η βασική παρατήρηση είναι η εξής. Υπάρχει μια NPTM M τέτοια ώστε για κάθε είσοδο x ισχύει $h(x) = \text{tot}_M(x)$. Έστω $T_{M(x)}$ το αντίστοιχο υπολογιστικό δέντρο. Θεωρήστε ότι επεκτείνουμε το $T_{M(x)}$ σε ένα τέλειο δυαδικό δέντρο $S_{M(x)}$ με ίδιο ύψος, έτσι ώστε όλα τα φύλλα του αρχικού δέντρου $T_{M(x)}$ και όλοι οι απόγονοί τους να έχουν την ταμπέλα "τερματικοί". Έτσι $h(x) = \#(\text{branching nodes of } T_{M(x)}) = \#(\text{μη "τερματικοί" κόμβοι του } S_{M(x)})$.

Κατασκευάζουμε ένα κύκλωμα C μη αυξον ως προς την \leq_{tree} , τέτοιο ώστε το πλήθος των αποδεκτών εισόδων του C ισούται με $h(x)$. Η ιδέα είναι να περιγράψουμε μια ένα προς ένα και επί αντιστοιχία μεταξύ των εισόδων του C και των μονοπατιών από τη ρίζα στους κόμβους του $S_{M(x)}$, εσωτερικούς και φύλλα. Το C αποδέχεται μια είσοδο αν και μόνο αν το αντίστοιχο μονοπάτι φτάνει σε μη "τερματικό" κόμβο του $S_{M(x)}$, το οποίο με τη σειρά του αντιστοιχεί σε σημείο διακλάδωσης του $T_{M(x)}$.

Θεώρημα 10. *Av $h \in \text{TotP}$ τότε $h \leq_m^p f_{\#MC}$.*

Απόδειξη. Έστω $h \in \text{TotP}$, και M η αντίστοιχη δυαδική NPTM. Υπενθυμίζουμε ότι για κάθε είσοδο x , $h(x) = \text{tot}_M(x) = \#(\text{branchings of } T_{M(x)})$, όπου $T_{M(x)}$ είναι το υπολογιστικό δέντρο της $M(x)$. Έστω p ένα πολυώνυμο που φράσσει το χρόνο εκτέλεσης της M , οπότε το ύψος του $T_{M(x)}$ είναι το πολύ $p(|x|)$. Δεδομένης μιας περιγραφής της M μπορούμε να κατασκευάσουμε μια M' τέτοια ώστε για κάθε είσοδο x της M :

1. Το $T_{M'(x)}$ είναι ένα τέλειο δυαδικό δέντρο ύψους $p(|x|) + 1$.
2. $\#(\text{accepting paths of } M'(x)) = \#(\text{branchings of } T_{M(x)})$.
3. Για $y_1, y_2 \in \{0, 1\}^{p(|x|)+1}$, αν $y_1 \leq_{tree} y_2$, τότε $M'(x, y_1) \geq M'(x, y_2)$.

Προκειμένου να περιγράψουμε την M' χρησιμοποιούμε τις συναρτήσεις path και bin από τον Ορισμό 19. Η λειτουργία της M' με είσοδο x εξελίσσεται ως εξής:

1. Διάλεξε μια δυαδική συμβολοσειρά y μήκους $p(|x|)+1$. Έστω $n_y = \text{bin}^{-1}(y)$.
2. Υπολόγισε $z = \text{path}(n_y)$.
3. Προσομοίωσε την M με είσοδο x και μη ντετερμινιστικές επιλογές z .
 - Αν η προσομοίωση φτάσει σε τερματική κατάσταση της M (πιθανώς χρησιμοποιώντας μόνο ένα prefix του z), τότε επέστρεψε 0.
 - Αν η προσομοίωση χρησιμοποιήσει όλα τα bits του z χωρίς να φτάσει σε τερματική κατάσταση της M , τότε επέστρεψε 1.

Τώρα θα δείξουμε ότι ισχύουν οι ιδιότητες (i), (ii), (iii):

1. Το υπολογιστικό δέντρο της M' είναι ένα τέλειο δυαδικό δέντρο ύψους $p(|x|)+1$, μιας και οι μόνες μη ντετερμινιστικές επιλογές γίνονται στο βήμα \square (Το βήμα \square είναι ντετερμινιστικό).
2. Το πλήθος των μονοπατιών αποδοχής της M' ισούται με το πλήθος των σημείων διακλάσωσης της M , αφού η M' επιστρέφει 1 αν και μόνο αν το z αντιστοιχεί σε ένα υπολογιστικό μονοπάτι της M που σταματάει σε σημείο διακλάδωσης: θυμηθείτε ότι η bin και η path είναι ένα προς ένα και επί.
3. Για να αποδείξουμε την τρίτη ιδιότητα, αρκεί να δείξουμε ότι για όλα τα y_1, y_2 για τα οποία $y_1 \leq_{tree} y_2$ έχουμε $M'(x, y_1) = 0 \Rightarrow M'(x, y_2) = 0$. Αν $y_1 \leq_{tree} y_2$, τότε $z_1 = \text{path}(\text{bin}^{-1}(y_1))$ είναι ένα prefix του $z_2 = \text{path}(\text{bin}^{-1}(y_2))$. Αυτό σημαίνει ότι όποτε η M' προσομοιώνει την M με μη ντετερμινιστικές επιλογές που καθορίζονται από το z_2 , πρώτα περνάει από τις ίδιες καταστάσεις που θα περνούσε αν προσομοίωνε την M με μη ντετερμινιστικές επιλογές που καθορίζονται από το z_1 . Οπότε, $M'(x, y_1) = 0$ σημαίνει ότι η προσομοίωση της M φτάνει σε τερματική κατάσταση χρησιμοποιώντας (μερικά από) τα bits της z_1 . Έτσι τα υπόλοιπα bits του z_2 αγνοούνται και επιστρέφεται 0, οπότε $M'(x, y_2) = 0$.

Προκειμένου να ολοκληρώσουμε την απόδειξη, πρέπει να κατασκευάσουμε για κάθε είσοδο x της h ένα κύκλωμα C_n^x με $n = p(|x|) + 1$ πύλες εισόδου, που προσομοιώνει την λειτουργία της M' με είσοδο x , δλδ. για κάθε $y \in \{0, 1\}^n$, $C_n^x(y) = M'(x, y)$. Είναι γνωστό ότι μια τέτοια κατασκευή μπορεί να γίνει σε πολωνυμικό χρόνο (βλ. πχ. [63], pp. 171–172]). Το C_n^x είναι μη αύξον ως προς την \leq_{tree} αφού και M' έχει αυτή την ιδιότητα (λόγω του (iii)). Έτσι έχουμε ότι $|\{y \in \{0, 1\}^n : C_n^x(y) = 1\}| = \#acc_{M'}(x) = \text{tot}_M(x)$, δλδ. $f_{\#MC}(C_n^x) = h(x)$ οπότε η αναγωγή είναι φειδωλή. \square

2.3.2 Το #MONOTONE CIRCUIT SAT ανήκει στην TotP

Από το θεώρημα \square (b), αρκεί να αποδείξουμε ότι η $f_{\#MC}$ είναι αυτοαναγώγιμη και ανήκει στην #PE.

Πρόταση 1. $f_{\#MC} \in \#PE$.

Απόδειξη. Δείχνουμε πρώτα ότι $f_{\#MC} \in \#P$. Έστω M η NPTM που παίρνει σαν είσοδο ένα κύκλωμα C_n , επιλέγει μη ντετερμινιστικά μια είσοδο y για το C_n , προσομοιώνει το C_n με είσοδο y και επιστρέφει $C_n(y)$. Προφανώς, το πλήθος των μονοπατιών αποδοχής της $M(C_n)$ είναι ίσο με $f_{\#MC}(C_n)$. Θα δείξουμε τώρα ότι η αντίστοιχη γλώσσα $L_{f_{\#MC}}$ είναι στο P. Για ένα μη αύξον κύκλωμα C_n , η ύπαρξη ενός y τέτοιου ώστε $C_n(y) = 1$ μπορεί να αποφασιστεί σε πολωνυμικό χρόνο προσομοιώνοντας το C_n με είσοδο 0^n : Είτε $C_n(0^n) = 1$ είτε δεν υπάρχει y τέτοιο ώστε $C_n(y) = 1$, αφού C_n είναι μη αυξον ως προς την \leq_{tree} και $0^n \leq_{tree} y$ για κάθε $y \in \{0, 1\}^n$. \square

2.3. TO #MONOTONE CIRCUIT SAT ΕΙΝΑΙ TOTP-ΠΛΗΡΕΣ ΥΠΟ KARP ΑΝΑΓΩΓΕΣ 73

Για να αποδείξουμε ότι η $f_{\#MC}$ είναι αυτοαναγώγιμη, η διαίσθηση είναι ότι το πλήθος των ικανοποιητικών εισόδων για ένα μη αύξον κύκλωμα C_n ως προς την \leq_{tree} , είναι 0 αν και μόνο αν το 0^n δεν είναι ικανοποιητική ανάθεση. Αλλιώς είναι ίσο με το πλήθος των ικανοποιητικών αναθέσεων που βρίσκονται στο αριστερό υποδέντρο του T_n , συν το πλήθος των ικανοποιητικών αναθέσεων που βρίσκονται στο δεξί υποδέντρο του T_n , συν 1. Θα δείξουμε ότι μπορούμε αποδοτικά να κατασκευάσουμε δύο κυκλώματα μη αύξοντα ως προς την \leq_{tree} : Το C_{n-1}^0 , που παίρνει τιμές συμβατές με τις τιμές που παίρνει το C_n στο αριστερό υποδέντρο του T_n , και το C_{n-1}^1 αντίστοιχα για το δεξί υποδέντρο.

Πρόταση 2. *Η $f_{\#MC}$ είναι αυτοαναγώγιμη.*

Απόδειξη. Αρχικά παρατηρούμε ότι το αριστερό υποδέντρο του T_n είναι ισομορφικό με το T_{n-1} , και το ίδιο ισχύει και για το δεξί υποδέντρο του T_n με ένα επιπλέον παιδί στο αριστερότερο του φύλλο. Έστω g_0, g_1 αυτοί οι δύο ισομορφισμοί, οι οποίοι ορίζονται αυστηρά παρακάτω.

Έστω $V_n^0 \subset \{0, 1\}^n$ το σύνολο κόμβων στο αριστερό υποδέντρο του T_n . Έστω V_n^1 το αντίστοιχο σύνολο για το δεξί υποδέντρο. Έστω $V_{n-1} = \{0, 1\}^{n-1}$ οι κόμβοι του T_{n-1} .

Δείχνουμε ότι οι ισομορφισμοί $g_0 : V_{n-1} \rightarrow V_n^0$, και $g_1 : V_{n-1} \rightarrow V_n^1 \cup \{v\}$, όπου v είναι ένας κόμβος προστεθειμένος στο δεξί υποδέντρο του T_n , είναι αποδοτικά υπολογίσιμοι.

Ορίζουμε $g_i(y) = \text{bin}_n(\text{path}^{-1}(i \parallel \text{path}(\text{bin}_{n-1}^{-1}(y))))$, $i \in \{0, 1\}$, όπου \parallel συμβολίζει την παράθεση συμβολοσειρών και $g_1(1^{n-1}) = v$. Είναι εύκολο να δεικνυθεί ότι οι g_i είναι πολωνυμικά υπολογίσιμοι ισομορφισμοί.

Ανάγουμε ένα κύκλωμα C_n σε δύο κυκλώματα C_{n-1}^0, C_{n-1}^1 τ.ώ. $f_{\#MC}(C_n) = C_n(0^n) + f_{\#MC}(C_{n-1}^0) + f_{\#MC}(C_{n-1}^1)$. Θεωρείστε την ντετερμινιστική μηχανή M η οποία με είσοδο ένα κύκλωμα C_n και $y \in \{0, 1\}^{n-1}$, $M(C_n, y) = C_n(g_1(y))$. Ο χρόνος εκτέλεσης της M είναι πολωνυμικός στο μέγεθος του C_n και του $|y|$. Υπάρχει ένα κύκλωμα $C_{n-1}^1(\cdot)$ που προσομοιώνει την $M(C_n, \cdot)$, δλδ. την M με το πρώτο της όρισμα σταθεροποιημένο στο δεδομένο C_n [63, pp. 171–172]. Το κύκλωμα C_{n-1}^0 μπορεί να κατασκευαστεί με παρόμοιο τρόπο.

Οπότε $f_{\#MC}(C_n) = C_n(0^n) + f_{\#MC}(C_{n-1}^0) + f_{\#MC}(C_{n-1}^1)$. Η αναδρομή τελειώνει μετά από n βήματα, και το μέγεθος του κάθε υποστιγμιοτύπου είναι πολωνυμικά σχετιζόμενο με το μέγεθος του αρχικού στιγμιοτύπου. Άρα η $f_{\#MC}$ είναι αυτοαναγώγιμη. \square

Πόρισμα 1. $f_{\#MC} \in \text{TotP}$.

Παρατήρηση Παρατηρείστε ότι η $f_{\#MC}$ είναι ένα πρόβλημα υπόσχεσης (promise problem), αφού δεν είναι γνωστό πώς να ελέγξουμε αν ένα κύκλωμα είναι μη αύξον ως προς την \leq_{tree} . Αυτό δεν είναι ουσιαστικό πρόβλημα, γιατί μπορούμε να επεκτείνουμε τη συνάρτηση $f_{\#MC}$ στις μη έγκυρες εισόδους, να είναι ίση με $\text{tot}_M(x)$, όπου M είναι η τιμή της NPTM που η ύπαρξή της συνεπάγεται από το γεγονός ότι η $f_{\#MC}$ είναι στην TotP (στις έγκυρες εισόδους).

Επίσης σημειώνουμε ότι το να είναι μια συνάρτηση αυτοαναγώγιμη με εύκολη απόφαση ύπαρξης λύσης, είναι ισχυρότερη ιδιότητα από το να ανήκει στην TotP. Αυτό ισχύει διότι η TotP με το να είναι το KarP-closure των αυτοαναγώγιμων συναρτήσεων με εύκολη απόφαση ύπαρξης, μπορεί να περιέχει και συναρτήσεις που δεν είναι αυτοαναγώγιμες. Οι παραπάνω αποδείξεις δείχνουν ότι η $f_{\#MC}$ έχει αυτήν την ισχυρότερη ιδιότητα.

2.3.3 Συζήτηση σχετικά με την επιλογή της κωδικοποίησης και τη μερική διάταξη

Η συγκεκριμένη επιλογή των συναρτήσεων path και num και η άμεσα σχετιζόμενη μερική διάταξη \leq_{tree} , δεν είναι η μόνη δυνατή. Αυτό που χρειάζεται είναι να κωδικοποιήσουμε συμβολοσειρές πεπερασμένου αλλά πιθανώς διαφορετικού μήκους, που αντιστοιχούν στα υπολογιστικά μονοπάτια της NPTM που σχετίζονται με μια συνάρτηση στην TotP, ως συμβολοσειρές ίδιου μήκους, που αντιστοιχούν στις εισόδους στο τελικό κύκλωμα. Δηλαδή, χρειαζόμαστε μια οικογένεια από ένα προς ένα και επί συναρτήσεις $E_k : \bigcup_{i=0}^{k-1} \{0, 1\}^i \cup \{0^k\} \rightarrow \{0, 1\}^k$. Κάθε τέτοια κωδικοποίηση συνεπάγεται μια μερική διάταξη \leq_k^* στο $\{0, 1\}^k$ για κάθε k .

Έστω μια τέτοια συνάρτηση $(E_k)_k$ και έστω A το πρόβλημα μέτρησης του πλήθους αποδεκτών εισόδων για ένα κύκλωμα μη αύξον ως προς την \leq_m^* , όπου το m αντιστοιχεί στο πλήθος πυλών εισόδου του κυκλώματος. Μπορούμε να αποδείξουμε ότι το A είναι TotP-πλήρες τροποποιώντας τις αποδείξεις αυτής της ενότητας, αρκεί η $(E_k)_k$ να έχει τις ακόλουθες ιδιότητες:

- Για να δείξουμε ότι το A είναι TotP-hard πρέπει η E_m^{-1} να υπολογίζεται εύκολα, έτσι ώστε η αναγωγή να είναι πολυωνυμικού χρόνου. Η αναγωγή είναι φειδωλή αφού η E_m είναι ένα προς ένα και επί. Για παράδειγμα η απλή προσθήκη μηδενικών στην αρχή της συμβολοσειράς, αν και θα αποτελούσε απολούστερη λύση, δεν είναι κατάλληλη, αφού δεν είναι ένα προς ένα.
- Για να δείξουμε ότι το A είναι στην TotP πρέπει να είναι εύκολο να βρει κανείς το ελάχιστο στοιχείο στο $\{0, 1\}^m$ ως προς την \leq_m^* , δλδ. να υπολογίσει το $E_m(\varepsilon)$, όπου ε είναι η κενή συμβολοσειρά. Επιπλέον, για κάθε $x \in \{0, 1\}^m$ πρέπει να είναι εύκολο να υπολογίσει κανείς το σύνολο των άμεσων γειτόνων του ως προς την \leq_m^* . Παρατηρούμε ότι αν η E_m^{-1} είναι εύκολα υπολογίσιμη, τότε αυτές οι ιδιότητες γίνονται ισοδύναμες με την απαίτηση η E_m να είναι εύκολα υπολογίσιμη.

Συμπερασματικά, για να ισχύουν οι αποδείξεις που παρουσιάσαμε και σε γενικότερες επιλογές κωδικοποίησης, χρειαζόμαστε μια κωδικοποίηση που να είναι εύκολα υπολογίσιμη και εύκολα αντιστρέψιμη, ένα προς ένα και επί. Αν και έχουμε διαλέξει, για λόγους ευκολίας στην παρουσίαση, μια κωδικοποίηση απλή και φυσιολογική, τονίζουμε ότι για κάθε κωδικοποίηση με τις παραπάνω ιδιότητες, το αντίστοιχο πρόβλημα θα ήταν επίσης TotP-πλήρες.

2.4 Άλλα TotP-πλήρη προβλήματα

Σε αυτή την ενότητα θα δείξουμε και για άλλα προβλήματα ότι είναι TotP-πλήρη υπό φειδωλές αναγωγές.

Ορισμός 24. Έστω U ένα μερικά διατεταγμένο σύνολο. Ένα υποσύνολο $V \subseteq U$ λέγεται lower set (ή downwards closed) αν για κάθε $y, x \in U$, ($y \in V$ και $x < y$) $\Rightarrow x \in V$.

Ορισμός 25. Έστω ένα κύκλωμα C_n με n πύλες εισόδου. Θα λέμε ένα υποσύνολο V του $\{0, 1\}^n$ C_n -accepting αν για κάθε $x \in V$, $C_n(x) = 1$.

Ορισμός 26. Ορίζουμε το πρόβλημα MAX-LOWER-SET-SIZE.

Είσοδος: Ένα κύκλωμα C_n με n πύλες εισόδου.

Εξοδος: Το μέγεθος του μεγαλύτερου lower set ως προς την w.r.t. \leq_{tree} , που είναι C_n -accepting.

Θεώρημα 11. Το πρόβλημα MAX-LOWER-SET-SIZE είναι TotP-πλήρες.

Απόδειξη. Για να δείξουμε TotP-hardness, παρατηρούμε ότι η ταυτοτική συνάρτηση ανάγει το πρόβλημα #MONOTONE CIRCUIT SAT στο MAX-LOWER-SET-SIZE αφού:

1. Τα στιγμιότυπα του #MONOTONE CIRCUIT SAT είναι μη αύξοντα κυκλώματα ως προς την \leq_{tree} .
2. Για ένα κύκλωμα C_n μη αύξον ως προς την \leq_{tree} , το σύνολο των αποδεκτών εισόδων είναι ακριβώς το μέγιστο C_n -accepting lower set ως προς την \leq_{tree} .

Η απόδειξη συμμετοχής στην TotP χρησιμοποιεί παρόμοια επιχειρήματα με την απόδειξη για το $f_{\#MC} \in \text{TotP}$. Ειδικότερα, ισχύει ότι το $C_n(0^n) = 0$ αν και μόνο εάν το μέγιστο C_n -accepting lower set είναι άδειο, έτσι η απόφαση ύπαρξης λύσης είναι εύκολη.

Από την άλλη πλευρά, ο υπολογισμός του μεγέθους του μέγιστου C_n -accepting lower set ανάγεται στο ίδιο πρόβλημα για δύο άλλα κυκλώματα έτσι ώστε καθένα από αυτά να προσομοιώνει το C_n σε ένα υποδέντρο της tree-partial-order, το δεξί ή το αριστερό αντίστοιχα. Οι λεπτομέρειες της αναγωγής είναι ανάλογες με την απόδειξη της πρότασης [2](#). \square

Στη συνέχεια υποθέτουμε ότι κάθε $n \in \mathbb{N}$ κωδικοποιείται από το $\text{path}(n)$ και έστω το $T_{\mathbb{N}}$ να είναι το άπειρο τέλει δυαδικό δέντρο που αντιπροσωπεύει την $\leq_{tree} \mathbb{N}$ (Figure [2.1](#)).

Το επόμενο πρόβλημα είναι διαισθητικά το πρόβλημα της καταμέτρησης του αριθμού των κόμβων ενός υποδέντρου S του $T_{\mathbb{N}}$, όπου το S δίνεται με ένα σύντομο τρόπο, δηλαδή όχι ρητά, αλλά μέσω ενός υπολογίσιμου σε πολυωνυμικό χρόνο κατηγορήματος (predicate) A που δηλώνει αν ένας κόμβος v του $T_{\mathbb{N}}$ ανήκει στο S . Θυμηθείτε ότι $d_{T_{\mathbb{N}}}(u, v)$ είναι η απόσταση των u, v στο γράφημα $T_{\mathbb{N}}$.

Ορισμός 27. *SIZE-OF-SUBTREE*, συμβολικά f_{ss} :

Είσοδος: $(M_A, u \in T_{\mathbb{N}}, 1^k, 1^t)$ όπου M_A είναι μια ντετερμινιστική μηχανή Turing που υπολογίζει ένα predicate $A : T_{\mathbb{N}} \rightarrow \{0, 1\}$ και $t, k \in \mathbb{N}$.

Εξοδος: Το μέγεθος του μέγιστου (συνδεδεμένου) υποδέντρου S του $T_{\mathbb{N}}$ με ρίζα u , όπου $S \subseteq \{v \in T_{\mathbb{N}} \mid u \leq_{tree} v, d_{T_{\mathbb{N}}}(u, v) \leq k, A(v) = 1 \text{ και } \eta \ A(v) \text{ υπολογίζεται από τη } M_A \text{ σε το πολύ } t \text{ βήματα}\}$.

Θεώρημα 12. *Η f_{ss} είναι TotP-πλήρης.*

Απόδειξη. 1. TotP-hardness: Έστω $g \in \text{TotP}$ και έστων x μια είσοδος για τη g . Θα αντιστοιχίσουμε το x σε μια είσοδο για την f_{ss} . Αφού $g \in \text{TotP}$, υπάρχει μια M_g που τρέχει σε χρόνο $q(n)$ για κάποιο πολυώνυμο q , έτσι ώστε $\#branchings \text{ of } M_g(x) = g(x)$. Κατασκευάζουμε μια M'_g τ.ω. $M'_g(x, y) = 1$ ανν $M_g(x, y)$ αναπαριστά ένα μονοπάτι που καταλήγει σε διακλάδωση. Η είσοδος για την f_{ss} είναι $z = (M'_g(x, \cdot), 0, 1^{q(|x|)}, 1^{q(|x|)})$. Οπότε $f_{ss}(z) = \#branchings \text{ of } M_g(x) = g(x)$.

2. TotP-membership: η f_{ss} έχει εύκολη απόφαση ύπαρξης λύσης, αφού για κάθε είσοδο $y = (M_A, u, 1^k, 1^t)$, $f_{ss}(y) = 0$ ανν είτε $A(u) = 0$ είτε ο υπολογισμός της $A(u)$ υπερβαίνει το t .

Επίσης η f_{ss} είναι αυτοαναγώγιμη. Έστω v_1, v_2 τα παιδιά του u . Ισχύει ότι αν $A(u) = 1$ και υπολογίζεται από την M_A σε χρόνο $\leq t$, τότε

$$f_{ss}(M_A, u, 1^k, 1^t) = f_{ss}(M_A, v_1, 1^{k-1}, 1^t) + f_{ss}(M_A, v_2, 1^{k-1}, 1^t) + 1,$$

$$\text{αλλιώς } f_{ss}(M_A, u, 1^k, 1^t) = 0.$$

Η αναγωγή τερματίζεται μετά από k βήματα και το μέγεθος των υποστιγμιότυπων σχετίζεται πολυωνυμικά με το μέγεθος του αρχικού στιγμιότυπου, έτσι ικανοποιούνται οι συνθήκες αυτοαναγωγής. \square

Στη συνέχεια, παρουσιάζουμε ένα άλλο πρόβλημα που είναι TotP -πλήρες, το οποίο είναι μια ειδική περίπτωση του #SAT. Οι έγκυροι τύποι εισόδου έχουν τις ακόλουθες ειδικές ιδιότητες. Αν θεωρήσουμε μια διάσπαση του χώρου των λύσεων $\{0, 1\}^n$ σε ομάδες, όπου κάθε ομάδα περιέχει όλες τις αναθέσεις με τις πρώτες k μεταβλητές να έχουν φιξαριστεί σε συγκεκριμένες τιμές, τότε ο τύπος έχει το πολύ μία ικανοποιητική ανάθεση από κάθε ομάδα, και είναι εύκολο να αποφασίσουμε αν υπάρχει μια τέτοια ανάθεση, και αν υπάρχει είναι εύκολο να την βρούμε. Επιπλέον, εάν ονοματίσουμε κάθε ομάδα σύμφωνα με τις σταθεροποιημένες τιμές των μεταβλητών, τότε έχουμε ένα συγκεκριμένο είδος μονοτονίας μεταξύ των ομάδων.

Ορισμός 28. 1. Για μια 3-CNF formula ϕ and $k \in \mathbb{N}$ ορίζουμε $f_{\phi}^k : \{0, 1\}^k \rightarrow \mathbb{N}$ s.t. $f_{\phi}^k(a) = \#(\text{satisfying assignments of } \phi \text{ with prefix } a)$ για $a \in \{0, 1\}^k$.

2. Μια 3-CNF formula ϕ με n μεταβλητές, λέγεται (k, n) -clustered-monotone για κάποιο $k \leq n$, αν για κάθε $a, b \in \{0, 1\}^k$ τέτοια ώστε $a \leq_{tree} b$, $f_{\phi}^k(a) = 0$ συνεπάγεται $f_{\phi}^k(b) = 0$.

- Ορισμός 29.** 1. $Y = \{(1^k, 1^n, \phi, M, 1^t) \mid k, n, t \in \mathbb{N}, \phi \in \Phi, \text{ντετερμινιστική } TM M : \{0, 1\}^k \times \Phi \rightarrow \mathbb{N}\}$, όπου Φ είναι το σύνολο των 3-CNF formulae με n μεταβλητές.
2. $U \subset Y$ είναι το σύνολο των διατεταγμένων πλειάδων $(1^k, 1^n, \phi, M, 1^t)$ όπου ϕ είναι (k, n) -clustered monotone, και η M είναι μία ντετερμινιστική TM τέτοια ώστε s.t. $\forall a \in \{0, 1\}^k, M(a, \phi) = \#(\text{satisfying assignments of } \phi \text{ with prefix } a)$, και t είναι ένα άνω φράγμα για το χρόνο εκτέλεσης της M σε κάθε a , και στη δεδομένη ϕ .

Σημειώστε ότι στον παραπάνω ορισμό, η λειτουργία της M είναι διαφοροποιημένη ανάλογα με το αν το στιγμιότυπο είναι στο U ή στο $Y \setminus U$. Στο U έχουμε την υπόσχεση ότι το ϕ είναι clustered monotone και ότι το M μετράει τον αριθμό ικανοποιητικών αναθέσεων σε κάθε ομάδα. Στο Y , και το ϕ και η M μπορεί να είναι αυθαίρετα.

Ορισμός 30. #CLUSTERED-MONOTONE-SAT, συμβολικά $f_{\#CMS}$

Είσοδος: $y = (1^k, 1^n, \phi, M, 1^t) \in Y$

Εξοδος: $f_{\#CMS}(y) = \begin{cases} \#(\text{satisfying assignments of } \phi) & , \text{ if } y \in U \\ \sum_{a \in S} M(a, \phi) & , \text{ if } y \in Y \setminus U \end{cases}$

όπου $S \subseteq T_k$ είναι το μεγαλύτερο υποδέντρο της T_k που περιέχει το 0^k έτσι ώστε $\forall a \in S [M(a, \phi) > 0$ και το $M(a, \phi)$ υπολογίζεται σε t βήματα].

Θεώρημα 13. Η $f_{\#CMS}$ είναι TotP-πλήρης.

Απόδειξη. 1. Ανάγουμε την $f_{\#MC}$ στην $f_{\#CMS}$, δείχνοντας έτσι ότι η $f_{\#CMS}$ είναι TotP-hard.

Έστων C_k ένα Boolean κύκλωμα, μη αύξον ως προς την \leq_{tree} , με k πύλες εισόδου, μία πύλη εξόδου και m επιπλέον (εσωτερικές) πύλες. Θα αντιστοιχίσουμε το C_k σε μια είσοδο y για το $f_{\#CMS}$.

Στη γνωστή αναγωγή του CIRCUIT-SAT στο 3SAT που μπορεί να βρεθεί στο [9, p. 111], μια φόρμουλα ϕ με $n = k + m + 1$ μεταβλητές κατασκευάζεται, έτσι ώστε κάθε μεταβλητή αντιστοιχεί σε μια πύλη του C_k και

$$\#(\text{satisfying assignments for } \phi) = \#(\text{satisfying assignments for } C_k).$$

Μπορούμε να κατασκευάσουμε τη ϕ με τέτοιο τρόπο ώστε οι πρώτες της k μεταβλητές x_1, \dots, x_k να αντιστοιχούν στις k πύλες εισόδου του C_k . Για κάθε $x_i, i \in k + 1, \dots, n$, κατασκευάζουμε (το πολυ τέσσερις) clauses που αναγκάζουν την x_i να πάρει την ίδια τιμή με την έξοδο της αντίστοιχης πύλης του C_k με είσοδο (x_1, \dots, x_k) .

Στη συνέχεια περιγράφουμε έναν αλγόριθμο ο οποίος, όταν δοθεί ένας τύπος ϕ που κατασκευάστηκε με τον παραπάνω τρόπο και μια ανάθεση $a \in \{0, 1\}^k$ στις πρώτες k μεταβλητές του ϕ , αποφασίζει αν υπάρχει κάποια ικανοποιητική ανάθεση του ϕ με a ως πρόθεμα. Εάν υπάρχει μια τέτοια ανάθεση τότε

θα είναι μοναδική αφού κάθε μία από τις μεταβλητές $x_{k+1}, \dots, x_{k+m+1}$ θα πρέπει να είναι ίσο με την έξοδο της αντίστοιχης πύλης C_k στην είσοδο a .

Ο αλγόριθμος ουσιαστικά προσομοιώνει το αρχικό κύκλωμα C_k . Αρχίζει γνωρίζοντας τις καθορισμένες τιμές των x_1, \dots, x_k και υπολογίζει τις τιμές που αντιστοιχούν στην έξοδο και τις εσωτερικές πύλες του C_k . Ενώ υπάρχουν μεταβλητές που δεν έχουν ακόμη καθορισμένη τιμή, κάνει επαναλήψεις ως εξής. Αν μια τέτοια μεταβλητή x_i αντιστοιχεί σε μια πύλη g_i του C_k που οι είσοδοί της αντιστοιχούν σε μεταβλητές στις οποίες έχουν ήδη δοθεί κάποιες τιμές από τον αλγόριθμο, τότε η έξοδος του g_i εκχωρείται στη x_i . Είναι εγγυημένο από την κατασκευή του ϕ ότι μια τέτοια μεταβλητή x_i υπάρχει πάντα. Τέλος, όταν έχουν εκχωρηθεί τιμές σε όλες τις μεταβλητές, ο αλγόριθμος απαντάει αν ο ϕ ικανοποιείται με αυτή την ανάθεση. Εάν ένας αυθαίρετος τύπος ϕ που δεν αντιστοιχεί σε ένα κύκλωμα δίνεται ως είσοδος στον αλγόριθμο, ο αλγόριθμος θα τερματίζει πάντα και θα επιστρέφει είτε FALSE ή TRUE. Για μια ακριβή περιγραφή, δείτε τον Αλγόριθμο [1](#).

Algorithm 1

```

procedure A( $(a_1, \dots, a_k), \phi$ )
    for  $i \leftarrow 1, k$  do
         $x_i \leftarrow a_i$ 
    end for
    for  $i \leftarrow k + 1, n$  do
         $x_i \leftarrow \text{UNDEFINED}$ 
    end for
     $count \leftarrow k$ 
    while  $count < n$  do
         $oldCount \leftarrow count$ 
        for each  $i \in \{k + 1, \dots, n\}$  and each clause  $c$  that occurs in  $\phi$  do
            if  $x_i = \text{UNDEFINED}$  and ( $x_i$  appears exactly once in  $c$ ) and
            (no variable set to UNDEFINED appears in  $c$  except for  $x_i$ ) and
            (the disjunction of literals of  $c$  that do not contain  $x_i$  is FALSE) then
                if  $c$  contains the literal  $x_i$  then
                     $x_i \leftarrow \text{TRUE}$ 
                else
                     $x_i \leftarrow \text{FALSE}$ 
                end if
            end if
             $count \leftarrow count + 1$ 
        end for
        if  $count = oldCount$  then
            return FALSE
        end if
    end while
    return  $\phi(x_1, \dots, x_n)$ 
end procedure

```

▷ ϕ has n variables

▷ The first k variables of ϕ correspond
▷ to the input gates of C_k

▷ The rest of the variables correspond
▷ to the rest of the gates of C_k

▷ #(variables of ϕ we have computed so far)

▷ c contains the literal $\neg x_i$

▷ ϕ has not been constructed by our reduction

Ο χρόνος εκτέλεσης του αλγορίθμου \square είναι πολυωνυμικός στο μέγεθος της εισόδου. Έστω M μια TM που υλοποιεί αυτόν τον αλγόριθμο σε πολυωνυμικό χρόνο και επιστρέφει '1' αν ο αλγόριθμος επιστρέψει TRUE, και '0' διαφορετικά. Έστω p ένα πολυώνυμο που φράσει τον χρόνο εκτέλεσης της M , και έστω s το μέγεθος της αναπαράστασης του ϕ . Μπορούμε να αντιστοιχίσουμε το C_k στην είσοδο $y = (1^k, 1^{k+m+1}, \phi, M, 1^{p(k+s)})$ για την $f_{\#CMS}$.

2. Τώρα θα δείξουμε ότι η $f_{\#CMS}$ είναι στην TotP. Έστων $y = (1^k, 1^n, \phi, A, 1^n)$ μια είσοδος για την $f_{\#CMS}$. Περιγράφουμε μια NPTM με $f_{\#CMS}(y) + 1$ φύλλα, δείχνοντας έτσι ότι το πρόβλημα είναι στην TotP.

Η περιγραφή της NPTM είναι: Αν $A(0^k, \phi) = 0$ ή ο υπολογισμός του $A(0^k, \phi)$ χρειάζεται περισσότερα από t βήματα, τότε HALT, αλλιώς διάλεξε μη ντετερμινιστικά ένα από τα κόλουθα:

(α') HALT

(β') EXPLORE(0^k)

όπου η μη ντετερμινιστική διαδικασία EXPLORE(a) for $a \in \{0, 1\}^k$ ορίζεται ως εξής:

(α') Έστω S το σύνολο των παιδιών του a ως προς την \leq_{tree} . Για κάθε $b \in S$, προσομοίωσε την $A(b, \phi)$ για το πολύ t βήματα. Έστω $S' = \{b \in S \mid A(b, \phi) > 0 \text{ and its computation ends within } t \text{ steps}\}$. Έστω $\rho = |S'| \in \{0, 1, 2\}$.

(β') Δημιούργησε διακλάδωση με $A(b, \phi) + \rho$ κλαδιά. Για καθένα από τα πρώτα $A(b, \phi)$ κλαδιά, HALT. Κάθε ένα από τα υπόλοιπα αντιστοιχούν σε κάποιο $b \in S'$. Εκτέλεσε την EXPLORE(b) για το αντίστοιχο b . \square

Με τον ορισμό του #CLUSTERED-MONOTONE-SAT, το οποίο είναι μια ειδική περίπτωση του #SAT, η διαίσθηση που θέλουμε να καταγράψουμε είναι η ακόλουθη. Κάθε πρόβλημα στην TotP ανάγεται, όπως προκύπτει από την παραπάνω απόδειξη, σε έναν τύπο 3-CNF που είναι clustered monotone και για όλους τους τύπους που δημιουργούνται με αυτόν τον τρόπο έχουμε έναν αποδοτικό αλγόριθμο που επιστρέφει τον αριθμό ικανοποιητικών αναθέσεων σε κάθε ομάδα. Επομένως, αυτή η TotP-πλήρης ειδική περίπτωση του #SAT είναι πολύ πιο δομημένη από την #P-πλήρη έκδοση. Αυτό το γεγονός, σε συνδυασμό με άλλα γνωστά αποτελέσματα σχετικά με την προσέγγιση των προβλημάτων καταμέτρησης, έχει ενδιαφέρουσες συνέπειες, όπως θα συζητήσουμε στην επόμενη υποενότητα, και όπως θα διαπιστώσουμε στα κεφάλαια \square και \square αυτής της εργασίας.

Παρατήρηση Αξίζει επίσης να σημειωθεί ότι το #CLUSTERED-MONOTONE-SAT είναι μια ειδική περίπτωση μιας άλλης #SAT παραλλαγής που είναι SpanP-πλήρης: δεδομένου ενός τύπου ϕ σε n μεταβλητές, και ενός αριθμού $k \leq n$, υπολογίστε τον

αριθμό ικανοποιητικών αναθέσεων που είναι διαφορετικοί στις πρώτες k μεταβλητές [52].

2.5 Επιπτώσεις

2.5.1 Σχετικά με την πολυπλοκότητα του Size-of-Subtree

Το πρόβλημα SIZE-OF-SUBTREE είναι επίσης γνωστό και ως το backtracking tree estimation πρόβλημα, δηλαδή το πρόβλημα του υπολογισμού του μεγέθους ενός backtracking δέντρου, χωρίς να το διατρέξει κανείς εξαντλητικά, το οποίο έχει αρχικά μελετηθεί από τον Knuth [51]. Υπάρχει μια πληθώρα εργασιών πάνω σε αυτό το πρόβλημα που το εξετάζουν από διάφορες οπτικές γωνίες, και προτείνουν αλγόριθμους που επιτυγχάνουν σε πολλές ειδικές περιπτώσεις, και περιπτώσεις που προκύπτουν στην πράξη, βλ. [51, 65, 21, 50, 15, 7].

Παρ' όλα αυτά η πολυπλοκότητα χειρότερης περίπτωσης για αυτό το πρόβλημα ήταν μέχρι τώρα άγνωστη (αν εξαιρέσουμε το [71] όπου η πολυπλοκότητά του μελετάται για ένα μοντέλο υπολογισμού που όμως δεν είναι ισοδύναμο με μηχανή Turing.) Εφόσον αποδεικνύουμε ότι το SIZE-OF-SUBTREE είναι TotP-πλήρες υπό φειδωλές αναγωγές, και εφόσον ως γνωστό, το PERMANENT είναι #P-πλήρες υπό αναγωγές Cook, το #IS είναι #P-πλήρες υπό αναγωγές που διατηρούν την προσέγγιση και τα δύο αυτά προβλήματα ανήκουν την TotP, προκύπτουν τα ακόλουθα πορίσματα.

Πόρισμα 2. • Το SIZE-OF-SUBTREE είναι #P-πλήρες υπό

- αναγωγές Cook (μέσω του PERMANENT)
- Approximation preserving (ή αλλιώς AP) αναγωγές (μέσω του #IS)
- Το SIZE-OF-SUBTREE δεν υπολογίζεται ακριβώς σε πολυωνυμικό χρόνο εκτός αν $PH=P$, και δεν προσεγγίζεται σε πολυωνυμικό χρόνο εκτός αν $NP=RP$.

Από την άλλη πλευρά είναι γνωστό ότι το SIZE-OF-SUBTREE είναι εύκολο να προσεγγιστεί στη μέση περίπτωση, κάτω από συγκεκριμένες κατανομές πιθανότητας πάνω στα στιγμιότυπα [29, 75], πράγμα που μας οδηγεί στο ακόλουθο συμπέρασμα.

Συμπέρασμα: Το #SAT που θεωρείται δύσκολο στη μέση περίπτωση να προσεγγιστεί, ανάγεται με αναγωγές που διατηρούν την προσέγγιση σε ένα πρόβλημα που είναι εύκολα προσεγγίσιμο στη μέση περίπτωση. Αυτό σημαίνει ότι οι αναγωγές που διατηρούν την προσέγγιση δεν διατηρούν απαραίτητα και τη μάζα πιθανότητας πάνω στα στιγμιότυπα. Με άλλα λόγια, τα πολλά δύσκολα στιγμιότυπα του πρώτου προβλήματος μπορεί να αντιστοιχούν μέσω της αναγωγής στα λίγα δύσκολα στιγμιότυπα του δεύτερου προβλήματος.

2.5.2 Σχετικά με την προσεγγισιμότητα της TotP

Είναι γνωστό ότι υπάρχουν προβλήματα στην TotP, π.χ. το #IS (όπως φαίνεται στο [62]), που δεν επιδέχονται ένα FPRAS εκτός αν $NP = RP$ [27] και στην πραγματικότητα δεν επιδέχονται ούτε μια προσέγγιση πολυωνυμικού παράγοντα. Το τελευταίο προκύπτει από το γεγονός ότι για τα αυτοαναγώγισμα προβλήματα στην #P μια προσέγγιση πολυωνυμικού παράγοντα μετατρέπεται σε FPRAS [69].

Θυμηθείτε ότι η TotP περιλαμβάνει ορισμένα προβλήματα που επιδέχονται αποδοτικούς αλγόριθμους προσέγγισης (π.χ. #DNF-SAT, #PERFECTMATCHINGS ενός διμερούς γραφήματος). Υπάρχουν επίσης προβλήματα στην TotP (π.χ. #BIS) που δεν είναι γνωστό ότι έχουν FPRAS, μέχρι τώρα, αλλά δεν φαίνεται να είναι ισοδύναμα με το #SAT ή το #IS.

Ωστόσο, αποδεικνύεται ότι η κλάση TotP επιδέχεται κάποιο είδος πολυωνυμικού χρόνου προσέγγιση: το πρόβλημα SIZE-OF-SUBTREE είναι μια ειδική περίπτωση του προβλήματος backtracking-tree, που μελετήθηκε στο [51]. Σε αυτό το άρθρο ο Knuth πρότεινε έναν πιθανοτικό αλγόριθμο, τον οποίο με κατάλληλη προσαρμογή μπορούμε να χρησιμοποιήσουμε για να προσεγγίσουμε το SIZE-OF-SUBTREE. Η αναμενόμενη τιμή εξόδου του αλγορίθμου είναι ακριβώς η επιθυμητή τιμή, αλλά η διασπορά μπορεί να είναι εκθετική στη χειρότερη περίπτωση. Έτσι, αυτός ο αλγόριθμος δεν δίνει FPRAS. Περιγράφουμε συνοπτικά τον αλγόριθμο του Knuth, προσαρμοσμένο στο πρόβλημά μας.

Προχωρά επιλέγοντας ένα τυχαίο μονοπάτι από τη ρίζα σε ένα φύλλο του δέντρου, μετρώντας τον αριθμό των παιδιών του κάθε κόμβου στο μονοπάτι και εκτιμώντας το μέγεθος του δέντρου να είναι αυτό που θα ήταν αν όλα τα μονοπάτια στο δέντρο ήταν ακριβώς όμοια με το τυχαίο που επιλέξαμε.

Knuth's algorithm [51] adapted for SIZE-OF-SUBTREE (see def. 27):

Step 1. Set $m \leftarrow 0$, $D_0 \leftarrow 1$, $D \leftarrow 0$, $v_0 \leftarrow u$.

Step 2. Compute $S_m \leftarrow \{v \text{ is a child of } v_m \text{ in } T_{\mathbb{N}} \text{ and } A(v) = 1 \text{ and } M_A \text{ computes } A(v) \text{ in at most } t \text{ steps}\}$. Set $d_m \leftarrow |S_m|$. Choose $v_{m+1} \in S_m$ uniformly at random.

Step 3. If $d_m = 0$ or $m \geq k$, then return D .

Step 4. Set $D_{m+1} \leftarrow d_m \cdot D_m$ and $D \leftarrow D + D_{m+1}$. Increase m by 1. Goto Step 2.

Το ακόλουθο θεώρημα είναι μια τροποποίηση του Θεωρήματος 1 του [51], (στο άρθρο αυτό, υπάρχει μια συνάρτηση κόστους c η οποία στην περίπτωσή μας έχει οριστεί ως η σταθερή συνάρτηση $c(\cdot) = 1$.)

Θεώρημα 14. Η αναμενόμενη τιμή του D που επιστρέφεται από τον παραπάνω αλγόριθμο για μια δεδομένη είσοδο $(M_A, u \in T_{\mathbb{N}}, 1^k, 1^t)$ ισούται με τη σωστή έξοδο του SIZE-OF-SUBTREE για αυτήν την είσοδο.

Απόδειξη. (σκαρίφιμα) [51] Έστω ότι v είναι ένας κόμβος του $T_{\mathbb{N}}$ έτσι ώστε $d_{T_{\mathbb{N}}}(u, v) = m$, $1 \leq m \leq k$, $A(v) = 1$ και η M_A υπολογίζει το $A(v)$ σε τα περισσότερα από t βήματα. Στη συνέχεια, το v επιλέγεται από τον αλγόριθμο με πιθανότητα $1/(d_0 d_1 \dots d_{m-1})$ και το D_{m+1} γίνεται ίσο με $d_0 d_1 \dots d_m$. Επομένως, με επαγωγή, το D_m έχει αναμενόμενη τιμή ίση με τον αριθμό των κόμβων στην απόσταση m από τη ρίζα, που ανήκουν στο S . Το άθροισμα όλων των D_m για $0 \leq m \leq k$ έχει αναμενόμενη τιμή ίση με τη σωστή έξοδο SIZE-OF-SUBTREE για τη δεδομένη είσοδο. \square

Το επόμενο θεώρημα είναι ένα πόρισμα του θεωρήματος 2 του [51].

Θεώρημα 15. *Η διασπορά της εξόδου του παραπάνω αλγορίθμου δίνεται από το*

$$\text{Var}(D) = \sum_{v \in S} \frac{1}{d_0^v d_1^v \dots d_{m-1}^v} (|S_{v_1}| - |S_{v_2}|)^2,$$

όπου m είναι το βάθος του κόμβου v , $\forall i$ d_i^v είναι ο αριθμός των παιδιών του κόμβου i στη διαδρομή από τη ρίζα στο v , και για $i = 1, 2$, S_{v_i} είναι το υποδέντρο του S με ρίζα το i -οστό παιδί του v , που συμβολίζουμε με v_i . Αν ο κόμβος v έχει παιδιά 0 ή 1, τότε η συνεισφορά του στο παραπάνω ποσό είναι 0.

Απόδειξη. Το αποτέλεσμα προκύπτει από την εφαρμογή της Εξίσωσης (13) από το [51], με απλοποίηση των όρων. Χρησιμοποιούμε τα γεγονότα ότι η πιθανότητα v που συναντάμε είναι $1/(d_0^v d_1^v \dots d_{m-1}^v)$ και ότι το δέντρο S είναι δυαδικό, έτσι κάθε κόμβος έχει 0, 1 ή 2 παιδιά. \square

Σημειώστε ότι η διασπορά του παραπάνω αλγορίθμου εξαρτάται από την ποσότητα ανισοροπίας στο S . Για παράδειγμα, εάν το S ήταν απόλυτα ισοροπημένο, με την έννοια ότι όλοι οι κόμβοι στο ίδιο βάθος είχαν τον ίδιο βαθμό, τότε η διακύμανση θα ήταν 0. Από την άλλη πλευρά, αν το S συνίστατο π.χ. από την ρίζα, μια μόνο διαδρομή ύψους $n - 1$ στα αριστερά και ένα πλήρες δυαδικό δέντρο ύψους $n - 1$ στα δεξιά, τότε, από το παραπάνω αποτέλεσμα, η διακύμανση θα ήταν εκθετικά μεγάλη.

Η TotP-πληρότητα του SIZE-OF-SUBTREE υπό Karp αναγωγές συνεπάγεται ότι τα παραπάνω αλγοριθμικά αποτελέσματα μπορούν να εφαρμοστούν σε κάθε πρόβλημα στην TotP. Θυμηθείτε ότι η TotP περιέχει όλα τα προβλήματα με δύσκολη μέτρηση πλήθους λύσεων, αλλά εύκολη απόφαση ύπαρξης λύσης [62]. Από την άλλη πλευρά, η πληρότητα που δείξαμε συνεπάγεται ότι αυτοί οι απλοί αλγόριθμοι είναι κατά κάποιον τρόπο οι καλύτεροι που μπορούμε να ελπίζουμε, αφού το #IS ανήκει στην TotP και ένα FPRAS για αυτό το πρόβλημα θα συνεπάγεται $\text{NP} = \text{RP}$. Ωστόσο, θα μπορούσαμε να έχουμε υποεκθετικό σφάλμα σε πολυωνυμικό χρόνο ή πολυωνυμική προσέγγιση σε υποεκθετικό χρόνο. Αφήνουμε την ακριβή κατάσταση προσεγγισιμότητας της TotP ως ανοιχτό ερώτημα.

2.5.3 Σχετικά με την προσέγγιση στη #P, και το τυχαίο SAT

Ένα από τα TotP-πλήρη προβλήματα που παρουσιάζονται σε αυτή την εργασία, το πρόβλημα #CLUSTERED-MONOTONE-SAT, είναι μια έκδοση του #SAT με την ιδιότητα ότι για κάθε έγκυρο στιγμιότυπο όλες οι ικανοποιητικές αναθέσεις συνδέονται με ένα συγκεκριμένο τρόπο. Αυτό μπορεί να ρίξει φως και να βοηθήσει στην καλύτερη κατανόηση της δυσκολίας προσέγγισης του γενικού προβλήματος #SAT όπως εξηγείται παρακάτω.

Υπάρχει μια σειρά άρθρων στη βιβλιογραφία (βλ. [1]) για μια πολύ ολοκληρωμένη έρευνα σε αυτόν τον τομέα), που διερευνά τις συνδέσεις μεταξύ της στατιστικής φυσικής και της θεωρητικής πληροφορικής. Μερικοί αλγόριθμοι που έχουν σχεδιαστεί για τη στατιστική φυσική εφαρμόζονται σε προβλήματα καταμέτρησης στην επιστήμη των υπολογιστών, καθώς και τα δύο έχουν την ίδια μαθηματική μορφή. Ρυθμίζοντας ορισμένες παραμέτρους, παρατηρούμε φαινόμενα αλλαγής φάσης. Για την περίπτωση του #SAT, μία παράμετρος είναι η πυκνότητα ενός τύπου ϕ , $a = \#(\text{clauses of } \phi) / \#(\text{variables of } \phi)$ και παρατηρήθηκε ότι για μια κρίσιμη τιμή a_c υπάρχει μια αλλαγή φάσης με την έννοια ότι σχεδόν όλοι οι τύποι είναι ικανοποιήσιμοι για μικρότερες τιμές από το a_c και σχεδόν όλοι οι τύποι είναι μη ικανοποιητικοί για μεγαλύτερες τιμές. Οι φόρμουλες του SAT και #SAT που θεωρούνται δύσκολα στιγμιότυπα, είναι εκείνες με πυκνότητα κοντά στην κρίσιμη τιμή.

Μια παρατήρηση που επιτυγχάνεται με αυτές τις προσεγγίσεις [2, 4], είναι ότι στην κρίσιμη πυκνότητα, το σύνολο των ικανοποιητικών αναθέσεων για μια τυχαία φόρμουλα είναι διάσπαρτα σε ομάδες μεταβλητών “παγωμένων”, δηλαδή οι ικανοποιητικές αναθέσεις σε μια ομάδα έχουν κάποιο αριθμό μεταβλητών που έχουν οριστεί σε μια κοινή τιμή. Οι ομάδες είναι διάσπαρτες στο χώρο των λύσεων με έναν άγνωστο τρόπο. Επομένως, τα ακόλουθα γεγονότα θεωρήθηκαν ως οι βασικές δυσκολίες των SAT και #SAT:

1. ο διασκορπισμός των λύσεων
2. η δυσκολία να βρεθεί έστω και μία λύση στην περίπτωση που υπάρχει

Στο [27], ορίστηκε η αναγωγή που διατηρεί την προσέγγιση, \leq_{AP} και η ισοδυναμία, \equiv_{AP} έτσι ώστε το $A \equiv_{AP} B$ ανν ένα FPRAS για το B υπάρχει αν και μόνο αν ένα FPRAS για το A υπάρχει. Επιπλέον, δεδομένου ότι για τα αυτοαναγόμενα προβλήματα στη #P, το FPRAS είναι ισοδύναμο με την προσέγγιση πολυωνυμικού παράγοντα σε πολυωνυμικό χρόνο [69], αυτό σημαίνει επίσης ότι το A έχει προσέγγιση πολυωνυμικού παράγοντα αν και μόνο αν το B έχει.

Όπως δείξαμε για το SIZE-OF-SUBTREE, προκύπτει παρόμοια και για το πρόβλημα #CLUSTERED-MONOTONE-SAT το ακόλουθο πόρισμα.

Πόρισμα 3. • Το #CLUSTERED-MONOTONE-SAT είναι #P-πλήρες υπό

- αναγωγές Cook (μέσω του PERMANENT)
- Approximation preserving (ή αλλιώς AP) αναγωγές (μέσω του #IS)

- Το $\#CLUSTERED-MONOTONE-SAT$ δεν υπολογίζεται ακριβώς σε πολυωνυμικό χρόνο εκτός αν $PH=P$, και δεν προσεγγίζεται σε πολυωνυμικό χρόνο εκτός αν $NP=RP$.

Κυρίως εστιάζουμε στο παρκάτω πόρισμα.

Πόρισμα 4. $\#SAT \equiv_{AP} \#CLUSTERED-MONOTONE-SAT$

Απόδειξη. Στο [27] αποδεικνύεται ότι $\#SAT \equiv_{AP} \#IS$. Αφού $\#IS \in TotP$ είναι φειδωλά αναγόμενο στο $\#CLUSTERED-MONOTONE-SAT$, και οι φειδωλές αναγωγές διατηρούν την προσέγγιση. \square

Έτσι, τα αποτελέσματά μας σε σχέση με τα αποτελέσματα στο [27] δείχνουν τα ακόλουθα. Κάθε τύπος (του γενικού προβλήματος SAT) ανάγεται με αναγωγές που διατηρούν την προσέγγιση, σε έναν άλλο τύπο με τις ακόλουθες ιδιότητες:

1. Οι λύσεις συνδέονται με έναν συγκεκριμένο τρόπο, που περιγράφεται ρητά από μια δομή δέντρου, έτσι ώστε για κάθε λύση είναι εύκολο να βρεθούν οι γειτονικές λύσεις ως προς αυτό το δέντρο.
2. Είναι εύκολο να αποφασίσουμε εάν υπάρχει λύση, και αν ναι, εύκολο να τη βρούμε.

Αυτό μπορεί να εκληφθεί με δύο τρόπους: Για έναν αισιόδοξο δείχνει ότι η προσέγγιση του $\#SAT$ μπορεί να μην είναι τόσο δύσκολη τελικά (π.χ. ίσως $NP = RP$). Από την άλλη πλευρά, ένας απαισιόδοξος μπορεί να καταλήξει στο συμπέρασμα ότι το $\#SAT$ δεν είναι μόνο δύσκολο γενικά, αλλά ακόμη και για φαινομενικά πιο εύκολα στιγμιότυπα (δλδ πολύ πιο δομημένα και με περισσότερη πληροφορία) θα είχε την ίδια δυσκολία.

Αυτό επίσης υποδηλώνει φυσικά μια νέα κατεύθυνση έρευνας σχετικά με την πολυπλοκότητα της προσέγγισης του $\#SAT$. Πρέπει να αναζητήσουμε και να αναλύσουμε όχι μόνο αλγόριθμους που βασίζονται μόνο στη δομή μιας φόρμουλας ή στη δομή του υπερκύβου, όπως γινόταν μέχρι τώρα, αλλά και για αλγόριθμους που εκμεταλλεύονται τη δομή των δέντρων που συνδέουν τις λύσεις μεταξύ τους.

2.6 Συμπεράσματα και ανοιχτά προβλήματα

Έχουμε παρουσιάσει για πρώτη φορά ορισμένα προβλήματα τα οποία είναι TotP-πλήρη υπό φειδωλές αναγωγές, κάτι που μπορεί να αποδειχθεί ένα σημαντικό βήμα προς την καλύτερη κατανόηση της κλάσης πολυπλοκότητας TotP. Ωστόσο, αυτά τα πλήρη προβλήματα δεν είναι επαρκώς μελετημένα από την επιστημονική κοινότητα, όπως άλλα προβλήματα στην TotP, για παράδειγμα το $\#IS$, το PERMANENT, κλπ. Η πληρότητα ήδη γνωστών προβλημάτων εξακολουθεί να αποτελεί μια ενδιαφέρουσα ανοιχτή ερώτηση. Σημειώστε ότι εάν, π.χ., οποιοδήποτε από τα PERMANENT, $\#ALLMATCHINGS$ ενός γράφου ή $\#PERFECTMATCHINGS$ ενός διμερούς γραφήματος είναι TotP-πλήρες υπό φειδωλές αναγωγές, τότε $NP = RP$,

αφού όλα αυτά τα προβλήματα επιδέχονται FPRAS. Εντούτοις, είναι ένα μακροχρόνια ανοιχτό ερώτημα αν το #PERFECTMATCHINGS ενός αυθαίρετου γραφήματος επιδέχεται FPRAS ή όχι. Σαφώς, το #PERFECTMATCHINGS ανήκει στην TotP, επειδή είναι αυτοαναγώγιμο και η απόφασή του είναι στο P. Έτσι, αν το πρόβλημα #PERFECTMATCHINGS ενός αυθαίρετου γραφήματος είναι TotP-πλήρες υπό φειδωλές μειώσεις, τότε αυτή η ερώτηση θα επιλυθεί, αφού τότε δεν θα επιδέχεται FPRAS εκτός αν $NP = RP$.

Μια άλλη ενδιαφέρουσα κατεύθυνση θα ήταν να διερευνηθεί η κατάσταση προσέγγισης των προβλημάτων που παρουσιάζονται σε αυτό το κεφάλαιο. Η πιθανή προσέγγιση των προβλημάτων αυτών μεταφέρεται άμεσα σε κάθε πρόβλημα στην TotP.

Είναι επίσης ένα ανοιχτό πρόβλημα να εξεταστεί η πιθανότητα μη τετριμμένων, υποεκθετικού χρόνου αλγορίθμων για την προσέγγιση του #SAT, που να εκμεταλλεύονται τη δομή δέντρου που συνδέει τις λύσεις του #CLUSTERED-MONOTONE-SAT, όπως συζητήσαμε στην προηγούμενη ενότητα. Για το σκοπό αυτό, θα ήταν επίσης σκόπιμο να μελετηθούν και να καθοριστούν άλλα είδη αναγωγών που δεν διατηρούν μόνο τα FPRAS αλλά και ασθενέστερες ιδιότητες προσέγγισης.

Τέλος, είναι ανοιχτό ερώτημα είναι να καθορίσουμε υποκλάσεις της TotP που επιδέχονται FPRAS ή άλλα είδη προσέγγισης, καλύτερα από τον αλγόριθμο του Knuth.

Κεφάλαιο 3

Προσεγγισιμότητα

3.1 Εκθετικού χρόνου πολυπλοκότητα προσέγγισης

Αυτή η ενότητα αφορά την προσέγγιση των συναρτήσεων στην TotP. Είναι γνωστό ότι FPRAS για όλα τα προβλήματα στο TotP είναι εφικτό αν και μόνο αν $NP = RP$. Το ίδιο ισχύει και για τη #P. Ωστόσο, σε αυτή την ενότητα δείχνουμε ότι μπορούμε να έχουμε κάποια καλύτερα αποτελέσματα για την TotP απ' ό,τι για τη #P εξετάζοντας την πολυπλοκότητα μεγαλύτερων χρόνων από τον πολυωνυμικό. Πρώτον, για κάθε στιγμιότυπο για οποιοδήποτε πρόβλημα στην TotP, αν ο αριθμός λύσεων είναι x , μπορούμε να υπολογίσουμε ακριβώς αυτόν τον αριθμό σε χρόνο $x \cdot poly(n)$, όπου n είναι το μέγεθος της εισόδου. Με άλλα λόγια, αν ο αριθμός των λύσεων είναι πολυωνυμικός (δηλαδή μικρός), μπορούμε να τις μετρήσουμε ακριβώς σε πολυωνυμικό χρόνο. Δεύτερον, αν ο αριθμός των λύσεων είναι $2^n/x$, μπορούμε να έχουμε RAS (δηλαδή αυθαίρετα μικρό πολλαπλασιαστικό σφάλμα) σε χρόνο $poly(n, x)$. Με άλλα λόγια, εάν ο αριθμός των λύσεων είναι $2^n/poly(n)$ (δηλαδή μεγάλος), μπορούμε να τον προσεγγίσουμε με FPRAS. Τρίτον, αν συνδυάσουμε τα παραπάνω αποτελέσματα με το γνωστό γεγονός ότι όλα τα προβλήματα στη #P επιδέχονται μια προσθετικού σφάλματος προσέγγιση, παίρνουμε καλύτερα εκθετικού χρόνου αλγοριθμικά αποτελέσματα για την TotP από τα αντίστοιχα γνωστά αποτελέσματα για τη #P. Παραμένει ανοιχτό το ερώτημα εάν αυτά τα αποτελέσματα είναι βέλτιστα υπό μια fine grained οπτική πολυπλοκότητας (δηλ. Με κάποια παραδοχή ανάλογη με την SETH, η οποία δηλώνει σε γενικές γραμμές ότι το SAT χρειάζεται για να λυθεί χρόνο $\Theta(2^n)$).

3.1.1 Εισαγωγή

Δεδομένου ότι τα υπολογιστικά προβλήματα ακριβούς μέτρησης φαίνονται δύσκολα (αν $P \neq NP$), μια πρώτη ερώτηση που προκύπτει είναι η δυνατότητα προσέγγισής τους. Όπως έχουμε ήδη αναφέρει στην εισαγωγή, και η #P και η TotP επιδέχονται FPRAS αν $NP=RP$, και ένα FPRAS για τα αυτοαναγώγιμα προβλήματα μπορεί να προκύψει ακόμα και από έναν πολυωνυμικού σφάλματος αλγόριθμο.

Οπότε μια άλλη ενδιαφέρουσα ερώτηση είναι η ακριβής (πιθανώς εκθετική) πολυπλοκότητα προσέγγισής τους, και πιο συγκεκριμένα, σε σύγκριση με το χρόνο που χρειάζεται η εξαντλητική αναζήτηση. Υπάρχουν εικασίες που λένε ότι η #P δεν προσεγγίζεται σε χρόνο μικρότερο από της εξαντλητικής αναζήτησης. Δείχνουμε ότι για την TotP μπορούμε να επιτύχουμε όσο μικρό σφάλμα θέλουμε σε χρόνο $O(\epsilon^{-2} \text{poly}(n) 2^{2n/3})$, που είναι αυστηρά μικρότερος από της εξαντλητικής αναζήτησης, όπως επίσης και από τους αντίστοιχους αλγόριθμους για την #P.

3.1.2 Συνεισφορά

Δείχνουμε ότι για κάθε f στην TotP, και $g : \mathbb{N} \rightarrow \mathbb{N}$ μια υπολογίσιμη σε $O(g(n))$ χρόνο συνάρτηση, μπορούμε να αποφασίσουμε ντετερμινιστικά αν $f(x) \leq g(n)$ σε χρόνο $g(n) \cdot \text{poly}(n)$, όπου n είναι το μέγεθος της εισόδου x . Δεύτερον αν $f(x) \geq 2^n/g(n)$ μπορούμε να επιτύχουμε ϵ -multiplicative προσέγγιση σε χρόνο $\text{poly}(n, g(n), \epsilon^{-1})$.

Συνδυάζοντας τα παραπάνω με το γνωστό αλγόριθμο προσθετικού σφάλματος για κάθε πρόσβλημα στη #P (θεώρημα [B](#)), δείχνουμε τα παρακάτω αποτελέσματα όσον αφορά στην εκθετικού χρόνου πολυπλοκότητα προσέγγισης προβλημάτων στην TotP.

Ο προσθετικού σφάλματος αλγόριθμος μπορεί ισοδύναμα να θεωρηθεί ότι υπολογίζει το $f(x)$ με απόλυτο σφάλμα $\epsilon \cdot 2^n, \forall \epsilon > 0$, οπότε θέτοντας το ϵ κατάλληλα, παίρνουμε ένα απόλυτο σφάλμα της τάξης του $2^{(\beta+1)n/2}$ σε χρόνο της τάξης του $2^{(1-\beta)n} \text{poly}(n), \forall \beta \in (0, 1)$. Δείχνουμε επίσης ότι μπορούμε να πετύχουμε σε χρόνο της τάξης του $(2^{(\beta+1)n/2} + 2^{(1-\beta)n}) \text{poly}(n), \forall \beta \in (0, 1)$ και πολυωνυμικό στο ϵ^{-2} , προσεγγιστικό σχήμα, (δλδ πολ/κό σφάλμα $\epsilon, \forall \epsilon > 0$). Επίσης θέτοντας $\beta = 1/3$ μπορούμε να επιτύχουμε όσο μικρό σφάλμα θέλουμε σε χρόνο $O(\epsilon^{-2} \text{poly}(n) 2^{2n/3})$. Όλοι αυτοί οι χρόνοι εκτέλεσης είναι καλύτεροι από την εξαντλητική αναζήτηση.

3.1.3 Σχετικές εργασίες και ανοιχτά προβλήματα

Όπως είπαμε ήδη, για την TotP, πολυωνυμικό σφάλμα σε πολυωνυμικό χρόνο είναι αδύνατο εκτός αν NP=RP. Τα αποτελέσματά μας δείχνουν ότι μπορούμε να έχουμε RAS σε χρόνο μικρότερο από την εξαντλητική αναζήτηση. Πρέπει όμως να τονίσουμε ότι αυτά τα αποτελέσματα δεν επεκτείνονται στο #SAT μέσω της αναγωγής στο #IS που διατηρεί το FPRAS ([\[27\]](#)), διότι αυτή η αναγωγή αντιστοιχεί μια φόρμουλα με n μεταβλητές, σε ένα γράφημα με n^2 κόμβους, οπότε οι εκθετικοί χρόνοι δεν διατηρούνται.

Μια ενδιαφέρουσα ανοιχτή ερώτηση είναι να βρούμε μέσα στην TotP έναν δομικό χαρακτηρισμό της κλάσης των προβλημάτων που επιδέχονται ένα FPRAS, δηλαδή να βρούμε ποια είναι η σημαντική κοινή ιδιότητα που τα καθιστά προσεγγίσιμα.

Η μελέτη της εκθετικής χρονικής πολυπλοκότητας των προβλημάτων στο NP ξεκίνησε από τον Impagliazzo et al στο [\[41\]](#) όπου έδειξαν αποτελέσματα εκθετικής

δυσκολίας. Για το #k-SAT υπήρξαν κάποιοι αλγόριθμοι στη βιβλιογραφία:

Στο [71] ο Stockmeyer απέδειξε ότι υπάρχει πολυωνυμικού χρόνου πιθανοτικός αλγόριθμος για την #P, με πρόσβαση σε ένα Σ_2P μαντείο. Στο [74] ο Taxler απέδειξε την ύπαρξη πιθανοτικού αλγόριθμου προσέγγισης σταθερού παράγοντα, με εκθετικό χρόνο αλλά μικρότερο από $2^n \cdot poly(m, n)$, όπου n είναι ο αριθμός μεταβλητών και m ο αριθμός των παρενθέσεων (clauses) της εισόδου, υπό την προϋπόθεση ότι το k-SAT (εννοείται το πρόβλημα απόφασης) είναι επιλύσιμο σε $O(2^{cn}m^d)$ για $0 < c < 1$ και $d \geq 1$ (δλδ με την υπόθεση ότι η εικασία ETH είναι ψευδής). Στο [72] ο Thurley δίνει σχήμα προσέγγισης, δηλαδή $\forall \epsilon > 0$ μπορεί να επιτύχει πολλαπλασιαστικό σφάλμα ϵ σε χρόνο $O^*(\epsilon^{-2}c_k^n)$ όπου $c_k < 2$. Στο [40] οι Impagliazzo et al δίνουν πιθανοτική ακριβή καταμέτρηση σε χρόνο $O^*(2^{(1-\frac{1}{30k})n})$. Υπάρχει επίσης ένας αλγόριθμος, χωρίς θεωρητική εγγύηση, στο [35] από τους Gomes et al. που υλοποιεί την ιδέα του Stockmeyer με κάποιον SAT solver, με εξαιρετική απόδοση σε πρακτικές εφαρμογές.

Δεδομένου ότι το #3-SAT είναι #P-πλήρες, όλα τα προβλήματα στην TotP μπορούν να αναχθούν σε αυτό και έτσι μπορούμε να επιτύχουμε τέτοιες προσεγγίσεις και για αυτά επίσης, χρησιμοποιώντας τους παραπάνω αλγόριθμους.

Ωστόσο, δεδομένου ότι η μέτρηση των λύσεων είναι γενικά πιο δύσκολη από την απόφαση ύπαρξης λύσης, είναι σκόπιμο να διερευνηθεί η εκθετική χρονική πολυπλοκότητα της μέτρησης ακόμη και για προβλήματα με απόφαση στο P, αφού όπως είδαμε ήδη, πολλά από τα τελευταία θεωρούνται μη προσεγγίσιμα σε πολυωνυμικό χρόνο.

Ο αλγόριθμός μας για τα προβλήματα που ανήκουν στην TotP είναι καλύτερος από όλα τα παραπάνω αποτελέσματα της βιβλιογραφίας, με την έννοια ότι μπορούμε να έχουμε ένα σχήμα προσέγγισης σε χρόνο $O(\epsilon^{-2}2^{\gamma n})$, για όλα τα $\gamma \in (2/3, 1)$, χωρίς κλήση σε κανένα oracle, και χωρίς καμία παραδοχή. Ο αλγόριθμος του Impagliazzo είναι καλύτερος από τον δικό μας με την έννοια ότι δίνει ακριβή μέτρηση, αλλά είναι χειρότερος ως προς το χρόνο εκτέλεσης. Σημειώστε βεβαίως ότι εάν αποπειραθούμε να λύσουμε τα προβλήματα της TotP μέσω αναγωγής τους στο 3-SAT και έπειτα λύνοντας το 3-SAT με τη χρήση των προαναφερθέντων αλγορίθμων της βιβλιογραφίας, τότε εάν ο αριθμός μεταβλητών του προκύπτοντος τύπου είναι μεγαλύτερος από $n + c$, για κάθε σταθερά c , όπου n το μέγεθος της εισόδου του αρχικού προβλήματος, οι παραπάνω αλγόριθμοι έχουν χρόνο εκτέλεσης ακόμη χειρότερο ως προς n .

Παρατηρούμε και πάλι ότι ντετερμινιστικό / πιθανοτικό σχήμα πολυωνυμικού χρόνου προσέγγισης για την TotP δεν υπάρχει, εκτός εάν $P = NP$ / $NP = RP$ αντίστοιχα. Είναι ένα ανοιχτό πρόβλημα αν μπορούμε να έχουμε προσεγγιστικό σχήμα με χρόνο εκτέλεσης υπερπολυωνυμικό, αλλά υποεκθετικό, όπως $n^{\log n}$.

Τέλος, υπάρχει πρόσφατο άρθρο των Lapinskas et.al. σε fine grained complexity της κατά προσέγγιση μέτρησης [23], όπου παρουσιάζουν το ανάλογο της SETH για το #SAT. Είναι μια ενδιαφέρουσα ανοιχτή ερώτηση να διαπιστώσουμε εάν τα αποτελέσματά μας είναι βέλτιστα βάσει αυτών των παραδοχών που παρουσιάζονται στο [23].

3.1.4 Προαπαιτούμενα

Υποθέτουμε ότι ο αναγνώστης είναι εξοικειωμένος με τις βασικές έννοιες της υπολογιστικής πολυπλοκότητας, όπως η ντετερμινιστική μηχανή Turing, το boolean κύκλωμα, ο τύπος CNF (conjunctive normal form), ο τύπος DNF (disjunctive normal form) και οι κλάσεις NP, P, RP, NEXP, EXP^{NP} , P / poly, #P, FP. Για τους ορισμούς βλέπε π.χ. [9].

Παραπέμπουμε στο εισαγωγικό κεφάλαιο αυτής της εργασίας για τους ορισμούς των τύπων προσεγγίσεων και της TotP.

3.1.5 Αποτελέσματα

Στο εξής, έστω f μια συνάρτηση στο TotP, και M η αντίστοιχη NPTM για την οποία $\forall x (\# \text{branchings of } M(x)) = f(x)$. Έστω n το μέγεθος της εισόδου ή κάποια παράμετρος πολυπλοκότητας που μας ενδιαφέρει (π.χ. ο αριθμός μεταβλητών σε ένα boolean τύπο ή κύκλωμα), και έστω n' το πλήθος των μη ντετερμινιστικών bits που χρησιμοποιεί η M όταν παίρνει είσοδο x , το οποίο πλήθος είναι ίσο με το ύψος του δέντρου υπολογισμού της $M(x)$ (όπου οι εσωτερικοί κόμβοι είναι τα σημεία διακλάδωσης δηλαδή οι θέσεις όπου το M κάνει μια μη ντετερμινιστική επιλογή). Φυσικά το n' είναι πολυωνυμικό στο n . Προσέξτε ότι το n' εδώ συμβολίζεται με n στην πρόταση 6, καθώς είναι το ύψος του υπολογιστικού δέντρου. Προκειμένου τα αποτελέσματα να έχουν κάποιο νόημα, θεωρούμε τις συναρτήσεις $s : \mathbb{N} \rightarrow \mathbb{N}$ που είναι θετικές, με τιμές όσο μικρές θέλουμε, αλλά το πολύ $O(2^n)$.

Αποδεικνύουμε τα εξής.

Θεώρημα 16. Για κάθε $f \in \text{TotP}$, $x \in \Sigma^*$, $s : \mathbb{N} \rightarrow \mathbb{N}$ όπως παραπάνω, μπορούμε να αποφασίσουμε ντετερμινιστικά σε χρόνο $O(s(n) \cdot \text{poly}(n))$ αν $f(x) \leq s(n)$.

Απόδειξη. Πραγματοποιούμε μια αναζήτηση bfs ή dfs στο υπολογιστικό δέντρο της $M(x)$ (δλδ. πραγματοποιούμε εξαντλητική αναζήτηση δοκιμάζοντας όλες τις μη ντετερμινιστικές επιλογές) μέχρι να μετρήσουμε το πολύ $s(n)+1$ διακλάδώσεις. Αν το δέντρο εξαντληθεί στο μεταξύ, τότε προφανώς $f(x) \leq s(n)$, αλλιώς $f(x) > s(n)$. \square

Θεώρημα 17. Για κάθε $f \in \text{TotP}$, $x \in \Sigma^*$, $s : \mathbb{N} \rightarrow \mathbb{N}$, αν $f(x) \geq 2^{n'}/s(n)$ μπορούμε πιθανοτικά να υπολογίσουμε μια τιμή $\hat{f}(x)$ σε χρόνο $O(\text{poly}(n, s(n), \epsilon^{-1}))$ τέτοια ώστε

$$\hat{f}(x) = f(x)(1 \pm \epsilon).$$

Απόδειξη. Προκύπτει από το unbiased estimator theorem:

Λήμμα 3. Έστω $A \subseteq B$ δύο πεπερασμένα σύνολα και έστω $p = \frac{|A|}{|B|}$. Έστω ότι παίρνουμε m τυχαία δείγματα από το B ομοιόμορφα και ανεξάρτητα, και έστω a το πλήθος αυτών των δειγμάτων που ανήκουν στο A . Τότε $\hat{p} = \frac{a}{m}$ είναι μια αμερόληπη εκτιμήτρια (unbiased estimator) του p , και αρκεί $m = \text{poly}(p^{-1}, \epsilon^{-1}, \log \delta^{-1})$ προκειμένου να έχουμε

$$\Pr[(1 - \epsilon)p \leq \hat{p} \leq (1 + \epsilon)p] \geq 1 - \delta.$$

(Για μια απόδειξη του unbiased estimator theorem, βλ. [68], ή στο εισαγωγικό κεφάλαιο της παρούσας διατριβής το θεώρημα 8.) Για να ολοκληρώσουμε την απόδειξη του θεωρήματός μας, θεωρούμε το τέλει δυαδικό δέντρο T ύψους n' , και διαλέγουμε m τυχαίους κόμβους του T ομοιόμορφα και ανεξάρτητα. Η επιθυμητή προσέγγιση είναι το πλήθος αυτών των κόμβων που ανήκουν στο υπολογιστικό δέντρο της $M(x)$. \square

Θεώρημα 18. Για κάθε $f \in TotP$, $\forall s : \mathbb{N} \rightarrow \mathbb{N}$, $\forall x \in \{0, 1\}^*$, $\forall \delta \in (0, 1)$, με πιθανότητα $1 - \delta$, σε χρόνο $\frac{2^{n'}}{s(n')} poly(n, \log \delta^{-1})$, όπου n' όπως πριν, μπορούμε να επιτύχουμε προσέγγιση $\hat{f}(x) = f(x) \pm 2^{n'/2} s(n')^{1/2}$. Για οποιοδήποτε $\beta \in (0, 1)$, σε χρόνο $2^{(1-\beta)n'} poly(n, \log \delta^{-1})$, μπορούμε να επιτύχουμε $\hat{f}(x) = f(x) \pm 2^{n'(1+\beta)/2}$.

Απόδειξη. Από την απόδειξη της πρότασης 8 και συγκεκριμένα από τα επιχειρήματα ανάλυσης διασποράς (βλ. κεφάλαιο εισαγωγής το θεώρημα 8), μπορούμε να διαπιστώσουμε ότι η πραγματική εξάρτηση του χρόνου εκτέλεσης με είσοδο ξ είναι ανάλογη του ξ^{-2} . Οπότε παίρνουμε την πρώτη εκτίμηση θέτοντας $\xi = \sqrt{\frac{s(n')}{2^{n'}}$, και τη δεύτερη θέτοντας $s(n') = 2^{\beta n'}$. \square

Το επόμενο θεώρημα δείχνει ότι μπορούμε να έχουμε RAS για κάθε πρόβλημα στην TotP, σε χρόνο αυστηρά μικρότερο αυτού της εξαντλητικής αναζήτησης. Ουμνηθείτε ότι δεν μπορούμε να έχουμε FPRAS, δλδ προσεγγιστικό σχήμα σε πολυωνυμικό χρόνο, εκτός αν $NP=RP$.

Θεώρημα 19. Για κάθε f , x , s , δ , n , n' όπως πριν, και για κάθε $k \in \mathbb{R}$, με πιθανότητα $1 - \delta$ και σε χρόνο $poly(k, n, \log \delta^{-1}) (\frac{2^{n'}}{s(n')} + 2^{n'/2} s(n')^{1/2})$, μπορούμε να επιτύχουμε εκτίμηση $\hat{f}(x) = f(x) (1 \pm \frac{1}{k})$.

Για κάθε $\beta \in (0, 1)$, μπορούμε να έχουμε όμοια εκτίμηση, δλδ. RAS, σε χρόνο $poly(k, n, \log \delta^{-1}) (2^{(1-\beta)n'} + 2^{(1+\beta)n'/2})$.

Μπορούμε επίσης να επιτύχουμε uniform sampling σε ανάλογο χρόνο.

Απόδειξη. Πρώτα ελέγχουμε ντετερμινιστικά αν $f(x) \leq k 2^{n'/2} s(n')^{1/2}$, στην οποία περίπτωση παίρνουμε την ακριβή τιμή του $f(x)$. Αλλιώς, αν $f(x) > k 2^{n'/2} s(n')^{1/2}$, εφαρμόζουμε τον αρχικό αλγόριθμο για να πάρουμε $\hat{f} = f(x) \pm 2^{n'/2} s(n')^{1/2}$ το οποίο είναι $< f(x) \pm \frac{1}{k} f(x) = (1 \pm \frac{1}{k}) f(x)$. Ο χρόνος εκτέλεσης προκύπτει από το θεώρημα 16 και το πόρισμα 18.

Μπορούμε επίσης να έχουμε uniform sampling σε ανάλογο χρόνο, αφού στο [69] αποδεικνύεται ότι ένα πιθανοτικό προσεγγιστικό σχήμα μπορεί να χρησιμοποιηθεί για uniform sampling με μία πολυωνυμικού χρόνου επιβάρυνση στο χρόνο εκτέλεσης. \square

Παρατηρήστε ότι το n' σε πολλές περιπτώσεις, όπως είναι διάφορα προβλήματα πάνω σε γραφήματα, φόρμουλες, κυκλώματα κλπ., ισούται με $n + constant$.

Για όλα αυτά τα προβλήματα, αφού $n' = n + constant$, όλα τα παραπάνω θεωρήματα ισχύουν έχοντας αντικαταστήσει το n' με n .

Πόρισμα 5. Για προβλήματα για τα οποία $n' = n + \text{constant}$, όπως το #IS, και #SAT για DNF formulas, monotone circuits κλπ., όλα τα παραπάνω πορίσματα ισχύουν βάζοντας n όπου n' .

Μπορούμε να διερευνήσουμε αν μπορούμε να επεκτείνουμε το πόρισμα [19] για προβλήματα στη #P. Ένας πιθανός τρόπος είναι να βρεθεί μια αναγωγή (πιθανώς εκθετικού χρόνου) που να διατηρεί την προσέγγιση από ένα πρόβλημα στη #P σε ένα πρόβλημα στην TotP έτσι ώστε το ποσό των μη ντετερμινιστικών δυαδικών ψηφίων που απαιτούνται για να λυθεί το πρώτο δεν αυξάνεται πάρα πολύ μέσω της αναγωγής.

Με άλλα λόγια εάν η f είναι στη #P με M_f να είναι η αντίστοιχη NPTM (της οποίας ο αριθμός των αποδεκτών διαδρομών υπολογισμού στην είσοδο x είναι $f(x)$), που χρησιμοποιεί n μη ντετερμινιστικά bits, και αν η g είναι στην TotP με M_g την αντίστοιχη NPTM (της οποίας ο συνολικός αριθμός διαδρομών υπολογισμού στην είσοδο x ισούται με $g(x) + 1$), που χρησιμοποιεί n' μη ντετερμινιστικά bits, τότε έχουμε το εξής.

Πόρισμα 6. Αν υπάρχει αναγωγή που διατηρεί στην προσέγγιση από ένα πρόβλημα $f \in \#P$ σε ένα πρόβλημα $g \in \text{TotP}$, έτσι ώστε $n' < (3 - \gamma)n/2$, για κάποιο $\gamma \in (0, 1)$, τότε για κάθε $x \in \{0, 1\}^n$, $\delta \in (0, 1)$, $k \in \mathbb{R}$, με πιθανότητα $1 - \delta$ και σε χρόνο $t = \text{poly}(k, |x|, \log \delta^{-1})(2^{(1-\gamma)n} + 2^{(1+\gamma)n/2})$, μπορούμε να επιτύχουμε προσέγγιση $\hat{f}(x) = f(x)(1 \pm \frac{1}{k})$. Η αναγωγή αρκεί να γίνεται σε χρόνο $O(t)$, και όχι αναγκαστικά σε πολυωνυμικό χρόνο.

Απόδειξη. Εφαρμόζουμε το πόρισμα [19] στη g με $\beta \geq 3 - \frac{n}{n'}(3 - \gamma)$. □

Παρατηρήστε ότι πήραμε σαν παράμετρο πολυπλοκότητας τα n, n' και όχι το μέγεθος της εισόδου, γιατί μας ενδιαφέρει η σύγκριση με τον αλγόριθμο εξαντλητικής αναζήτησης.

Ανοιχτά προβλήματα Παραμένει ανοιχτό ερώτημα το κατά πόσο τα παραπάνω αποτελέσματα είναι βέλτιστα ύπο μια fine grained complexity οπτική.

3.2 FPRAS vs. TotP

Ένα πολύ σημαντικό θεώρημα της παρούσας εργασίας, αν και εύκολο να αποδειχθεί (βλ. θεώρημα [5]), είναι ότι $\text{NP}=\text{RP}$ αν και μόνον αν όλα τα προβλήματα της TotP επιδέχονται FPRAS. Αυτό είναι σημαντικό διότι μεταφράζει το ερώτημα του αν $\text{NP}=\text{RP}$, (δλδ. το πρόβλημα του αν όλα τα προβλήματα στην NP θα μπορούσαν να λυθούν σε πολυωνυμικό χρόνο με τη χρήση τυχαιότητας), σε όρους μετρητικής πολυπλοκότητας και μάλιστα μετρητικών προβλημάτων με αντίστοιχο πρόβλημα απόφασης στο P. Περιττό είναι να αναφέρουμε ότι το NP vs. RP αποτελεί ένα από τα σημαντικότερα ανοιχτά προβλήματα της θεωρητικής πληροφορικής, με πολλές επιπτώσεις τόσο θεωρητικές (πχ. στην ψευδοτυχειότητα) όσο και πρακτικές (πχ. στην κρυπτογραφία και την ασφάλεια). Εκεί που θέλουμε να καταλήξουμε με όλα

αυτά είναι ότι η μελέτη της σχέσης της TotP με την κλάση προβλημάτων που επιδέχονται FPRAS, είναι ένα από τα σημαντικότερα προβλήματα μετρητικής πολυπλοκότητας, αφού είναι ισοδύναμο με το NP vs. RP.

Αυτή η ενότητα αφορά μια διαισθητική πεποίθηση πολλών επιστημόνων ότι τα μόνα προβλήματα στη #P που μπορεί να έχουν FPRAS ανήκουν στην TotP και αντιπαραδείγματα σε αυτή την εικασία δεν είναι γνωστά. Αποδεικνύουμε ότι αυτή η εικασία είναι λάθος εκτός εάν $P = RP$. Προκειμένου να το δείξουμε, εισάγουμε δύο νέες κλάσεις πολυπλοκότητας #RP1 και #RP2 με την βοήθεια των οποίων το αποτέλεσμα προκύπτει εύκολα. Δείχνουμε επίσης ότι η τάξη των προβλημάτων που επιδέχονται FPRAS βρίσκεται μεταξύ αυτών των δύο κλάσεων και ότι αυτές οι κλάσεις δεν συμπίπτουν εκτός αν $NP = RP$. Τέλος, για να αποκτήσουμε μια πιο ξεκάθαρη εικόνα των σχέσεων των παραπάνω κλάσεων με τη #P και την TotP (όπως και με μερικές άλλες σχετικές κλάσεις), μελετάμε τους εγκλεισμούς μεταξύ τους και παρουσιάζουμε τους τέσσερις δυνατούς κόσμους σε σχέση με τα (NP vs. RP) και (RP vs. P) σημαντικά ανοικτά ερωτήματα της θεωρίας πολυπλοκότητας.

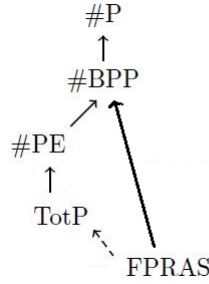
3.2.1 Εισαγωγή

Ένα ανοικτό ερώτημα στην μετρητική πολυπλοκότητα είναι να προσδιοριστούν τα προβλήματα τα οποία επιδέχονται ένα f.p.r.a.s, από άποψη δομικής πολυπλοκότητας. Σε αυτή την υποενότητα και μόνο, θα συμβολίζουμε με FPRAS την υποκλάση των προβλημάτων στη #P που επιδέχονται f.p.r.a.s.. Το ερώτημα που εξετάζεται από ορισμένους επιστήμονες είναι να αναγνωριστεί μια κλάση πολυπλοκότητας που συλλαμβάνει ακριβώς την FPRAS, σε όρους π.χ. καταμέτρησης μονοπατιών μηχανών Turing (path counting) [62, 11], συναρτήσεων μέτρησης μεγεθών διαστημάτων (interval size functions) [13], ή σε όρους περιγραφικής πολυπλοκότητας (descriptive complexity) [8].

Πολλοί επιστήμονες έχουν εκφράσει τη διαίσθηση ότι αφού τα μετρητικά προβλήματα που έχουν NP-πλήρη απόφαση ύπαρξης λύσης δεν είναι επιλύσιμα αποδοτικά εκτός αν $NP = RP$, αυτά που επιδέχονται FPRAS θα πρέπει να αναζητηθούν μεταξύ αυτών με εύκολη απόφαση ύπαρξης λύσης (π.χ. [9] κεφάλαιο 17, [34] κεφάλαιο 6.2). Ακόμη πιο συγκεκριμένα, αναζητώντας μια περιγραφική τάξη πολυπλοκότητας που συλλαμβάνει ακριβώς την FPRAS, εκφράζεται έμμεσα η πεποίθηση ότι η FPRAS είναι ένα υποσύνολο της TotP, κι ότι έτσι μπορεί κανείς να επικεντρωθεί στη μελέτη υποκλάσεων της TotP με κάποιες επιθυμητές ιδιότητες ώστε να είναι υποψήφιες να έχουν προσεγγίσιμα προβλήματα ([8], σελ. 7-8).

Φυσικά ήταν ήδη γνωστό ότι τα προβλήματα στην FPRAS έχουν απόφαση ύπαρξης λύσης στο BPP [8, 34], αλλά αυτό το γεγονός από μόνο του δεν μπορεί να αντικρούσει την προαναφερθείσα εικασία. Ο κόσμος πιστεύεται ότι είναι όπως στο σχήμα 1, όπου #BPP δηλώνει την τάξη των προβλημάτων στη #P με απόφαση ύπαρξης λύσης στην BPP.

Επιπλέον, δεν υπάρχουν αντιπαραδείγματα στην εικασία ότι η FPRAS είναι υποσύνολο της TotP, έτσι θα μπορούσε η εικασία να είναι στην πραγματικότητα θεώρημα.



Σχήμα 3.1: Η εικαζόμενη θέση της FPRAS. Τα βελάκια υποδηλώνουν εγκλεισμούς συνόλων (\subseteq).

Σε αυτή την εργασία εξετάζουμε αυτήν την ερώτηση και όπως αποδεικνύεται, αυτή η εικασία δεν ισχύει εκτός εάν $P = RP$.

Παρατηρούμε πρώτα ότι τα προβλήματα στην FPRAS έχουν το αντίστοιχο πρόβλημα απόφασης ύπαρξης λύσης στην RP. Αλλά ακόμα και αν αντικαταστήσουμε τη #BPP με την #RP (δηλαδή την κλάση του προβλήματος στο #P με απόφαση ύπαρξης λύσης στην RP), το σενάριο του σχήματος 1 είναι ακόμα δυνατό.

Ωστόσο, η RP έχει (τουλάχιστον) δύο διαφορετικούς ισοδύναμους ορισμούς. Έστω $acc_M(x)$ ο αριθμός των διαδρομών αποδοχής μιας NPTM M και έστω p_M ένα πολυώνυμο που φράσσει τον χρόνο εκτέλεσης της M .

Ορισμός 31. (αρχικός ορισμός της RP)

$L \in RP \Leftrightarrow$ υπάρχει πολυωνυμικού χρόνου πιθανοτικός αλγόριθμος A τέτοιος
αν $x \in RP$ τότε $\Pr[A(x) = 1] \geq \frac{1}{2}$
αν $x \notin RP$ τότε $\Pr[A(x) = 1] = 0$

Ορισμός 32. (ισοδύναμος ορισμός της RP)

$L \in RP \Leftrightarrow \exists$ NPTM M τέτοια ώστε
αν $x \in RP$ τότε $acc_M(x) > \frac{1}{2}2^{p_M(|x|)}$
αν $x \notin RP$ τότε $acc_M(x) = 0$.

Για κάθε έναν από τους παραπάνω ορισμούς, ορίζουμε δύο αντίστοιχες κλάσεις μέτρησης #RP2 (που αντιστοιχούν στον αρχικό ορισμό του RP) και #RP1 (που αντιστοιχεί στον ισοδύναμο ορισμό του RP).

Με τη βοήθεια του #RP1 αποδεικνύουμε ότι αν $P \neq RP$, τότε $FPRAS \not\subseteq TotP$, και στην πραγματικότητα $FPRAS \not\subseteq \#PE$. Επιπλέον, αποδεικνύουμε ότι η FPRAS βρίσκεται μεταξύ των #RP1 και #RP2.

Στη συνέχεια, δημιουργείται ένα νέο ερώτημα. Είναι πιθανό η #RP1 και η #RP2 να συμπίπτουν και συνεπώς η FPRAS να είναι ακριβώς η #RP2; Αποδεικνύουμε ότι αυτό δεν ισχύει εκτός αν $NP = RP$. Το γεγονός αυτό είναι κάπως εντυπωσιακό, καθώς οι αντίστοιχοι ορισμοί των κλάσεων απόφασης συμπίπτουν.

Τέλος, για να αποκτήσουμε μια πιο ξεκάθαρη εικόνα των σχέσεων μεταξύ των ήδη αναφερθεισών υποκλάσεων της #P, δηλαδή των #PE, TotP, #RP1, #RP2, εξετάζουμε περαιτέρω όλους τους εγκλεισμούς μεταξύ τους σε σχέση με τις ανοιχτές ερωτήσεις NP έναντι RP και RP έναντι P, και παρουσιάζουμε τους τέσσερις πιθανούς κόσμους.

3.2.2 Προαπαιτούμενα

Παραπέμπουμε στο κεφάλαιο της εισαγωγής για ορισμούς των TotP, #P, #PE, FP.

Υπενθυμίζουμε το εξής θεώρημα.

Θεώρημα 20. [62] (a) $FP \subseteq TotP \subseteq \#PE \subseteq \#P$. Οι εγκλεισμοί είναι γνήσιοι εκτός αν $P = NP$.

(b) Η TotP είναι το KarP closure των αυτοαναγώγιμων #PE συναρτήσεων.

Σε αυτή την ενότητα συμβολίζουμε με FPRAS την κλάση των συναρτήσεων στη #P που επιδέχονται f.p.r.a.s.

Υπενθυμίζουμε επίσης το εξής θεώρημα.

Θεώρημα 21. (a) Αν $NP \neq RP$ τότε υπάρχουν συναρτήσεις στην TotP που δεν είναι στην FPRAS.

(b) Αν $NP = RP$ τότε $\#P \subseteq FPRAS$.

Απόδειξη. Το #IS ανήκει στην TotP, και δεν επιδέχεται FPRAS εκτός αν $NP = RP$ [25]. Η δεύτερη πρόταση προκύπτει από ένα γνωστό θεώρημα του Stockmeyer, βλ. εισαγωγικό κεφάλαιο. \square

Τώρα εισάγουμε δύο κλάσεις, έχοντας απόφαση ύπαρξης λύσης στην RP. Για το λόγο αυτό, πρέπει να ορίσουμε το σύνολο \mathcal{MR} των Μηχανών Turing που σχετίζονται με προβλήματα στην RP.

Ορισμός 33. Έστω M μια NPTM, πλήρως δυαδική. Συμβολίζουμε p_M το πολυώνυμο για το οποίο με είσοδο μεγέθους n , η M κάνει $p_M(n)$ μη ντετερμινιστικές επιλογές.

$$\mathcal{MR} = \{NPTM M \mid \forall x \in \Sigma^* \text{ είτε } acc_M(x) = 0 \text{ ή } acc_M > \frac{1}{2}2^{p_M(|x|)}\}.$$

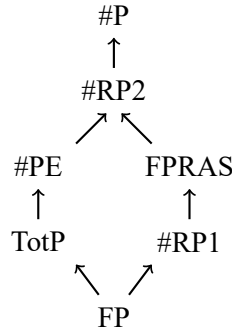
Ορισμός 34. $\#RP1 = \{f \in \#P \mid \exists M \in \mathcal{MR} \text{ έτσι ώστε } \forall x f(x) = acc_M(x)\}$.

Ορισμός 35. $\#RP2 = \{f \in \#P \mid L_f \in RP\}$.

Για τις αποδείξεις θα χρειαστούμε το λήμμα 3.

3.2.3 Αποτελέσματα

Παρουσιάζουμε πρώτα εγκλεισμούς χωρίς προϋποθέσεις μεταξύ των παραπάνω κλάσεων. Αυτοί οι εγκλεισμοί μαζί με αυτούς που είναι ήδη γνωστοί από το θεώρημα 20 μπορούν να συνοψιστούν στο ακόλουθο διάγραμμα.



Στη συνέχεια, διερευνάμε περισσότερους εγκλεισμούς μεταξύ αυτών των κλάσεων καταμέτρησης, σε σχέση με το NP vs. RP και το RP vs. P. Τα αποτελέσματα μπορούν να συνοψιστούν στα σχήματα του θεωρήματος 24.

Οι σημαντικότερες συνέπειες αυτής της έρευνας είναι ότι το FPRAS δεν περιλαμβάνεται στην TotP, εκτός εάν $RP = P$ και η #RP1 δεν ταυτίζεται με τη #RP2, εκτός αν $NP = RP$.

3.2.4 Αποδείξεις

Εγκλεισμοί χωρίς προϋποθέσεις

Θεώρημα 22. $FP \subseteq \#RP1 \subseteq \#RP2 \subseteq \#P$. Επίσης $\#PE \subseteq \#RP2$

Απόδειξη. Έστω $f \in FP$. Θα δείξουμε ότι $f \in \#RP1$. Θα κατασκευάσουμε μια NPTM $M \in \mathcal{MR}$ τέτοια ώστε με είσοδο x $acc_M(x) = f(x)$. Έστω $x \in \Sigma^*$. Η M υπολογίζει το $f(x)$. Μετά υπολογίζει ένα $i \in \mathbb{N}$ τέτοιο ώστε $f(x) \in (2^{i-1}, 2^i]$. Η M κάνει i μη ντετερμινιστικές επιλογές b_1, b_2, \dots, b_i . Κάθε τέτοιο $b \in \{0, 1\}^i$ καθορίζει ένα μονοπάτι, συγκεκριμένα το b αντιστοιχεί στο $(b+1)$ -οστό μονοπάτι (αφού 0^i είναι το πρώτο μονοπάτι). Η M επιστρέφει yes αν $b+1 \leq f(x)$, οπότε $acc_M = f(x)$. Αφού $f(x) > 2^{i-1}$, $M \in \mathcal{MR}$.

Ο άλλος εγκλεισμός είναι άμεσος από τους ορισμούς. □

Θεώρημα 23. $\#RP1 \subseteq FPRAS \subseteq \#RP2$.

Απόδειξη. Για τον πρώτο εγκλεισμό έστω $\epsilon > 0, \delta > 0$. Έστω $f \in \#RP1$. Υπάρχει μια $M_f \in \mathcal{MR}$ τέτοια ώστε $\forall x acc_{M_f}(x) = f(x)$. Έστω $q(|x|)$ το πλήθος των μη ντετερμινιστικών επιλογών της M_f . Έστω $p = \frac{f(x)}{2^{q(|x|)}}$. Μπορούμε να υπολογίσουμε μια εκτίμηση \hat{p} του p , επιλέγοντας $m = poly(\epsilon^{-1}, \log \delta^{-1})$ τυχαία μονοπάτια ομοιόμορφα και ανεξάρτητα. Τότε μπορούμε να υπολογίσουμε $f(\hat{x}) = \hat{p}2^{q(|x|)}$.

Αν $f(x) = 0$ τότε $f(\hat{x}) = 0$. Αν $f(x) \neq 0$, τότε $p > \frac{1}{2}$, οπότε από το unbiased estimator lemma 3, η $f(\hat{x})$ ικανοποιεί τον ορισμό του f.p.r.a.s.

Για τον δεύτερο εγκλεισμό, έστω $f \in FPRAS$, θα δείξουμε ότι το πρόβλημα απόφασης για την f , δλδ η απόφαση αν $f(x) = 0$, είναι στην RP. Με είσοδο x εκτελούμε το f.p.r.a.s. για την f με ως πούμε $\epsilon = \delta = \frac{1}{4}$. Επιστρέφουμε yes αν $f(\hat{x}) \geq \frac{1}{2}$.

Αν $f(x) = 0$ το f.p.r.a.s. επιστρέφει 0, οπότε επιστρέφουμε yes με πιθανότητα 0. Αν $f(x) \geq 1$, τότε $f(x) \geq \frac{1}{2}$ με πιθανότητα τουλάχιστον $1 - \delta$, οπότε επιστρέφουμε yes με την ίδια πιθανότητα. \square

Πόρισμα 7. Αν $FPRAS \subseteq TotP$ τότε $RP=P$.

Απόδειξη. Αν $FPRAS \subseteq TotP$, τότε $\#RP1 \subseteq TotP$, και τότε για κάθε $f \in \#RP1$ $L_f \in P$. Άρα αν $A \in RP$ τότε υπάρχει $f_A \in \#RP1$ που να έχει ως αντίστοιχο πρόβλημα απόφασης το A , κι έτσι $A = L_{f_A} \in P$. Οπότε $RP=P$. \square

Παρατηρήστε ότι η f_A δεν ταυτίζεται απαραίτητα με την #, διότι δεν μετράει λύσεις του προβλήματος απόφασης, αλλά μετράει πλήθος τυχαίων επιλογών που οδηγούν σε σωστή απόφαση ύπαρξη λύσης. Για να το κατανοήσει κανείς αυτό, πρέπει να κατανοήσει καλά τους διαφορετικούς ορισμούς της RP.

Πάμε τώρα στο επόμενο πόρισμα.

Πόρισμα 8. Αν $\#RP1 = \#RP2$ τότε $NP=RP$.

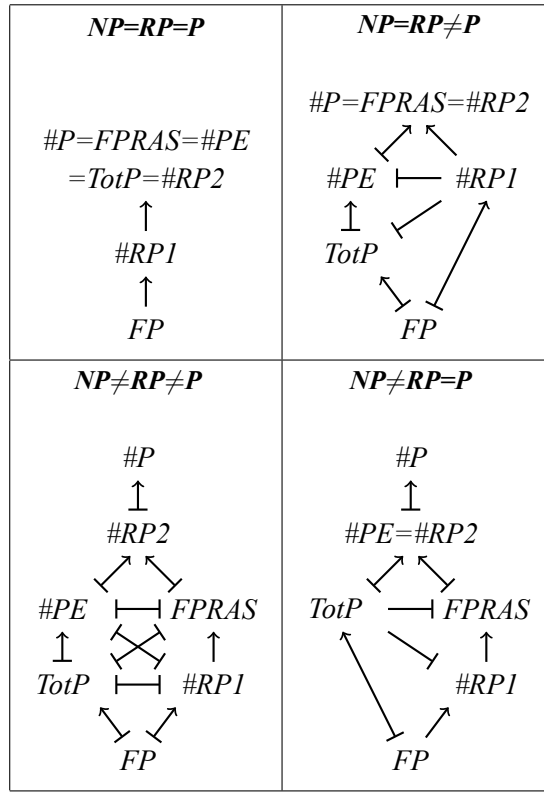
Απόδειξη. Αν $\#RP1 = \#RP2$ τότε και οι δύο είναι ίσες με την FPRAS, άρα $TotP \subseteq FPRAS$, οπότε $NP=RP$ από το θεώρημα [21](#). \square

Οι τέσσερις πιθανοί κόσμοι

Τώρα θα διερευνήσουμε περαιτέρω σχέσεις μεταξύ των προαναφερθέντων κλάσεων και θα παρουσιάσουμε και τους τέσσερις πιθανούς κόσμους μέσα στη #P, σε σχέση με το NP vs. RP vs. P.

Θεώρημα 24. Ισχύει η παρακάτω εικόνα.

Στα σχήματα, $A \rightarrow B$ σημαίνει $A \subseteq B$, $A \nrightarrow B$ σημαίνει $A \not\subseteq B$, και $A \leftrightarrow B$ σημαίνει $A \subseteq B$.



Απόδειξη. Καταρχάς οι τομές μεταξύ οποιονδήποτε από τις παραπάνω κλάσεις είναι μη κενές, αφού η FP είναι μια μη κενή υποκλάση όλων αυτών. Για τους υπόλοιπους εγκλεισμούς έχουμε τα εξής.

$$\#P \subseteq \#RP2 \Leftrightarrow NP=RP \text{ (εξ ορισμού).}$$

$$\#RP2 \subseteq \#PE \Leftrightarrow RP=P \text{ (εξ ορισμού).}$$

$\#P \subseteq TotP \Rightarrow NP=P$ (από το θεώρημα 20). Επίσης $NP=P \Rightarrow \#SAT \in TotP$, επειδή το $\#SAT$ είναι αυτοαναγώγιμο, και έτσι θα είχε εύκολη απόφαση ύπαρξης λύσης. Άρα $\#P \subseteq TotP$, επειδή η $TotP$ είναι το Karp-closure των αυτοαναγώγιμων προβλημάτων με εύκολη απόφαση ύπαρξης λύσης, και το $\#SAT$ είναι $\#P$ -complete υπό Karp αναγωγές. Οπότε παίρνουμε $\#P = \#PE = TotP \Leftrightarrow P=NP$.

$$TotP \subseteq FPRAS \Rightarrow NP=RP \text{ (από το θεώρημα 21).}$$

$$\#RP2 \subseteq FPRAS \Rightarrow TotP \subseteq FPRAS \Rightarrow NP=RP.$$

$$\#RP2=\#RP1 \Rightarrow NP=RP \text{ (από το πόρισμα 8).}$$

$$\#P \subseteq FPRAS \Leftrightarrow NP=RP \text{ (από το θεώρημα 21).}$$

$$\#PE \subseteq FPRAS \Rightarrow TotP \subseteq FPRAS \Rightarrow NP=RP.$$

$$\#PE \subseteq \#RP1 \Rightarrow \#PE \subseteq FPRAS \Rightarrow NP=RP.$$

$$\#RP1 \subseteq \#PE \Rightarrow RP=P \text{ (ίδια απόδειξη με το πόρισμα 7).}$$

$$FPRAS \subseteq \#PE \Rightarrow \#RP1 \subseteq \#PE \Rightarrow RP=P.$$

$$FPRAS \subseteq TotP \Rightarrow RP=P \text{ (πόρισμα 7).}$$

$$TotP \subseteq \#RP1 \Rightarrow TotP \subseteq FPRAS \Rightarrow NP=RP.$$

$$\#RP1 \subseteq TotP \Rightarrow RP=P \text{ (ίδια απόδειξη με το πόρισμα 7).}$$

$\#RP1 \subseteq FP \Rightarrow \#RP1 \subseteq TotP \Rightarrow RP=P.$

$TotP \subseteq FP \Rightarrow NP=P$ (από το θεώρημα 20). □

3.2.5 Συζήτηση και ανοιχτά προβλήματα

Όσον αφορά το ερώτημα αν $FPRAS \subseteq TotP$, το πόρισμα 7 σημαίνει ότι αφενός δεν ισχύει αυτός ο εγκλεισμός εκτός αν $P = RP$, και αφετέρου αν ισχύει, τότε είναι πιο δύσκολο να το αποδείξουμε, από ότι να αποδείξουμε $RP = P$.

Ο καθορισμός εάν $(RP = P \text{ συνεπάγεται } FPRAS \subseteq TotP)$, είναι μια ανοιχτή ερώτηση, ενδιαφέρουσα από μόνη της. Φαίνεται ότι είτε ισχύει είτε όχι, και οι δύο δυνατότητες είναι συμβατές με τους τέσσερις δυνατούς κόσμους. Επιπλέον αν ισχύει, τότε η ερώτηση $(FPRAS \subseteq TotP?)$ θα ήταν μια ισοδύναμη διατύπωση της ερώτησης $RP \text{ vs. } P$. Σημειώστε ότι ήδη γνωρίζουμε ότι η ερώτηση $(TotP \subseteq FPRAS?)$ είναι μια ισοδύναμη διατύπωση του $NP \text{ vs. } RP$.

Το πόρισμα 8 σημαίνει ότι παρόλο που η $\#RP1$ και η $\#RP2$ είναι φυσικές αντίστοιχες μετρητικές κλάσεις της RP , δεν μπορούν να είναι ίσες εκτός εάν $NP = RP$. Αυτό συμβαίνει επειδή όταν θεωρούμε τις συναρτήσεις στη $\#P$ ως συναρτήσεις που μετράνε τον αριθμό των λύσεων σε κάποιο πρόβλημα απόφασης, τότε στην πρώτη κλάση οι τυχαίες επιλογές που οδηγούν σε αποδοχή είναι σε 1-1 αντιστοιχία με τις λύσεις που θέλουμε να μετρήσουμε, ενώ στην δεύτερη κλάση, οι τυχαίες επιλογές και οι λύσεις δεν συμπίπτουν απαραίτητα.

Είναι ενδιαφέρον ότι όσον αφορά την απόφαση, οι δύο ανάλογοι ορισμοί της RP είναι ισοδύναμοι, δηλαδή για κάθε πρόβλημα στην RP , υπάρχει μια NPTM στο \mathcal{MR} που αποφασίζει το πρόβλημα και το αντίστροφο. Αλλά για τα αντίστοιχα προβλήματα καταμέτρησης, αυτό δεν μπορεί να ισχύει πια, εκτός αν $NP = RP$.

Όσον αφορά τη δυνατότητα χαρακτηρισμού της $FPRAS$ σε όρους καταμέτρησης μονοπατιών μηχανών Turing, το πόρισμα 8 συνεπάγεται έναν τέτοιο χαρακτηρισμό, εάν οι δύο κατηγορίες συμπίπτουν. Ωστόσο, σε αυτήν την περίπτωση, όπως είδαμε, η $FPRAS$ θα είναι επίσης ίση με τη $\#P$, ο οποίος φυσικά είναι ένας πολύ απλούστερος χαρακτηρισμός.

Από την άλλη πλευρά, χωρίς υποθέσεις, το θεώρημα 23 σημαίνει ότι ο χαρακτηρισμός της $FPRAS$ που ψάχνουμε, είναι κάτι ανάμεσα στους δύο ορισμούς των $\#RP1$ και $\#RP2$, μια χαλάρωση του πρώτου και ενός περιορισμού του δεύτερου. Ωστόσο, μπορεί τελικά να μην υπάρχει κοινός χαρακτηρισμός αυτού του είδους για την $FPRAS$.

Είναι ανοιχτό το ερώτημα εάν η $FPRAS$ βρίσκεται στη $\#RP1$. Φαίνεται ότι τόσο η αρνητική όσο και η θετική απάντηση είναι συμβατές με τους τέσσερις κόσμους. Αν η απάντηση είναι θετική, τότε η $\#RP1$ θα ήταν ένας ισοδύναμος χαρακτηρισμός της $FPRAS$.

3.2.6 Σχετικές εργασίες

Υπάρχει μια τεράστια βιβλιογραφία σχετικά με αλγόριθμους προσέγγισης και αποτελέσματα μη προσεγγισιμότητας για μεμονωμένα προβλήματα στη $\#P$, π.χ.

[76, 43, 46, 23, 79].

Αρκετές κατηγορίες προβλημάτων με εύκολη απόφαση ύπαρξης λύσης μελετώνται στο [47, 62, 61, 13, 39, 6]. Επίσης, μετρητικά προβλήματα στη #P μελετώνται από την άποψη της περιγραφικής πολυπλοκότητας στο [66, 19, 8, 27, 22].

Κλάσεις που μέχρι στιγμής αποδεικνύεται ότι επιδέχονται f.p.r.a.s. είναι οι #RΣ2, #Σ1 [66] και μερικές επεκτάσεις της #Σ1 [8]. Σημειώστε ότι όλες αυτές είναι υποκλάσεις της TotP.

3.2.7 Συμπεράσματα

Σε αυτή την ενότητα εκλεπτύναμε την εικόνα της μετρητικής πολυπλοκότητας μέσα στη #P, ιδιαίτερα όσον αφορά την κατά προσέγγιση μέτρηση.

Έχουμε εισάγει δύο υποκλάσεις της #P: #RP1 και #RP2, που και οι δύο μπορούν να θεωρηθούν ως μετρητικές εκδοχές της κλάσης απόφασης RP. Δείξαμε ότι η FPRAS βρίσκεται μεταξύ τους και ότι αυτές οι κλάσεις δεν συμπίπτουν εκτός αν $NP = RP$. Με τη βοήθεια αυτών των κλάσεων αποδείξαμε επίσης ότι η FPRAS δεν μπορεί να περιέχεται στην TotP, εκτός αν $RP = P$.

Τέλος, μελετήσαμε τις συνέπειες της πιθανοκρατικής πολυπλοκότητας απόφασης, δηλαδή RP vs. NP και RP vs. P, στις σχέσεις μεταξύ μερικών κλάσεων μέτρησης μέσα στη #P, οι οποίες έχουν απόφαση είτε στην P είτε στην RP.

Περαιτέρω έρευνα θα μπορούσε να είναι η μελέτη των σχέσεων μεταξύ των νέων εισαγόμενων τάξεων με άλλες γνωστές υποκατηγορίες της #P, όπως αναφέρεται στην σχετική ενότητα 4.6.

3.3 Τα δύσκολα στιγμιότυπα του Size-of-Subtree

Το πρόβλημα Size-of-Subtree είναι TotP-πλήρες υπό φειδωλές αναγωγές, όπως δείξαμε στο κεφάλαιο 2. Αυτό σημαίνει ότι είναι επίσης #P-πλήρες κάτω από Cook αναγωγές, που σημαίνει ότι (α) όλα τα προβλήματα στην #P ανάγονται σε αυτό, και (β) δεν μπορεί να υπολογιστεί ούτε ακριβώς, ούτε με ένα μικρό απόλυτο σφάλμα (σε πολυωνυμικό χρόνο), εκτός αν $NP = RP$. Επίσης συνεπάγεται ότι είναι #P-complete κάτω από αναγωγές που διατηρούν την προσέγγιση, πράγμα που σημαίνει ότι (α) η προσέγγιση κάθε προβλήματος στη #P με πολυωνυμικά μεγάλο πολλαπλασιαστικό σφάλμα ανάγεται στην προσέγγιση του Size-of-Subtree με πολυωνυμικά μεγάλο σφάλμα και (β) δεν μπορεί να προσεγγιστεί με πολυωνυμικά μεγάλο σφάλμα (σε πολυωνυμικό χρόνο), εκτός αν $NP = RP$.

Παρ' όλα αυτά δείξαμε στην πρώτη ενότητα αυτού του κεφαλαίου ότι τα μικρά στιγμιότυπα του προβλήματος μπορούν να υπολογιστούν με ακρίβεια και επίσης ότι τα μεγάλα στιγμιότυπα του προβλήματος μπορούν να προσεγγιστούν με μικρό πολλαπλασιαστικό σφάλμα σε πολυωνυμικό χρόνο. Υπάρχουν επίσης ορισμένα αποτελέσματα στη βιβλιογραφία που δείχνουν ότι αυτό το πρόβλημα μπορεί να προσεγγιστεί καλά για ειδικούς τύπους δέντρων, όπως για πολύ συμμετρικά δέντρα, και για κοντόχοντρα δένδρα [51], για μακρυνά και λεπτά δέντρα [63], για τυχαία

δένδρα [29, 75], και για δέντρα που προκύπτουν από συγκεκριμένες backtracking διαδικασίες (βλ. [15] και τις αναφορές αυτού). Έτσι, φαίνεται να είναι ένα πρακτικά εύκολο πρόβλημα.

Επειδή, όμως, όπως είπαμε, είναι επίσης TotP-πλήρες και η TotP περιλαμβάνει και δύσκολα μετρητικά προβλήματα, πράγμα που σημαίνει ότι στη χειρότερη περίπτωση είναι δύσκολο πρόβλημα, το ερώτημα που τίθεται είναι ποιά είναι τα δύσκολα στιγμιότυπα του προβλήματος Size-of-Subtree.

Σε αυτή την ενότητα δείχνουμε ότι τα δύσκολα στιγμιότυπα του προβλήματος είναι εκείνα που θα ονομάσουμε "χριστουγεννιάτικα δέντρα" (επειδή το σκίτσο τους μοιάζει με χριστουγεννιάτικο δέντρο): ένα τέτοιο δέντρο αποτελείται από ένα πλήρες δυαδικό δέντρο ύψους n_1 , από κάποιο φύλλο του οποίου κρέμεται άλλο ένα πλήρες δυαδικό δέντρο ύψους n_2 . Δείχνουμε ότι εάν μπορούμε να προσεγγίσουμε το μέγεθος ενός τέτοιου δέντρου, τότε μπορούμε να αποφασίσουμε το SAT με μεγάλη πιθανότητα. Με άλλα λόγια, το μέγεθός τους είναι μη προσεγγίσιμο εκτός εάν $NP = RP$.

3.3.1 Δέντρα με δύσκολα προσεγγίσιμο μέγεθος

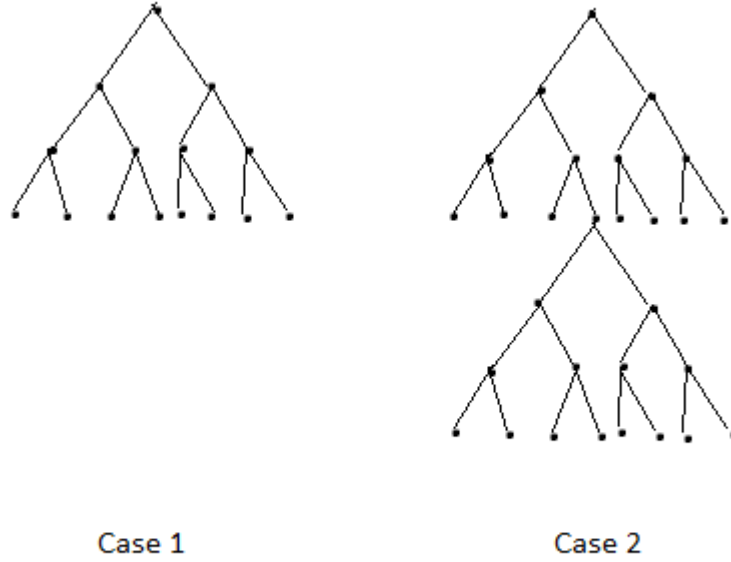
Ορισμός 36. Έστω $n_1, n_2, n \in \mathbb{N}$ τέτοια ώστε $n_1 + n_2 = n$. Ονομάζουμε " (n_1, n_2) -χριστουγεννιάτικο δέντρο" ένα δυαδικό δέντρο ύψους το πολύ n που αποτελείται από ένα τέλειο δυαδικό δέντρο ύψους n_1 , και με το πολύ ένα φύλλο από το οποίο κρέμεται άλλο ένα τέλειο δυαδικό δέντρο ύψους n_2 .

Για παράδειγμα το τέλειο δυαδικό δέντρο ύψους n_1 είναι ένα (n_1, n_2) -χριστουγεννιάτικο. Επίσης η παρακάτω εικόνα δείχνει άλλο ένα (n_1, n_2) -χριστουγεννιάτικο δέντρο, χρήσιμο για τις αποδείξεις μας.

Θεώρημα 25. Το πρόβλημα Size-of-Subtree περιορισμένο σε $(n/2, n/2)$ -χριστουγεννιάτικα δέντρα, είναι μη προσεγγίσιμο σε πολυωνυμικό χρόνο με πολυωνυμικό πολλαπλασιαστικό σφάλμα εκτός αν $NP=RP$.

Απόδειξη. Θα δείξουμε ότι τα 'χριστουγεννιάτικα' δέντρα είναι μη προσεγγίσιμα ανάγοντας το USAT σε αυτά. Το USAT είναι το SAT περιορισμένο σε φόρμουλες που έχουν το πολύ μία ικανοποιητική ανάθεση. Αντιστοιχούμε κάθε μη ικανοποιήσιμη φόρμουλα σε ένα χριστουγεννιάτικο δέντρο ύψους $n_1 = n/2$ (περίπτωση 1) και κάθε ικανοποιήσιμη φόρμουλα σε ένα χριστουγεννιάτικο δέντρο ύψους $n = n_1 + n_2 = n/2 + n/2$ (περίπτωση 2). Αν μπορούμε να προσεγγίσουμε το μέγεθος ενός οποιουδήποτε $(n/2, n/2)$ -χριστουγεννιάτικου δέντρου, τότε μπορούμε να διακρίνουμε μεταξύ των περιπτώσεων 1 και 2 και έτσι μπορούμε να διακρίνουμε μεταξύ ικανοποιήσιμων και μη ικανοποιήσιμων τύπων του USAT.

Στη συνέχεια, από το λήμμα των Valiant-Vazirani [78] που ανάγει το SAT στο USAT, παίρνουμε το συμπέρασμα. Διότι η αναγωγή είναι πιθανοτική, οπότε αν μπορεί κανείς να λύσει το USAT σε πολυωνυμικό χρόνο, τότε μπορεί επίσης σε πολυωνυμικό χρόνο να λύσει το SAT με μεγάλη πιθανότητα.



Σχήμα 3.2: Δύο $(n/2, n/2)$ -χριστουγεννιάτικα δέντρα.

Για περισσότερες λεπτομέρειες ως προς την αναγωγή, δείτε το αντίστοιχο αποτέλεσμα για τα χριστουγεννιάτικα δέντρα στο κεφάλαιο των αλλαγών φάσεων (βλ. απόδειξη του θεωρήματος 42). □

Κεφάλαιο 4

Μαρκοβιανές αλυσίδες για TotP-πλήρη προβλήματα

Όπως παρουσιάσαμε στο κεφάλαιο 2, δύο TotP-πλήρη προβλήματα κάτω από φειδωλές αναγωγές είναι το Size-of-Subtree και το #CM-SAT. Ένα σημαντικό θεώρημα που αποδείξαμε είναι ότι το #SAT ανάγεται στο #CM-SAT με αναγωγές που διατηρούν την προσέγγιση. Η δειγματοληψία και η κατά προσέγγιση μέτρηση συχνά εκτελούνται με τη χρήση μαρκοβιανών αλυσίδων. Ωστόσο, για το #SAT είναι γνωστό ότι δεν μπορούμε να σχεδιάσουμε μη αναγώγιμες μαρκοβιανές αλυσίδες, των οποίων ο χώρος καταστάσεων να είναι το σύνολο ικανοποιητικών αναθέσεων ενός τύπου που δίνεται ως είσοδος, εξαιτίας ενός φαινομένου διασκορπισμού του συνόλου των λύσεων. Αντίθετα, το σύνολο των λύσεων του #CM-SAT, καθώς και του Size-of-Subtree, συνδέεται με έναν συγκεκριμένο τρόπο που επιτρέπει το σχεδιασμό μη αναγώγιμων μαρκοβιανών αλυσίδων.

Στην παρούσα διατριβή σχεδιάζουμε και μελετούμε μερικές μαρκοβιανές αλυσίδες, των οποίων ο χώρος καταστάσεων είναι το σύνολο λύσεων των παραπάνω προβλημάτων. Αναλύουμε το χρόνο σύγκλισης, τις στάσιμες κατανομές τους και την πολυπλοκότητα του υπολογισμού των συντελεστών κανονικοποίησης και το μέγεθος του στηρίγματος των στάσιμων κατανομών. Τέλος, συζητάμε τα αποτελέσματα σε σχέση με την δυσκολία της καταμέτρησης στην TotP και με άλλα ανοιχτά προβλήματα στη θεωρία της πολυπλοκότητας.

Τα κύρια αποτελέσματα της μελέτης μας είναι καταρχάς ότι το SAT ανάγεται στον υπολογισμό του συντελεστή κανονικοποίησης της στάσιμης κατανομής μιας οικογένειας μαρκοβιανών αλυσίδων που σχεδιάζουμε. Με άλλα λόγια, ο ακριβής υπολογισμός αυτού του συντελεστή κανονικοποίησης είναι αδύνατος εκτός αν $NP=P$. Δεύτερον, αυτός ο συντελεστής κανονικοποίησης μπορεί να προσεγγιστεί με FPRAS (δηλ. με ένα αυθαίρετα μικρό πολλαπλασιαστικό σφάλμα).

□

¹Το περιεχόμενο αυτού του κεφαλαίου έχει δημοσιευτεί στο International Journal of Scientific and Engineering Research [10]

4.1 Εισαγωγή

Στο κεφάλαιο [2](#) εμφανίζονται τα πρώτα αποτελέσματα πληρότητας για την TotP, κάτω από φειδωλές αναγωγές, δηλ. αναγωγές που διατηρούν τον αριθμό των λύσεων. Τα πλήρη προβλήματα είναι αντιπροσωπευτικά μιας κλάσης, υπό την έννοια ότι όλα τα προβλήματα της κλάσης ανάγονται στα πλήρη, έτσι κάθε αλγοριθμικό αποτέλεσμα για ένα από τα πλήρη προβλήματα μεταφέρεται αυτόματα σε ολόκληρη την κλάση.

Δύο από αυτά τα προβλήματα είναι το Size-of-Subtree και το Clustered-Monotone-SAT (abr. #CM-SAT). Το πρώτο είναι το πρόβλημα του υπολογισμού του μεγέθους του δέντρου μιας backtracking διαδικασίας, χωρίς να το διασχίσουμε εξαντλητικά, ένα πρόβλημα που μελετήθηκε αρχικά από τον Knuth [\[51\]](#). Το #CM-SAT είναι το πρόβλημα του υπολογισμού του αριθμού των λύσεων ενός λογικού τύπου με τις εξής ιδιότητες: Υπάρχει ένα δέντρο πολυωνυμικού ύψους του οποίου οι κόμβοι αντιστοιχούν στις ικανοποιητικές αναθέσεις (ή λύσεις) αυτού του τύπου, έτσι ώστε για κάθε δεδομένη λύση είναι εύκολο να πάρουμε οποιαδήποτε λύση δίπλα σε αυτή κάνοντας μερικούς κατάλληλους μετασχηματισμούς σε πολυωνυμικό χρόνο. Επιπλέον, είναι εύκολο να βρεί κανείς την ικανοποιητική ανάθεση που αντιστοιχεί στη ρίζα αυτού του δέντρου σε πολυωνυμικό χρόνο.

Το #CM-SAT είναι ιδιαίτερα ενδιαφέρον επειδή αποδεικνύεται ότι το γενικό #SAT ανάγεται στο #CM-SAT με αναγωγή που διατηρεί την προσέγγιση. Αυτό σημαίνει ότι κάθε λογική φόρμουλα μπορεί να αναχθεί σε μια άλλη φόρμουλα με τις παραπάνω ιδιότητες έτσι ώστε να μπορέσουμε να προσεγγίσουμε τον αριθμό των λύσεων στην πρώτη αν και μόνο αν μπορούμε να προσεγγίσουμε τον αριθμό λύσεων στη δεύτερη.

Το γεγονός αυτό είναι σημαντικό λόγω του ακόλουθου φαινομένου που προέκυψε από τη μελέτη του random SAT. Για τους τύπους που θεωρούνται δύσκολοι, οι ικανοποιητικές αναθέσεις είναι ευρέως διάσπαρτες στο χώρο όλων των αναθέσεων [\[1, 4, 2\]](#). Οι λύσεις σχηματίζουν ομάδες, και αφενός είναι δύσκολο να βρεθεί έστω και μια λύση, αφετέρου ακόμη και αν δοθεί μια λύση σε κάποια ομάδα, είναι δύσκολο να βρεί κανείς μια άλλη σε διαφορετική ομάδα. Οι λύσεις δεν φαίνεται να σχετίζονται μεταξύ τους με κάποιον αλγοριθμικά κατανοητό τρόπο. Αυτή η σκέδαση εξηγεί τον λόγο της αποτυχίας πολλών αλγοριθμικών προσεγγίσεων για το #SAT, και ιδιαίτερα μεθόδων που βασίζονται στις μαρκοβιανές αλυσίδες. Προκειμένου να υπάρχει μια μοναδική στάσιμη κατανομή, είναι απαραίτητο μια μαρκοβιανή αλυσίδα να είναι μη αναγώγιμη, δηλ. πρέπει να μπορεί να μετακινηθεί από οποιαδήποτε κατάσταση σε οποιαδήποτε άλλη κάποια στιγμή. Αλλά όπως αναφέρθηκε προηγουμένως, δεν είναι γνωστό πώς να κατασκευάσουμε μια μαρκοβιανή αλυσίδα με έναν χώρο καταστάσεων που να αποτελείται από το σύνολο των λύσεων μιας φόρμουλας της οποίας είναι διάσπαρτο το σύνολο των λύσεων.

Αντίθετα, για την TotP-πλήρη εκδοχή του #SAT, δηλαδή το #CM-SAT, η κατάσταση είναι τελείως διαφορετική. Οι λύσεις μιας φόρμουλας εισόδου σχηματίζουν μια δομή γειτονιάς, πιο συγκεκριμένα ένα δέντρο πολυώνυμου ύψους, έτσι ώστε από οποιαδήποτε λύση να είναι εύκολο να κινηθεί κανείς γρήγορα προς τις γειτο-

νικές λύσεις.

Αυτό υποδηλώνει ότι η μελέτη των μαρκοβιανών αλυσίδων για το #CM-SAT καθώς και για άλλα TotP-πλήρη προβλήματα, που παρουσιάζουν την ίδια ιδιότητα συνδεσιμότητας των λύσεων, είναι μια φυσική κατεύθυνση έρευνας. Αυτή είναι η κατεύθυνση που ακολουθούμε σε αυτό το κεφάλαιο.

4.1.1 Πρώτες απόπειρες και αναδυόμενα ερωτήματα

Ένας απλός τυχαίος περίπατος σε ένα τέλειο δυαδικό δέντρο συγκλίνει σε πολυωνυμικό χρόνο σε σχέση με τον αριθμό των κόμβων του δέντρου. Ωστόσο, το δέντρο που εξετάζουμε είναι αυτό που αναφέρθηκε προηγουμένως, των οποίων οι κόμβοι είναι οι ικανοποιητικές αναθέσεις κάποιας φόρμουλας. Όπως είπαμε, για κάθε είσοδο στο #CM-SAT, το αντίστοιχο δέντρο έχει πολυωνυμικό ύψος σε σχέση με το μέγεθος της εισόδου, οπότε θεωρούμε όλους τους χρόνους εκτέλεσης σε σχέση με το ύψος του δέντρου. Έτσι το μέγεθος του τέλειου δυαδικού δέντρου είναι εκθετικό σε σχέση με το ύψος του και έτσι ο χρόνος σύγκλισης απλού τυχαίου περιπάτου είναι εκθετικός.

Ένας διαισθητικός λόγος που έχουμε αργή σύγκλιση του απλού τυχαίου περιπάτου στο τέλειο δυαδικό δέντρο είναι ότι από κάθε εσωτερικό κόμβο η πιθανότητα μετάβασης σε ένα επίπεδο κάτω είναι διπλάσιο από την πιθανότητα μετάβασης σε ένα επίπεδο επάνω, (δεδομένου ότι κάθε εσωτερικός κόμβος έχει δύο παιδιά, αλλά έναν γονέα).

Σκεφτήκαμε λοιπόν να σχεδιάσουμε μια μαρκοβιανή αλυσίδα όπου η πιθανότητα μετάβασης από κάθε εσωτερικό κόμβο σε ένα επίπεδο πάνω είναι ίση με την πιθανότητα μετάβασης σε ένα επίπεδο κάτω. Αν το n είναι το ύψος του δέντρου, μπορούμε να αποδείξουμε ότι ο χρόνος σύγκλισης αυτής της μαρκοβιανής αλυσίδας ισούται με το χρόνο σύγκλισης ενός απλού τυχαίου περιπάτου σε μια διαδρομή μήκους n , ο οποίος είναι γνωστό ότι είναι της τάξης του $O(n^2)$.

Στη συνέχεια γενικεύουμε αυτή την μαρκοβιανή αλυσίδα για κάθε δυαδικό δέντρο, όχι απαραίτητα πλήρες, και προκύπτουν ορισμένα ερωτήματα:

- Αυτή η μαρκοβιανή αλυσίδα σε ένα αυθαίρετο δυαδικό δέντρο συγκλίνει γρήγορα;
- Ποια είναι η στάσιμη κατανομή της γενικευμένης αλυσίδας σε ένα αυθαίρετο δέντρο;
- Μπορούμε να υπολογίσουμε τον συντελεστή κανονικοποίησης της στάσιμης κατανομής;
- Μπορούμε να υπολογίσουμε το μέγεθος του στηρίγματος της στάσιμης κατανομής; Σημειώστε ότι το μέγεθος του στηρίγματος ισούται με το μέγεθος του δέντρου και έτσι αντιστοιχεί ακριβώς στο πρόβλημα καταμέτρησης Size-of-Subtree.

- Μπορούμε να ανάγουμε το πρόβλημα καταμέτρησης στον υπολογισμό του συντελεστή κανονικοποίησης της στάσιμης κατανομής; Σημειώστε ότι για την ομοιόμορφη κατανομή ο συντελεστής κανονικοποίησης είναι απλά ένα πολλαπλάσιο του μεγέθους του στηρίγματος, αλλά όπως θα δούμε, αυτό δεν ισχύει για τις στάσιμες κατανομές των μαρκοβιανών αλυσίδων αυτού του κεφαλαίου.
- Μπορούμε να έχουμε ένα FPRAS για το πρόβλημα καταμέτρησης; (Ένα FPRAS είναι ένας αλγόριθμος πολυωνυμικής χρονικής προσέγγισης με ένα αυθαίρετα μικρό πολλαπλασιαστικό σφάλμα). Εάν όχι, ποιος είναι ο λόγος αυτής της δυσκολίας;

4.1.2 Κύρια αποτελέσματα και συζήτηση

Αρχικά αναλύουμε δύο μαρκοβιανές αλυσίδες στο τέλειο δυαδικό δέντρο: (α) τον απλό τυχαίο περίπατο και (β) μια μαρκοβιανή αλυσίδα που από κάθε εσωτερικό κόμβο η πιθανότητα να πάει στο γονέα είναι διπλάσια από την πιθανότητα να πάει σε κάθε παιδί. Αποδεικνύουμε ότι η δεύτερη μαρκοβιανή αλυσίδα συγκλίνει γρήγορα.

Στη συνέχεια γενικεύουμε τη δεύτερη μαρκοβιανή αλυσίδα σε ένα αυθαίρετο δυαδικό δέντρο. Ορίζουμε μια οικογένεια μαρκοβιανών αλυσίδων $(P_S)_S$, που έχουν ως καταστάσεις τους κόμβους ενός δυαδικού δέντρου S , ως εξής.

Έστω S ένα υποδέντρο του τέλειου δυαδικού δέντρου T ύψους n , που περιέχει τη ρίζα του T . Ορίζουμε την μαρκοβιανή αλυσίδα P_S στους κόμβους του S , με τις ακόλουθες πιθανότητες μετάβασης.

$$p_S(i, j) = 1/2 \text{ if } j \text{ is the parent of } i,$$

$$p_S(i, j) = 1/4 \text{ if } j \text{ is a child of } i,$$

$$p_S(i, j) = 0 \text{ for every other } j \neq i, \text{ and}$$

$$p_S(i, i) = 1 - \sum_{j \neq i} p_S(i, j).$$

Αποδεικνύουμε τα εξής.

- Για κάθε S η αντίστοιχη μαρκοβιανή αλυσίδα P_S συγκλίνει σε πολυωνυμικό χρόνο σε σχέση με το ύψος του δέντρου n . Σημειώστε ότι αυτό σημαίνει ότι ο χρόνος σύγκλισης είναι λογαριθμικός στο μέγεθος του δέντρου, όταν αυτό το μέγεθος είναι εκθετικά μεγάλο.
- Η στάσιμη κατανομή P_S είναι $\pi_S(u) = \alpha \cdot 2^{n-i}$, όπου i είναι το βάθος του κόμβου u και α είναι ο συντελεστής κανονικοποίησης της π_S , δηλαδή μια σταθερά τέτοια ώστε $\sum_{u \in V(S)} \pi_S(u) = 1$.
- Ο συντελεστής κανονικοποίησης μπορεί να προσεγγιστεί σε πολυωνυμικό χρόνο. Ο ακριβής υπολογισμός του συντελεστή κανονικοποίησης είναι δύσκολος.
- Ο υπολογισμός του μεγέθους του στηρίγματος μπορεί να αναχθεί στον υπολογισμό του συντελεστή κανονικοποίησης. Ωστόσο, ο ακριβής καθώς και ο

κατά προσέγγιση υπολογισμός του συντελεστή κανονικοποίησης είναι δύσκολος.

Τα τελευταία δύο αποτελέσματα φαίνονται αντιφατικά. Μπορούμε να προσεγγίσουμε τον συντελεστή κανονικοποίησης και μπορούμε να ανάγουμε τον υπολογισμό του μεγέθους του στηρίγματος στον υπολογισμό του συντελεστή κανονικοποίησης, αλλά δεν μπορούμε να προσεγγίσουμε το μέγεθος του στηρίγματος. Ο λόγος για τον οποίο αυτό συμβαίνει είναι ότι η αναγωγή περιλαμβάνει αφαίρεση και τέτοιες αναγωγές δεν διατηρούν τα πολλαπλασιαστικά σφάλματα. Επομένως, αν χρησιμοποιήσουμε την προσέγγιση του συντελεστή κανονικοποίησης για να προσεγγίσουμε το μέγεθος του στηρίγματος, το σφάλμα του τελευταίου μπορεί να είναι εκθετικά μεγάλο.

Μια παρατήρηση που προκύπτει από τα αποτελέσματά μας είναι η ακόλουθη. Σύμφωνα με το [69] αποδεικνύεται ότι για την ομοιόμορφη κατανομή πάνω από το σύνολο των λύσεων σε ένα πρόβλημα στη #P, η τυχαία δειγματοληψία, ο υπολογισμός του μεγέθους του στηρίγματος (δλδ το μετρητικό πρόβλημα), και ο υπολογισμός του συντελεστή κανονικοποίησης είναι υπολογιστικά ισοδύναμα. Όπως αποδεικνύεται, αυτό δεν ισχύει για τις κατανομές μας. Στην πραγματικότητα δείχνουμε ότι ένα FPRAS για τον συντελεστή κανονικοποίησης συνεπάγεται ένα FPRAS για το μετρητικό πρόβλημα αν και μόνο αν $NP = RP$.

Ένα τελικό συμπέρασμα που προκύπτει από τα αποτελέσματά μας είναι ένας νέος αλγόριθμος προσέγγισης με προσθετικό σφάλμα για οποιοδήποτε πρόβλημα στην TotP. Αυτός ο αλγόριθμος εκμεταλλεύεται τα ιδιαίτερα χαρακτηριστικά της TotP και έτσι ανοίγει νέες ερευνητικές κατευθύνσεις σχετικά με την αποτυχοποίηση αλγορίθμων. Σημειώστε ότι ένας προσεγγιστικός αλγόριθμος σφάλματος προσθετικού για προβλήματα στη #P είναι ήδη γνωστός ([34], κεφάλαιο 6.2.2), αλλά η αποτυχοποίησή του είναι μια μακρόχρονη ανοιχτή ερώτηση που απεδείχθη ότι είναι τόσο δύσκολη όσο η απόδειξη διαφόρων circuit lower bounds [81]. Δείτε την ενότητα 4.5 για περισσότερες λεπτομέρειες σχετικά με αυτό το ζήτημα.

4.2 Ο απλός τυχαίος περίπατος στο τέλειο δυαδικό δέντρο

Θεωρούμε τον απλό τυχαίο περίπατο W σε ένα πλήρες πλήρες δυαδικό δέντρο T ύψους n . Δηλαδή οι πιθανότητες μετάβασης είναι

$$\begin{aligned} r(i, j) &= 1/3 \text{ for all } i \neq j, \\ r(i, i) &= 1/3 \text{ for } i=\text{root}, \\ r(i, i) &= 2/3 \text{ for } i=\text{leaf}, \text{ and} \\ r(i, i) &= 0 \text{ in any other case.} \end{aligned}$$

Θεώρημα 26. *Ο απλός τυχαίος περίπατος W συγκλίνει στην ομοιόμορφη κατανομή $U(i) = \frac{1}{2^n - 1}$ για κάθε κόμβο i .*

Απόδειξη. Ελέγξτε ότι ισχύει για κάθε κόμβο j $\sum_i U(i)r(i, j) = U(j)$. □

Θεώρημα 27. *Ο χρόνος σύγκλισης του W είναι εκθετικός στο n .*

Απόδειξη. Έστω Y το σύνολο των κόμβων στο αριστερό υποδέντρο του T . $U(Y) = \frac{1}{2} - \frac{1}{2^n - 1}$. Υπάρχει μόνο μία ακμή $e = (i, j)$ που βγαίνει από το Y : i είναι το αριστερό παιδί της ρίζας, και j είναι η ρίζα. Η ακμή e έχει βάρος $w_e = r_{ij} U_i = \frac{1}{3} \frac{1}{2^n - 1}$. Οπότε $\Phi(Y) \leq \frac{2}{3(2^n - 3)}$, κι έτσι από το λήμμα 2 έχουμε $\tau_{mix} \geq \frac{3(2^n - 3)}{8}$. \square

4.3 Μια ταχέως συγκλίνουσα μαρκοβιανή αλυσίδα στο τέλει δυαδικό δέντρο

Θεωρήστε μια μαρκοβιανή αλυσίδα Q στο τέλει δυαδικό δέντρο T ύψους n , με πιθανότητες μετάβασης

$$\begin{aligned} q(i, j) &= 1/2 \text{ if } j \text{ is the parent of } i, \\ q(i, j) &= 1/4 \text{ if } j \text{ is a child of } i, \\ q(i, j) &= 0 \text{ for every other } j \neq i, \text{ and} \\ q(i, i) &= 1 - \sum_{j \neq i} p_S(i, j). \end{aligned}$$

Θεώρημα 28. Η στάσιμη κατανομή της Q είναι $\pi_Q(v) = 2^{-\text{depth}(v)}(n+1)^{-1}$ για κάθε v .

Απόδειξη. Για κάθε j ισχύει $\sum_i \pi_Q(i)q(i, j) = \pi_Q(j)$. \square

Θεώρημα 29. Ο χρόνος σύγκλισης της Q ξεκινώντας από τη ρίζα, είναι πολυωνυμικός στο n , άρα λογαριθμικός στο μέγεθος του T .

Απόδειξη. Έστω $\{L_t\}_{t \geq 0}$ μια μαρκοβιανή αλυσίδα σε ένα μονοπάτι με $n+1$ κόμβους, που ορίζεται ως εξής $L_t = \text{depth}(Q_t)$, όπου $\text{depth}(v)$ συμβολίζει το βάθος του κόμβου v στο T . Οι πιθανότητες μετάβασης της L είναι

$$l(i, j) = \Pr[L_t = j | L_{t-1} = i] = \Pr[\text{depth}(Q_t) = j | \text{depth}(Q_{t-1}) = i]$$

οπότε

$$\begin{aligned} l(i, j) &= 1/2 \text{ για κάθε } i \neq j \\ l(0, 0) &= l(n, n) = 1/2. \end{aligned}$$

Οπότε η L είναι ένας απλός τυχαίος περίπατος στο μονοπάτι μήκους $n+1$. Η στάσιμη της κατανομή είναι η ομοιόμορφη στους κόμβους του μονοπατιού και ο χρόνος σύγκλισης είναι πολυωνυμικός στο n . Το τελευταίο είναι γνωστό, αλλά για λόγους πληρότητας του κεφαλαίου δίνουμε μια σύντομη απόδειξη:

Καταρχάς θεωρούμε την τεμπέλικη εκδοχή της αλυσίδας, δηλ με πιθανότητα $1/2$ δεν κάνουμε τίποτα, και με πιθανότητα $1/2$ ακολουθούμε τους κανόνες της L . Η αγωγιμότητα $\Phi(Y)$ ελαχιστοποιείται για $Y_1 = \{0, 1, \dots, \lfloor \frac{n+1}{2} \rfloor\}$, $w_{\frac{n+1}{2}, \frac{n+1}{2}+1} = \frac{1}{2(n+1)}$, οπότε $\Phi(Y_1) \geq \frac{1}{n+1}$. Οπότε από το λήμμα 3 για $\epsilon = \frac{1}{4}$ συμπεραίνουμε ότι ο χρόνος σύγκλισης, ξεκινώντας από οποιονδήποτε αρχικό κόμβο x , είναι $O(n^2 \log n)$.

Επιστρέφουμε στην απόδειξη του θεωρήματος. Όταν το L έχει συγκλίνει στην στάσιμη κατανομή του, το Q έχει συγκλίνει σε μια κατανομή που είναι ομοιόμορφη

στα επίπεδα του T . Για να ολοκληρώσουμε την απόδειξη παρατηρούμε ότι οι συμμετρικές του τέλειου δυαδικού δέντρου συνεπάγονται ότι όταν ξεκινάμε από τη ρίζα, για κάθε βήμα t , η κατανομή του Q_t εξαρτάται μόνο από το βάθος των κόμβων, δηλαδή η πιθανότητα $\Pr[Q_t = v]$ είναι ίδια για όλα τα v που βρίσκονται στο ίδιο βάθος. Το τελευταίο μπορεί επίσης να αποδειχθεί με επαγωγή στο t .

Έτσι, τη στιγμή που το L έχει συγκλίνει στην ομοιόμορφη κατανομή, το Q έχει συγκλίνει στην π_Q . \square

4.4 Μια γενίκευση για αυθαίρετο δυαδικό δέντρο

Γενικεύουμε την μαρκοβιανή αλυσίδα της προηγούμενης ενότητας σε ένα αυθαίρετο δυαδικό δένδρο, όχι απαραίτητα πλήρες. Ο χώρος καταστάσεων αποτελείται από τους κόμβους ενός δένδρου ύψους n , και οι πιθανότητες μετάβασης είναι όπως στην προηγούμενη ενότητα.

Ορισμός 37. Έστω S ένα υποδέντρο που τέλειου δυαδικού δέντρου T ύψους n , που περιέχει τη ρίζα του T . Ορίζουμε τη μαρκοβιανή αλυσίδα P_S στους κόμβους του S , με τις ακόλουθες πιθανότητες μετάβασης.

$$p_S(i, j) = 1/2 \text{ if } j \text{ is the parent of } i,$$

$$p_S(i, j) = 1/4 \text{ if } j \text{ is a child of } i,$$

$$p_S(i, j) = 0 \text{ for every other } j \neq i, \text{ and}$$

$$p_S(i, i) = 1 - \sum_{j \neq i} p_S(i, j).$$

4.4.1 Στάσιμη κατανομή και χρόνος σύγκλισης

Θεωρήστε την ακόλουθη οικογένεια κατανομών $(\pi_S)_S$.

Ορισμός 38. Έστω S ένα δυαδικό δέντρο ύψους n και έστω $V(S)$ το σύνολο των κόμβων του S . Για κάθε $u \in V(S)$ $\pi_S(u) = \alpha_S \cdot 2^{n-i}$, όπου i είναι το βάθος του κόβου u και α_S είναι ο συντελεστής κανονικοποίησης της π_S , δηλ. μια σταθερά τέτοια ώστε $\sum_{u \in V(S)} \pi_S(u) = 1$.

Θεώρημα 30. Η στάσιμη κατανομή της P_S είναι η π_S όπως στον ορισμό [38](#).

Απόδειξη. Ισχύει $\sum_i \pi_S(i) p_S(i, j) = \pi_S(j)$. \square

Σημείωση Για απλοποίηση των συμβολισμών θα θεωρούμε το S φιξαρισμένο, και θα το παραλείπουμε από τους δείκτες στα $P_S, p_S, \pi_S, \alpha_S$, εκτός από όταν αναφερόμαστε σε περισσότερα από ένα δέντρα στην ίδια απόδειξη.

Τώρα θα δείξουμε ότι η P συγκλίνει γρήγορα, δηλ σε πολυωνυμικό χρόνο ως προς το ύψος του δέντρου S .

Το επόμενο λήμμα αποδεικνύει δύο ιδιότητες των μαρκοβιανών αλυσίδων που ορίσαμε, οι οποίες απαιτούνται για τις αποδείξεις που θα ακολουθήσουν.

Λήμμα 4. Έστω R ένα δυαδικό δέντρο ύψους n , και έστω α_R ο συντελεστής κανονικοποίησης της στάσιμης κατανομής π_R της παραπάνω μαρκοβιανής αλυσίδας (def. [37](#), [38](#)). Ισχύει $\alpha_R^{-1} \leq (n+1)2^n$, και $\pi_R(\text{root}) \geq \frac{1}{n+1}$

Απόδειξη. Έστω r_i το πλήθος των κόμβων σε βάθος i .

$$\begin{aligned} 1 &= \sum_{u \in S} \pi_R(u) = \sum_{i=0}^n \sum_{u \text{ in level } i} \pi_R(u) = \sum_{i=0}^n r_i \alpha_R \cdot 2^{n-i} \\ &\Rightarrow \frac{1}{\alpha_R} = \sum_{i=0}^n r_i \cdot 2^{n-i} \end{aligned}$$

το οποίο μεγιστοποιείται όταν τα r_i μεγιστοποιούνται, δηλ όταν το δέντρο είναι τέλει δυαδικό (ας το συμβολίσουμε T), στην οποία περίπτωση $r_i = 2^i$ και $\alpha_T^{-1} = (n+1)2^n$. Αυτό επίσης συνεπάγεται ότι για τη ρίζα του R ισχύει $\pi_R(\text{root}) = \alpha_R \cdot 2^n \geq \frac{1}{n+1}$. \square

Πρόταση 3. Ο χρόνος σύγκλισης της P , όταν ξεκινάμε από τη ρίζα, είναι πολυωνυμικός στο ύψος του δέντρου n .

Απόδειξη. Πρώτα απ' όλα, θα εξετάσουμε την τεμπέλικη έκδοση της μαρκοβιανής αλυσίδας, δηλαδή σε κάθε βήμα, με πιθανότητα $1/2$ δεν κάνουμε τίποτα και με πιθανότητα $1/2$ ακολουθούμε τους κανόνες όπως στον ορισμό [37](#). Ο χρόνος σύγκλισης της P περιορίζεται από το χρόνο σύγκλισης της τεμπέλικης έκδοσης του. Η στάσιμη κατανομή είναι η ίδια. Η μαρκοβιανή αλυσίδα είναι αναστρέψιμη στο χρόνο και το υποκείμενο γράφημα είναι ένα δέντρο με βάρη ακμών $w_{uv} = \pi_u p_{uv} = 2^i \alpha \times \frac{1}{8} = 2^{i-3} \alpha$, όπου u είναι ο γονέας του v και $2^i \alpha$ είναι η πιθανότητα π_u .

Η ποσότητα $\pi^{-1}(\text{root})$ είναι $O(n)$, όπως δείξαμε στη λήμμα [4](#).

Τώρα αρκεί να δείξουμε ότι το $1/\Phi(H)$ είναι πολυωνυμικό στο n .

Έστω \mathcal{X} το σύνολο των κόμβων του S , δηλ. ο χώρος καταστάσεων της μαρκοβιανής αλυσίδας P . Θα θεωρήσουμε όλα τα δυνατά $Y \subseteq \mathcal{X}$ with $0 \leq \pi(Y) \leq 1/2$.

Θα φράξουμε την ποσότητα $\frac{\sum_{i \in Y, j \notin Y} w_{ij}}{\sum_{i \in Y} \pi_i}$.

Αν το Y είναι συνδεδεμένο και δεν περιέχει τη ρίζα του S , τότε είναι ένα υποδέντρο του S , με ρίζα ας πούμε u , και $\pi_u = \alpha 2^k$ για κάποιο $k \in \mathbb{N}$. Έχουμε

$$\sum_{i \in Y, j \notin Y} w_{ij} \geq w_{u, \text{father}(u)} = 2^{k-2} \alpha.$$

Τώρα έστω Y' το τέλει δυαδικό δέντρο με ρίζα u και ύψος το ίδιο με το Y , δηλαδή k . Έχουμε

$$\begin{aligned} \sum_{i \in Y} \pi_i &\leq \sum_{i \in Y'} \pi_i = \sum_{j=0}^k 2^{k-j} \alpha \times 2^j = \\ &2^k (k+1) \alpha \leq 2^k (n+1) \alpha \end{aligned}$$

όπου αυτό προκύπτει αν αθροίσουμε πάνω στα επίπεδα του δέντρου Y' . Οπότε ισχύει

$$\frac{\sum w_{ij}}{\sum \pi_i} \geq \frac{2^{k-2} \alpha}{2^k (n+1) \alpha} = \frac{1}{4(n+1)}.$$

Αν Y είναι η ένωση δύο υποδέντρων του S , που δεν περιέχουν τη ρίζα του S , και η ρίζα του πρώτου είναι πρόγονος της ρίζας του δεύτερου, τότε τα ίδια επιχειρήματα ισχύουν, όπου τώρα παίρνουμε ως u τη ρίζα του πρώτου υποδέντρου.

Αν το Y είναι η ένωση από λ υποδέντρα που δεν περιέχουν την ρίζα του S , και για τα οποία ισχύει ότι κανενός η ρίζα δεν είναι πρόγονος της ρίζας κάποιου άλλου, τότε αποδεικνύουμε παρόμοιο φράγμα ως εξής. Έστω Y_1, \dots, Y_λ τα υποδέντρα, και έστω $k_1, k_2, \dots, k_\lambda$, οι αντίστοιχοι εκθέτες στις πιθανότητες των ριζών αυτών, στη στάσιμη κατανομή. Τότε όπως πριν

$$\sum w_{ij} \geq 2^{k_1-2}\alpha + 2^{k_2-2}\alpha + \dots + 2^{k_\lambda-2}\alpha$$

και

$$\sum_{i \in Y} \pi_i = \sum_{j=1 \dots \lambda} \sum_{i \in Y_j} \pi_i \leq \sum_{j=1 \dots \lambda} 2^{k_j}(n+1)\alpha$$

οπότε

$$\frac{\sum w_{ij}}{\sum \pi_i} \geq \frac{\alpha \sum_{j=1 \dots \lambda} 2^{k_j-2}}{(n+1)\alpha \sum_{j=1 \dots \lambda} 2^{k_j}} = \frac{1}{4(n+1)}.$$

Αν το Y είναι ένα υποδέντρο του S που περιλαμβάνει τη ρίζα του S , τότε το συμπλήρωμα του Y , δηλαδή το $S \setminus Y$ είναι η ένωση από λ υποδέντρα της προηγούμενης μορφής. Οπότε αν θέσουμε τα Y_i, k_i όπως πριν, τότε

$$\sum w_{ij} = \alpha \sum_{j=1 \dots \lambda} 2^{k_j-2}$$

και αφού από την υπόθεση $\pi(Y) \leq 1/2$, έχουμε

$$\sum_{i \in Y} \pi_i \leq \sum_{i \in S \setminus Y} \pi_i \leq (n+1)\alpha \sum_{j=1 \dots \lambda} 2^{k_j}$$

άρα το ίδιο φράγμα ισχύει ξανά.

Τέλος, παρόμοια επιχειρήματα συνεπάγονται το ίδιο φράγμα όταν το Y είναι αυθαίρετο υποσύνολο του S δλδ μια αυθαίρετη ένωση υποδέντρων του S .

Συνολικά έχουμε $1/\Phi(H) \leq 4(n+1)$. \square

Σημειώστε ότι αυτό το αποτέλεσμα συνεπάγεται χρόνο σύγκλισης $O(n^2 \log n)$. Αυτό συμφωνεί με το θεώρημα στην προηγούμενη ενότητα, που λέει ότι στο πλήρες δυαδικό δέντρο ο χρόνος σύγκλισης θα πρέπει να είναι όσο ο χρόνος σύγκλισης ενός απλού τυχαίου περιπάτου πάνω στα επίπεδα του δέντρου, δηλαδή πάνω σε ένα μονοπάτι μήκους n .

4.4.2 Η πολυπλοκότητα υπολογισμού του συντελεστή κανονικοποίησης

Θα αναλύσουμε την πολυπλοκότητα ακριβούς και προσεγγιστικού υπολογισμού του συντελεστή κανονικοποίησης για την οικογένεια κατανομών $(\pi_S)_S$ (def [38](#)).

Πρέπει να διευκρινήσουμε σε αυτό το σημείο ότι το FPRAS που παρουσιάζουμε προϋποθέτει ότι γνωρίζουμε το ύψος του δέντρου n . Στο κεφάλαιο 2 δείξαμε ότι το Size-of-Subtree είναι TotP-πλήρες όταν δεν γνωρίζουμε το ύψος εκ των προτέρων, παρά μόνο ένα άνω φράγμα αυτού του ύψους. Εάν θεωρήσουμε την παραλλαγή του προβλήματος όπου γνωρίζουμε το ύψος του δέντρου, τότε το Size-of-Subtree δεν είναι απαραίτητα TotP-πλήρες υπό φειδωλές αναγωγές, όμως είναι πλήρες υπό αναγωγές που διατηρούν την προσέγγιση. Αυτό μπορεί κανείς να το δει αν πραγματοποιήσει την αναγωγή στο Size-of-Subtree όχι ξεκινώντας από μια οποιαδήποτε συνάρτηση στην TotP, αλλά ξεκινώντας από το #IS. Για το #IS εάν οι διακλάδώσεις της NPTM αντιστοιχούν στην μη ντετερμινιστική επιλογή "παίρνω ή δεν παίρνω" κάποιον κόμβο στο ανεξάρτητο σύνολο, τότε το υπολογιστικό δέντρο ξέρουμε ότι έχει ύψος n όσο και το πλήθος των κόμβων του δοσμένου γραφήματος ως είσοδος στο #IS. Εφόσον λοιπόν το #IS είναι #P-πλήρες (άρα και TotP-πλήρες αφού ανήκει στην TotP), υπό αναγωγές που διατηρούν την προσέγγιση, προκύπτει ότι ισχύει το ίδιο και για το Size-of-Subtree γνωρίζοντας το ύψος του δέντρου.

Όμως εάν δεν γνωρίζουμε το ύψος εκ των προτέρων, η Μαρκοβιανή αλυσίδα δεν μπορεί να το ανακαλύψει σε πολυωνυμικό χρόνο. Μάλιστα αποδεικνύεται ότι δεν γίνεται να ανακαλύψουμε το ύψος του δέντρου εκτός αν $NP=RP$, και επιπλέον το πρόβλημα υπολογισμού του συντελεστή κανονικοποίησης α_S είναι στη χειρότερη περίπτωση αδύνατο να προσεγγιστεί εκτός αν $NP=RP$. Κάποιες από τις χειρότερες περιπτώσεις για το α_S , είναι τα "χριστουγεννιάτικα δέντρα". Αποδείξεις των παραπάνω ισχυρισμών για τις περιπτώσεις που το n δεν είναι γνωστό, δίνονται σε γενικότερη μορφή στο επόμενο κεφάλαιο με τις αλλαγές φάσης.

Θεώρημα 31. *Ο υπολογισμός του συντελεστή κανονικοποίησης α_S για κάθε κατανομή π_S στην οικογένεια του ορισμού [38](#)*

1. είναι TotP-hard κάτω από Turing αναγωγές αν δεν γνωρίζουμε το ύψος του S ,
2. επιδέχεται FPRAS αν γνωρίζουμε το ύψος του S ,
3. ο ακριβής του υπολογισμός είναι αδύνατος ντετερμινιστικά (ή αντίστοιχα πιθανοτικά) αν $NP \neq P$ (αντίστοιχα $NP \neq RP$), είτε γνωρίζουμε το ύψος του S είτε όχι.

Απόδειξη. 1. Θα ανάγουμε τον υπολογισμό του μεγέθους του S στον υπολογισμό των συντελεστών κανονικοποίησης των παραπάνω κατανομών πιθανοτήτων $(\pi_S)_S$. Η αναγωγή είναι κατά Turing (δηλαδή το πιο γενικό είδος αναγωγών, αντίθετα με άλλα είδη αναγωγών που έχουν επιπλέον ιδιότητες, όπως είναι οι φειδωλές). Δεδομένου ότι το μέγεθος του στηρίγματος είναι TotP-πλήρες κάτω από parsimonious αναγωγές (αν δεν γνωρίζουμε το ύψος του S), καταλήγουμε στο συμπέρασμα ότι ο υπολογισμός του συντελεστή κανονικοποίησης είναι TotP-πλήρης υπό αναγωγές Turing. Απομένει να δείξουμε την ακόλουθη πρόταση.

Πρόταση 4. *Εστω S ένα δυαδικό δέντρο ύψους n , και $\forall i = 0 \dots n$, έστω S_i το υποδέντρο του S που περιέχει όλους τους κόμβους μέχρι και βάθος i ,*

και έστω α_{S_i} οι αντίστοιχοι συντελεστές κανονικοποίησης όπως ορίσαμε ήδη προωτέρα. Τότε

$$|S| = \frac{1}{\alpha_{S_n}} - \sum_{k=0}^{n-1} \frac{1}{\alpha_{S_k}}$$

Απόδειξη. Για $i = 1, \dots, n$ έστω r_i το πλήθος κόμβων σε βάθος i . Οπότε $|S| = r_0 + \dots + r_n$.

Προφανώς αν το S δεν είναι κενό,

$$r_0 = 1 = \frac{1}{\alpha_{S_0}}. \quad (4.1)$$

Θα δείξουμε ότι $\forall k = 1 \dots n$

$$r_k = \frac{1}{\alpha_{S_k}} - 2 \frac{1}{\alpha_{S_{k-1}}}, \quad (4.2)$$

οπότε τότε $|S| = \frac{1}{\alpha_{S_0}} + \sum_{k=1}^n \left(\frac{1}{\alpha_{S_k}} - 2 \frac{1}{\alpha_{S_{k-1}}} \right) = \frac{1}{\alpha_{S_n}} - \sum_{k=0}^{n-1} \frac{1}{\alpha_{S_k}}$.

Θα αποδείξουμε τον ισχυρισμό (4.2) με επαγωγή.

Για $k = 1$ έχουμε

$$\sum_{u \in S_1} \pi_{S_1}(u) = 1 \Rightarrow \alpha_{S_1} \cdot r_1 + 2\alpha_{S_1} \cdot r_0 = 1 \Rightarrow$$

$$r_1 = \frac{1}{\alpha_{S_1}} - 2r_0 = \frac{1}{\alpha_{S_1}} - 2 \frac{1}{\alpha_{S_0}}.$$

Υποθέτουμε ότι ο ισχυρισμός (4.2) ισχύει για $k < i \leq n$. Θα δείξουμε ότι ισχύει για $k = i$.

$$\sum_{u \in S_i} \pi_{S_i}(u) = 1 \Rightarrow \sum_{k=0}^i 2^{i-k} \alpha_{S_i} \cdot r_k = 1 \Rightarrow$$

$$r_i = \frac{1}{\alpha_{S_i}} - \sum_{k=0}^{i-1} 2^{i-k} r_k$$

και αντικαθιστώντας τα r_k για $k = 0, \dots, i-1$ από την (4.1) και την (4.2), παίρνουμε

$$r_i = \frac{1}{\alpha_{S_i}} - 2 \frac{1}{\alpha_{S_{i-1}}}.$$

Τέλος, εάν το ύψος του δέντρου είναι n , αλλά εμείς γνωρίζουμε μόνο ένα άνω φράγμα του $n' \geq n$, τότε αρκεί να παρατηρήσουμε ότι μέχρι και βάθος

n ισχύει ο τύπος 4.2, ενώ για κάθε $i > n$ ισχύει $\alpha_{S_i} = \alpha_S$ και $r_i = 0$, πράγμα που δεν ισχύει για κανένα $i < n$. Έτσι αν μπορώ να υπολογίσω τα α_{S_k} για κάθε k , βρίσκω το n βλέποντας για ποιά i ισχύει για πρώτη φορά $\alpha_{S_i} = \alpha_{S_{i+1}}$, κι εφαρμόζω τον τύπο $|S| = \frac{1}{\alpha_{S_n}} - \sum_{k=0}^{n-1} \frac{1}{\alpha_{S_k}}$ για αυτό το n . \square

2. Τώρα θα δώσουμε ένα FPRAS για τον υπολογισμό του συντελεστή κανονικοποίησης α_S , όταν γνωρίζουμε το ύψος n του S , χρησιμοποιώντας την ήδη ορισμένη μαρκοβιανή αλυσίδα P_S .

Πρόταση 5. Για κάθε δυαδικό δέντρο R ύψους n μπορούμε να εκτιμήσουμε το α_R , με σφάλμα $(1 \pm \zeta)$ για κάθε $\zeta > 0$, με πιθανότητα $1 - \delta$ για κάθε $\delta > 0$, σε χρόνο $\text{poly}(n, \zeta^{-1}, \log \delta^{-1})$.

Απόδειξη. Έστω R ένα δυαδικό δέντρο ύψους n . Μπορούμε να εκτιμήσουμε το α_R ως εξής.

Όπως είδαμε, $\pi_R(\text{root}) = 2^n \alpha_R$, και παρατηρούμε ότι αυτό είναι πάντα τουλάχιστον ίσο με $\frac{1}{n+1}$ (το οποίο συμβαίνει όταν το R είναι τέλειο δυαδικό). Οπότε μπορούμε να εκτιμήσουμε $\pi_R(\text{root})$ με σφάλμα $(1 \pm \zeta)$ για κάθε $\zeta > 0$, δειγματοληπτώντας m κόμβους του R σύμφωνα με την π_R και παίρνοντας ως εκτίμηση το ποσοστό $\hat{p} = \sum_{i=1}^m \frac{1}{m} X_i$, όπου $X_i = 1$ αν το i -οστό δείγμα ήταν η ρίζα, αλλιώς $X_i = 0$.

Είναι γνωστό από κλασικά επιχειρήματα ανάλυσης διασποράς (βλ. π.χ. το unbiased estimator theorem στο [68], το οποίο δίνουμε και στο κεφάλαιο 1) ότι αρκούν $m = O(\pi_R(\text{root}) \cdot \zeta^{-2}) = \text{poly}(n, \zeta^{-1})$ για να πετύχουμε

$$\Pr[(1 - \zeta)\pi_R(\text{root}) \leq \hat{p} \leq (1 + \zeta)\pi_R(\text{root})] \geq \frac{3}{4}$$

Μπορούμε να αυξήσουμε αυτή την πιθανότητα σε $1 - \delta$ για κάθε $\delta > 0$, επαναλαμβάνοντας την παραπάνω διαδικασία δειγματοληψίας $t = O(\log \delta^{-1})$ φορές, και παίρνοντας σαν τελική εκτίμηση τη διάμεσο των t εκτιμήσεων που υπολογίζονται κάθε φορά, (βλ. το median trick στο [68] ή το κεφάλαιο 1 της παρούσας εργασίας).

Η τυχαία δειγματοληψία σύμφωνα με την π_R μπορεί να εκτελεστεί προσομοιώνοντας την μαρκοβιανή αλυσίδα που ορίστηκε νωρίτερα στους κόμβους του R . Παρατηρήστε ότι η απόκλιση ϵ από τη στάσιμη κατανομή μπορεί να είναι αμελητέα και να απορροφηθεί στο ζ , με μόνο μια πολυωνυμική αύξηση του χρόνου λειτουργίας της μαρκοβιανής αλυσίδας.

Τελικά η εκτίμηση του α_R είναι $\hat{\alpha}_R = 2^{-n} \hat{p}$, και ισχύει

$$\Pr[(1 - \zeta)\alpha_R \leq \hat{\alpha}_R \leq (1 + \zeta)\alpha_R] \geq 1 - \delta.$$

\square

3. Το τρίτο μέρος του θεωρήματος [31](#) αποδεικνύεται ως εξής. Το $\#IS \in \text{TotP}$. Αν $NP \neq P$ (αντίστοιχα $NP \neq RP$) τότε $\#IS$ δεν επιδέχεται FPTAS (αντίστοιχα FPRAS) [\[67, 25\]](#).

Αφού ο υπολογισμός των συντελεστών κανονικοποίησης της οικογένειας κατανομών $(\pi_S)_S$ είναι TotP-hard (όταν το ύψος του S δεν είναι γνωστό), άρα το $\#IS$ ανάγεται σε αυτόν, άρα αν μπορούσαμε να υπολογίσουμε ακριβώς τους συντελεστές κανονικοποίησης των $(\pi_S)_S$, θα μπορούσαμε επίσης να υπολογίσουμε ακριβώς το $\#IS$, το οποίο θα συνεπαγόταν $NP=P$ (αντίστοιχα $NP=RP$ αν ο υπολογισμός είναι πιθανοτικός).

Όμως το $\#IS$ μπορεί όπως είπαμε να αναχθεί κατά Karρ/φειδωλά στο Size-of-Subtree όπου το ύψος του S είναι γνωστό, και μέσω της απόδειξης του πρώτου μέρους του παρόντος θεωρήματος, γίνεται φανερό ότι ανάγεται κατά Cook/Turing και στον υπολογισμό του α_S όπου το S είναι γνωστό. Οπότε πάλι ο ακριβής υπολογισμός του συντελεστή κανονικοποίησης α_S για κάθε S , γνωρίζοντας το ύψος του S , συνεπάγεται ακριβή υπολογισμό του $\#IS$, και άρα $NP=P$ (αντίστοιχα $NP=RP$ αν ο υπολογισμός είναι πιθανοτικός). □

4.4.3 Η πολυπλοκότητα υπολογισμού του μεγέθους του στηρίγματος

Αναλύουμε την πολυπλοκότητα υπολογισμού του μεγέθους του στηρίγματος των κατανομών στην οικογένεια $(\pi_S)_S$ (ορισμός [38](#)). Μετά συζητάμε δύο παρατηρήσεις που προκύπτουν από αυτή την ανάλυση.

Ορισμός 39. Καλούμε *additive approximation* σε μια πιθανότητα p , έναν αριθμό $\hat{p} = p \pm \xi$, για κάποιο $\xi \in (0, 1)$. Στην περίπτωση του *Size-of-Subtree* η ζητούμενη πιθανότητα είναι η $p \equiv |S|/2^n$. Στην περίπτωση του *Circuit Acceptance Probability Estimation problem (CAPE)* [\[87\]](#) η ζητούμενη πιθανότητα είναι η $p \equiv \#\text{sat. assignments}/2^n$, όπου n είναι το πλήθος των πυλών εισόδου του δοσμένου κυκλώματος.

Θεώρημα 32. Ο υπολογισμός του μεγέθους του στηρίγματος για μια κατανομή στην οικογένεια $(\pi_S)_S$ (ορισμός [38](#))

1. είναι TotP-complete κάτω από φειδωλές αναγωγές αν δεν γνωρίζουμε το ύψος του S , και TotP-complete υπό AP-αναγωγές αν γνωρίζουμε το ύψος του S ,
2. ανάγεται στον ακριβή υπολογισμό των συντελεστών κανονικοποίησης, ανεξαρτήτως αν ξέρουμε το ύψος του S ,
3. *additive error approximation* (βλ. ορισμό [39](#)) γίνεται σε πιθανοτικό πολυωνυμικό χρόνο, (παρατηρήστε ότι εν γένει το μέγεθος του στηρίγματος είναι εκθετικά μεγάλο στο n), ανεξαρτήτως αν ξέρουμε το ύψος του S ,
4. ο ακριβής του υπολογισμός είναι αδύνατος ντετερμινιστικά (ή αντίστοιχα πιθανοτικά) αν $NP \neq P$ (ή αντίστοιχα αν $NP \neq RP$), ανεξαρτήτως αν ξέρουμε το ύψος του S ,

5. προσέγγιση με πολλαπλασιαστικό πολυωνυμικό σφάλμα είναι αδύνατο ντετερμινιστικά (ή αντίστοιχα πιθανοτικά) αν και μόνο αν $NP \neq P$ (ή αντίστοιχα αν $NP \neq RP$), ανεξαρτήτως αν ξέρουμε το ύψος του S .

Απόδειξη. 1. Από τον ορισμό [38](#), βλέπουμε ότι μια θετική πιθανότητα δίνεται σε κάθε κόμβο του αντίστοιχου δέντρου εισόδου S , έτσι το μέγεθος του στηρίγματος ισούται ακριβώς με το μέγεθος του δέντρου. Η δήλωση του θεωρήματος προκύπτει αφενός από την TotP-πληρότητα του Size-of-Subtree κάτω από φειδωλές αναγωγές. Αφετέρου από την TotP-πληρότητα του #IS υπό αναγωγές που διατηρούν την προσέγγιση, και το γεγονός ότι το #IS ανάγεται στο Size-of-Subtree όπου το ύψος του δέντρου που δίνεται ως είσοδος είναι γνωστό.

2. Η δήλωση προκύπτει από την πρόταση [4](#).
3. Αποδεικνύουμε πρώτα την εξής πρόταση.

Πρόταση 6. *Αν γνωρίζουμε το ύψος του S , τότε για κάθε $\xi > 0, \delta > 0$ μπορούμε να πάρουμε μια εκτίμηση $|\hat{S}|$ του $|S|$ σε χρόνο $\text{poly}(n, \xi^{-1}, \log \delta^{-1})$ τέτοια ώστε*

$$\Pr[|S| - \xi 2^n \leq |\hat{S}| \leq |S| + \xi 2^n] \geq 1 - \delta$$

Απόδειξη. Έστω $\zeta = \frac{\xi}{2^{(n+1)}}$ και $\epsilon = \frac{\zeta}{1+\zeta}$, οπότε $\text{poly}(\epsilon^{-1}) = \text{poly}(\zeta^{-1}) = \text{poly}(n, \xi^{-1})$.

Άρα σύμφωνα με την πρόταση [5](#) έχουμε σε χρόνο $\text{poly}(n, \xi^{-1}, \log \delta^{-1})$ εκτιμήσεις $\forall i = 1, \dots, n$

$$(1 - \epsilon)\alpha_{S_i} \leq \hat{\alpha}_{S_i} \leq (1 + \epsilon)\alpha_{S_i}. \quad (4.3)$$

Θα χρησιμοποιήσουμε την πρόταση [4](#). Έστω $A = \frac{1}{\alpha_{S_n}}$ και $B = \sum_{k=0}^{n-1} \frac{1}{\alpha_{S_k}}$, οπότε $|S| = A - B$, και σαφώς είναι $B \leq A$.

Από την [\(4.3\)](#) έχουμε $\frac{1}{1+\epsilon}A \leq \hat{A} \leq \frac{1}{1-\epsilon}A \Leftrightarrow (1 - \zeta)A \leq \hat{A} \leq (1 + \zeta)A$ και ομοίως $(1 - \zeta)B \leq \hat{B} \leq (1 + \zeta)B$.

Συνεπώς $(1 - \zeta)A - (1 + \zeta)B \leq \hat{A} - \hat{B} \leq (1 + \zeta)A - (1 - \zeta)B \Leftrightarrow$

$A - B - \zeta(A + B) \leq \hat{A} - \hat{B} \leq A - B + \zeta(A + B)$, και αφού $A \geq B$, έχουμε

$|S| - 2\zeta A \leq |\hat{S}| \leq |S| + 2\zeta A$. Και αφού από το λήμμα [4](#) το μέγιστο A είναι $2^n(n + 1)$, έχουμε

$$|S| - 2\zeta(n + 1)2^n \leq |\hat{S}| \leq |S| + 2\zeta(n + 1)2^n \Leftrightarrow$$

$$|S| - \xi \cdot 2^n \leq |\hat{S}| \leq |S| + \xi \cdot 2^n.$$

□

Για να ολοκληρώσουμε την απόδειξη, έστω $p = \frac{|S|}{2^n}$. Για κάθε $\xi > 0, \delta > 0$ μπορούμε να πάρουμε μια εκτίμηση \hat{p} σε χρόνο $\text{poly}(n, \xi^{-1}, \log \delta^{-1})$ τέτοια ώστε

$$\Pr[p - \xi \leq \hat{p} \leq p + \xi] \geq 1 - \delta$$

η οποία ικανοποιεί τον ορισμό του additive approximation για το $|S|$, δηλαδή για το μέγεθος του στηρίγματος της π_S .

Τέλος, αν το ύψος του S δεν είναι γνωστό, παρά μόνο ένα άνω φράγμα του n' , μπορούμε πάλι να έχουμε additive approximation με απλή δειγματοληψία από το τέλει δυαδικό δέντρο ύψους n' . Συζητούμε παρακάτω την πιθανή σημασία του εναλλακτικού μας αλγόριθμου για όταν γνωρίζουμε το ύψος του S .

4. Τα επιχειρήματα είναι παρόμοια με αυτά για το τρίτο μέρος του θεωρήματος [31](#). Το $\#IS \in \text{TotP}$ και δεν επιδέχεται FPTAS (αντίστοιχα FPRAS) αν $\text{NP} \neq \text{P}$ (αντίστοιχα $\text{NP} \neq \text{RP}$) [\[67, 25\]](#).

Από τη δυσκολία του υπολογισμού του μεγέθους του στηρίγματος των $(\pi_S)_S$, προκύπτει ότι δεν μπορούμε να το υπολογίσουμε ακριβώς, αλλιώς θα μπορούσαμε να υπολογίσουμε ακριβώς και το $\#IS$, γεγονός που θα συνεπαγόταν $\text{NP}=\text{P}$ (αντίστοιχα $\text{NP}=\text{RP}$ αν ο υπολογισμός ήταν πιθανοτικός).

5. Γεγονός 1: Αν $\text{NP}=\text{RP}$ τότε όλα τα προβλήματα στην TotP επιδέχονται FPRAS.

Απόδειξη για το γεγονός 1: Στο [\[71\]](#) ο Stockmeyer απέδειξε ότι ένα FPRAS, με πρόσβαση σε Σ_2^P μαντείο, υπάρχει για κάθε πρόβλημα στην $\#P$. Αν $\text{NP}=\text{RP}$ τότε $\Sigma_2^P = \text{RP}^{\text{RP}} \subseteq \text{BPP}$. Τέλος είναι εύκολο να δει κανείς ότι ένα FPRAS με πρόσβαση σε ένα BPP μαντείο, μπορεί να αντικατασταθεί από ένα άλλο FPRAS, που προσομοιώνει τις κλήσεις στο μαντείο μόνο του.

Γεγονός 2: Αν $\text{NP} \neq \text{RP}$ τότε είναι αδύνατο να έχουμε FPRAS για κάθε πρόβλημα στην TotP.

Απόδειξη για το γεγονός 2: Το πρόβλημα $\#IS$ είναι μη προσεγγίσιμο αν $\text{NP} \neq \text{RP}$, και ανήκει στην TotP.

Τέλος είναι αποδεδειγμένο ότι για κάθε αυτοαναγώγιμο πρόβλημα στην $\#P$, ένας αλγόριθμος με πολυωνυμικό πολλαπλασιαστικό σφάλμα μπορεί να μετατραπεί σε FPRAS [\[69\]](#).

Εφόσον ο υπολογισμός του μεγέθους του στηρίγματος μιας π_S είναι ανεξαρτήτως αν ξέρουμε το ύψος του S TotP-complete υπό αναγωγές που διατηρούν την προσέγγιση (αφού και οι φειδωλές αναγωγές διατηρούν την προσέγγιση), καταλήγουμε ότι επιδέχεται αλγόριθμο με πολυωνυμικό πολλαπλασιαστικό σφάλμα αν και μόνο αν $\text{NP}=\text{P}$ (αντίστοιχα $\text{NP}=\text{RP}$ αν ο αλγόριθμος είναι πιθανοτικός).

□

4.5 Παρατηρήσεις και ανοιχτά ερωτήματα

Παρατήρηση 1 Έχουμε εξετάσει τρία υπολογιστικά προβλήματα που σχετίζονται με οποιαδήποτε κατανομή πιθανότητας: δειγματοληψία, υπολογισμός του συντελεστή κανονικοποίησης και υπολογισμός του μεγέθους του στηρίγματος. Για την ομοιόμορφη κατανομή ο συντελεστής κανονικοποίησης είναι πολλαπλάσιο του μεγέθους του στηρίγματος και η δειγματοληψία είναι ισοδύναμη με την ύπαρξη FPRAS για το μέγεθος του στηρίγματος [59]. Ωστόσο, για μια γενική κατανομή δεν είναι μόνο άγνωστη η πολυπλοκότητά των παραπάνω τριών προβλημάτων, αλλά δεν είναι καν σαφές εάν αυτά τα τρία προβλήματα είναι υπολογιστικά ισοδύναμα ή όχι.

Για την οικογένεια των κατανομών που μελετήσαμε εδώ (ορισμός 38) αποδεικνύεται ότι τα τρία αυτά προβλήματα δεν είναι όλα ισοδύναμα εκτός αν $NP = RP$.

Επίσης, δείξαμε ότι ο ακριβής υπολογισμός του μεγέθους του στηρίγματος ανάγεται στον ακριβή υπολογισμό του συντελεστή κανονικοποίησης (fact 2), αλλά όχι με αναγωγή που διατηρεί την προσέγγιση. Τα προηγούμενα επιχειρήματα υποδηλώνουν ότι μια τέτοια αναγωγή, μεταξύ των δύο προβλημάτων, υπάρχει αν και μόνο αν $NP = RP$.

Ανοιχτό πρόβλημα 1 Επομένως, είναι ένα ανοιχτό πρόβλημα ισοδύναμο με το NP vs. RP η ύπαρξη μιας αναγωγής που διατηρεί την προσέγγιση, από τον υπολογισμό του μεγέθους του στηρίγματος στον υπολογισμό των συντελεστών κανονικοποίησης των κατανομών $(\pi_S)_S$ (def. 38). Μάλιστα αρκεί αναγωγή που να λαμβάνει υπόψιν ότι γνωρίζουμε τα ύψη των δέντρων που λαμβάνουν χώρα στους υπολογισμούς, αφού όπως ήδη συζητήσαμε, το #IS ανάγεται στο Size-of-Subtree με γνωστό ύψος δέντρου, και έχει FPRAS αν και μόνο αν $NP=RP$.

Παρατήρηση 2 Έχουμε δείξει πώς να πάρουμε μια πιθανοτική προσεγγιστική λύση με προσθετικό σφάλμα για το πρόβλημα Size-of-Subtree. Θα πρέπει να αναφέρουμε ότι μια τέτοια προσέγγιση θα μπορούσε επίσης να επιτευχθεί με μια απλή τυχαία διαδικασία δειγματοληψίας που επιλέγει ομοιόμορφα τυχαία $m = poly(n)$ κόμβους του πλήρους δυαδικού δέντρου T ύψους n και λαμβάνει ως εκτίμηση το μέγεθος του $|S|$, το ποσοστό των m δειγμάτων που ανήκουν στο S . Αυτή είναι μια εφαρμογή της γενικής μεθόδου του [34] κεφάλαιο 6.2.2.

Η εναλλακτική μας μέθοδος εκμεταλλεύεται ορισμένα ειδικά χαρακτηριστικά της TotP και έτσι δεν μπορεί να γενικευτεί για κάθε πρόβλημα στη #P.

Είναι γνωστό ότι η αποτυχαιοποίηση της γενικής απλής μεθόδου είναι τόσο δύσκολη όσο η απόδειξη διαφόρων circuit lower bounds [81]. Ωστόσο, δεν γνωρίζουμε μια παρόμοια σχέση μεταξύ των circuit lower bounds και της ντετερμινιστικής προσέγγισης με προσθετικό σφάλμα, όταν η τελευταία περιορίζεται στα προβλήματα στην TotP, οπότε ίσως να μην είναι εξίσου δύσκολο να αποτυχαιοποιηθεί η μέθοδος μας.

Ανοιχτό πρόβλημα 2 Πρόκειται για ένα ανοιχτό πρόβλημα το πώς να αποτυχοποιήσουμε τους αλγόριθμους προσέγγισης σφάλματος προσθετικού για το μέγεθος του στηρίγματος, σε υποεκθετικό χρόνο. Αυτό θα οδηγούσε σε μια ντετερμινιστική λύση του προβλήματος CAPE (βλέπε def. [39]) με προσθετικό σφάλμα, για οικογένειες κυκλωμάτων για τα οποία η μέτρηση του αριθμού των αποδεκτών εισόδων είναι στην TotP (θα το ονομάσουμε TotP-CAPE.)

Σημειώστε ότι ο καλύτερος (ακριβής και πρόσθετικού σφάλματος) ντετερμινιστικός αλγόριθμος που είναι γνωστός για το CAPE, σε ένα αυθαίρετο κύκλωμα, είναι με εξαντλητική αναζήτηση. Αποτυχοποίηση αυτού σε χρόνο πιο γρήγορο από τον εξαντλητικό αλγόριθμο αναζήτησης, δηλαδή ακόμη και σε χρόνο $2^{\gamma n} \text{poly}(n)$ για κάποιο $\gamma < 1$, θα δώσει ότι $\text{NEXP} \not\subseteq \text{P} / \text{poly}$ [81]. Το τελευταίο είναι μια μακροχρόνια εικασία.

Ανοιχτό πρόβλημα 3 Ένα τελικό ανοιχτό πρόβλημα είναι το αν μπορούμε να επιτύχουμε την αποτυχοποίηση του ίδιου αλγόριθμου σε πολυωνυμικό χρόνο. Ένα τέτοιο αποτέλεσμα θα συνεπαγόταν επίσης μια λύση στο πρόβλημα CAPE σε ντετερμινιστικό πολυωνυμικό χρόνο για κυκλώματα βάθους δύο AC^0 (δηλ. DNF και CNF φόρμουλες). Ο καλύτερος ντετερμινιστικός αλγόριθμος που μέχρι τώρα είναι γνωστός είναι χρόνου $n^{O(\log \log n)}$ [37]. (Για περισσότερα στο AC^0 - CAPE, δείτε την έρευνα [82] σελ.13 και [57] για κάποιο παλαιότερο αποτέλεσμα.)

4.6 Σχετικές εργασίες

Σχετικά με το Size-of-Subtree: Στο [51] ο Knuth παρέχει έναν πιθανοτικό αλγόριθμο πρακτικά χρήσιμο, αλλά με ένα εκθετικό σφάλμα χειρότερης περίπτωσης. Κάποιες τροποποιήσεις και επεκτάσεις του αλγορίθμου του Knuth παρουσιάστηκαν και δοκιμάστηκαν πειραματικά στα [65, 21, 50], χωρίς σημαντικές βελτιώσεις για τις χειρότερες περιπτώσεις. Υπάρχουν επίσης πολλά ευρετικά και πειραματικά αποτελέσματα σχετικά με το πρόβλημα περιορισμένο σε ειδικούς backtracking αλγόριθμους, ή ειδικά στιγμιότυπα αυτών, βλέπε π.χ. [15] για περισσότερες αναφορές. Παραδόξως, υπάρχουν FRAS για τυχαία μοντέλα του προβλήματος [29, 75]. Στο [7] μελετώνται κβαντικοί αλγόριθμοι για το πρόβλημα. Στο [71] ο Stockmeyer παρείχε χωρίς προϋποθέσεις κάτω φράγματα για το πρόβλημα, αλλά για ένα μοντέλο υπολογισμού που είναι διαφορετικό από τη μηχανή Turing, ήτοι μια παραλλαγή του (μη ομοιόμορφου) μοντέλου δέντρων αποφάσεων.

Υπάρχουν πολυάριθμα άρθρα σχετικά με αλγοριθμικά αποτελέσματα και αποτελέσματα δυσκολίας για μεμονωμένα προβλήματα στη #P και την TotP, π.χ. [76, 43, 46, 25, 79]. Εντούτοις, εκτός από το πρόβλημα Size-of-Subtree, άλλα προβλήματα TotP-πλήρη δεν έχουν μελετηθεί αλγοριθμικά.

Υπάρχει επίσης μια τεράστια βιβλιογραφία για μαρκοβιανές αλυσίδες και τα υπολογιστικά ερωτήματα που σχετίζονται με αυτές, όπως αυτά που εξετάζονται σε αυτό το κεφάλαιο, δηλαδή προσδιορισμός του χρόνου σύγκλισης, της στάσιμης κατανομής και της πολυπλοκότητας του υπολογισμού της partition function (δηλαδή

του συντελεστή κανονικοποίησης). Τέτοιοι αλγόριθμοι είναι γνωστοί με ονομασίες όπως Glauber dynamics, Gibbs sampling, Metropolis - Hastings algorithm, κλπ. [32, 59, 38]. Αυτές οι μαρκοβιανές αλυσίδες είναι σχεδιασμένες για μεμονωμένα προβλήματα που αφορούν τον υπολογισμό ενός σταθμισμένου αθροίσματος πάνω στο σύνολο λύσεων για ένα συνδυαστικό πρόβλημα. Τέτοια προβλήματα είναι για παράδειγμα το μοντέλο hard core και το μοντέλο Potts από τη στατιστική φυσική. Η βιβλιογραφία για τα θέματα αυτά είναι τεράστια, αναφέρουμε μόνο ενδεικτικά μερικά [16, 14, 18, 70, 80, 33].

Κεφάλαιο 5

Αλλαγές φάσης για το tree-depth μοντέλο

Σε αυτό το κεφάλαιο σχεδιάζουμε και αναλύουμε ένα πιθανοτικό μοντέλο (που αποτελείται από μια οικογένεια κατανομών πιθανότητας P_λ πάνω στους κόμβους ενός δέντρου, και οικογένεια αλυσίδων M_λ που συγκλίνουν σε αυτές), το οποίο μοντέλο είναι παραμετροποιημένο από μια παράμετρο $\lambda \in \mathbb{R}$, και γενικεύει όλες τις μαρκοβιανές αλυσίδες του προηγούμενου κεφαλαίου και τις στάσιμες κατανομές τους. Για αυτό το μοντέλο παρατηρούμε και αποδεικνύουμε φαινόμενα αλλαγής φάσης. Αφενός υπάρχει αλλαγή φάσης ως προς τον χρόνο σύγκλισης της M_λ συναρτήσει του λ . Συγκεκριμένα, υπάρχει μια ασυνεχής μετάβαση από εκθετικό σε πολυωνυμικό χρόνο σύγκλισης για λ που εξαρτάται από το δέντρο. Για το πλήρες δέντρο, όπως και για τα δέντρα που αποτελούν δύσκολα στιγμιότυπα του προβλήματος Size-of-Subtree, η αλλαγή φάσης είναι στο $\lambda = 2$, ενώ για το μονοπάτι (το οποίο βρίσκεται στον αντίποδα του πλήρους δέντρου) η αλλαγή φάσης είναι στο $\lambda = 1$. Επίσης αποδεικνύουμε ότι υπάρχει αλλαγή φάσης για την πολυπλοκότητα του προβλήματος από δύσκολα προσεγγίσιμο (NP-hard to approximate) σε προσεγγίσιμο με FPRAS για κάποιο $\lambda \in [1, 2]$.

5.1 Εισαγωγή

Υπάρχουν, όπως ήδη είδαμε στο κεφάλαιο 1, δύσκολα μετρικά προβλήματα των οποίων το αντίστοιχο πρόβλημα απόφασης ύπαρξης λύσης είναι εύκολο, όπως π.χ. το Permanent, το #IS, το #DNF. Κάποια από αυτά επιδέχονται FPRAS. Για παράδειγμα ένα από τα σημαντικότερα #P-πλήρη προβλήματα είναι το Permanent, το οποίο επιδέχεται FPRAS, και μάλιστα πρέπει να σημειωθεί ότι ο αλγόριθμος προσέγγισής του χρησιμοποιεί μια σταθμισμένη εκδοχή του προβλήματος [44, 45].

Όμως το Permanent δεν είναι πλήρες υπό αναγωγές που να διατηρούν την προσέγγιση. Εδώ επικεντρωνόμαστε στο πρόβλημα Size-of-Subtree, γνωστό και ως το πρόβλημα υπολογισμού του μεγέθους του δέντρου μιας backtracking διαδικασίας,

επειδή είναι πλήρες για την κλάση όλων των αυτοαναγώγιμων μετρητικών προβλημάτων με αντίστοιχο πρόβλημα απόφασης στο P, υπό αναγωγές που διατηρούν την προσεγγισιμότητα.

Μελετούμε μια σταθμισμένη εκδοχή του προβλήματος, η οποία εξαρτάται από μια παράμετρο $\lambda \in \mathbb{R}_{>0}$.

Δείχνουμε καταρχάς ότι για κάθε $\lambda > 0$ είναι δύσκολο να υπολογιστεί ακριβώς εκτός αν NP=P. Στη συνέχεια ανακαλύπτουμε και αποδεικνύουμε αλλαγή φάσης ως προς την πολυπλοκότητα προσεγγισής του, σε κάποια κρίσιμη τιμή του $\lambda \in [1, 2]$, πάνω από την οποία επιδέχεται FPRAS, ενώ κάτω από την οποία είναι μη προσεγγίσιμο εκτός αν NP=RP.

Επίσης σχεδιάζουμε προσεγγιστικό αλγόριθμο που βασίζεται σε μαρκοβιανή αλυσίδα τύπου Metropolis, της οποίας αναλύουμε το χρόνο σύγκλισης, και έτσι αποδεικνύουμε ότι παρουσιάζει αλλαγή φάσης ως προς το χρόνο εκτέλεσής του από εκθετικό σε πολυωνυμικό, σε κάποια κρίσιμη τιμή του $\lambda \in [1, 2]$, που εξαρτάται από το εκάστοτε στιγμιότυπο. Π.χ. για το μονοπάτι ύψους n η αλλαγή φάσης είναι στο $\lambda = 1$ ενώ για το τέλειο δυαδικό δέντρο η αλλαγή φάσης είναι στο $\lambda = 2$.

Επιπλέον μελετούμε μια παραλλαγή του προβλήματος Size-of-Subtree, στην οποία το ύψος του δέντρου που δίνεται ως είσοδος δεν είναι γνωστό, παρά μόνο ένα άνω φράγμα αυτού. Αυτή η παραλλαγή είναι ακόμα πιο δύσκολη από την προηγούμενη και συγκεκριμένα είναι TotP-πλήρης υπό φειδωλές αναγωγές.

Αποδεικνύουμε ότι το πρόβλημα υπολογισμού του αντίστοιχου σταθμισμένου προβλήματος είναι για κάθε $\lambda > 0$ μη προσεγγίσιμο εκτός αν NP=RP. Παράλληλα μέσω αναγωγής από το SAT προσδιορίζουμε και χαρακτηρίζουμε μια οικογένεια δύσκολων στιγμιότυπων για το σταθμισμένο πρόβλημα.

Τέλος, προκύπτει από τα αποτελέσματά μας ότι το πρόβλημα NP vs. RP είναι ισοδύναμο με το ερώτημα ύπαρξης FPRAS για τις δύσκολες εκδοχές του προβλήματος που μελετάμε.

5.1.1 Σύνδεση με τα προηγούμενα

Στο προηγούμενο κεφάλαιο μελετήσαμε μερικές οικογένειες μαρκοβιανών αλυσίδων για μερικά TotP-πλήρη προβλήματα. Για κάθε δυαδικό δέντρο S εξετάσαμε δύο διαφορετικές μαρκοβιανές αλυσίδες που συγκλίνουν σε δύο διαφορετικές στάσιμες κατανομές P_1^S, P_2^S . Αυτές οι κατανομές μπορούν να οριστούν με την ανάθεση κάποιου βάρους σε κάθε κόμβο του δέντρου και στη συνέχεια διαιρώντας με το άθροισμα όλων των βαρών έτσι ώστε το άθροισμα των πιθανοτήτων να είναι 1. Αυτό το άθροισμα ονομάζεται "συντελεστής κανονικοποίησης" ή "partition function" μιας κατανομής πιθανότητας. Έστω Z_1^S, Z_2^S οι αντίστοιχοι συντελεστές κανονικοποίησης των P_1^S και P_2^S .

Σε αυτό το κεφάλαιο δείχνουμε ότι μπορούμε να γενικεύσουμε τις δύο παραπάνω κατανομές πιθανοτήτων με ένα ενιαίο μοντέλο $P^S(\lambda)$, $\lambda \in \mathbb{R}_{>0}$, έτσι ώστε για κάθε S να έχουμε $P^S(1) = P_1^S$ και $P^S(2) = P_2^S$.

Από τα αποτελέσματα του προηγούμενου κεφαλαίου παρατηρούμε ότι αυτό το μοντέλο παρουσιάζει τελείως διαφορετική συμπεριφορά για $\lambda = 1$ και $\lambda = 2$:

- Και για τα δύο $\lambda = 1$ και $\lambda = 2$, ο υπολογισμός του Z_λ^S είναι δύσκολος (#P-complete), αλλά
- Για $\lambda = 1$ έχουμε
 - εκθετικό χρόνο σύγκλισης για την αντίστοιχη μαρκοβιανή αλυσίδα.
 - αδύνατη ύπαρξη FPRAS για το Z_1^S εκτός αν NP=RP.
- Για $\lambda = 2$ έχουμε
 - πολυωνυμικό χρόνο σύγκλισης για την αντίστοιχη μαρκοβιανή αλυσίδα
 - FPRAS για το Z_2^S .

Ερωτήματα που προκύπτουν Το ερώτημα που τίθεται είναι τι συμβαίνει με τις άλλες τιμές του $\lambda > 0$.

- Είναι ο υπολογισμός του Z_λ^S δύσκολος για κάθε λ ;
- Μπορούμε να γενικεύσουμε τις μαρκοβιανές αλυσίδες του προηγούμενου κεφαλαίου με μια κοινή οικογένεια μαρκοβιανών αλυσίδων παραμετροποιημένων από το λ ;
- Ποιός είναι ο χρόνος σύγκλισης αυτών των μαρκοβιανών αλυσίδων ως προς λ ;
- Υπάρχει αλλαγή φάσης στο χρόνο σύγκλισης αυτής της οικογένειας μαρκοβιανών αλυσίδων ως προς λ ; Με άλλα λόγια, η μετάβαση από τον εκθετικό χρόνο σύγκλισης για $\lambda = 1$ στον πολυωνυμικό χρόνο σύγκλισης για το $\lambda = 2$ συμβαίνει ομαλά, ή "ξαφνικά" (δηλαδή μη αναλυτικά, π.χ. ασυνεχώς); Εάν υπάρχει αλλαγή φάσης, ποια είναι η κρίσιμη τιμή του λ όπου αυτή συμβαίνει;
- Το Z_λ^S για ποιές τιμές του λ είναι προσεγγίσιμο;
- Υπάρχει αλλαγή φάσης ως προς την πολυπλοκότητα προσέγγισης του Z_λ^S , και αν ναι, εμφανίζεται στην ίδια τιμή του λ που (ενδεχομένως) εμφανίζει αλλαγή φάσης ο χρόνος σύγκλισης των παραπάνω μαρκοβιανών αλυσίδων;

5.2 Το tree-depth μοντέλο

Ορίζουμε για κάθε δυαδικό δέντρο S και κάθε πραγματικό $\lambda > 0$ την ακόλουθη οικογένεια κατανομών πιθανότητας P_λ^S .

Ορισμός 40. Έστω S ένα δυαδικό δέντρο ύψους n και έστω $V(S)$ το σύνολο των κόμβων του. Ορίζουμε την κατανομή πιθανότητας $P_\lambda^S : V(S) \rightarrow [0, 1]$ ως εξής. Για κάθε $v \in V(S)$, $\lambda > 0$

$$P_\lambda^S(v) = \frac{\lambda^{n-\text{depth}(v)}}{Z_\lambda^S}$$

όπου

$$Z_\lambda^S = \sum_{v \in V(S)} \lambda^{n - \text{depth}(v)}$$

5.3 Αποτελέσματα

Αναλούμε το χρόνο σύγκλισης της μαρκοβιανής αλυσίδας τύπου Metropolis για το πρόβλημά μας.

Όπως αποδεικνύεται παρακάτω, το σημείο όπου εμφανίζεται η αλλαγή φάσης εξαρτάται από το δέντρο. Για το τέλειο δυαδικό δένδρο ύψους n , η αλλαγή φάσης εμφανίζεται στο $\lambda = 2$. Για τον άλλο ακραίο τύπο δέντρου, δηλαδή το μονοπάτι μήκους n , η αλλαγή φάσης εμφανίζεται στο $\lambda = 1$.

Πιο συγκεκριμένα, για $\lambda < 1$ ο χρόνος σύγκλισης της μαρκοβιανής αλυσίδας είναι εκθετικός για κάθε δέντρο. Για $\lambda \geq 2$ ο χρόνος σύγκλισης είναι πολυωνυμικός για κάθε δέντρο. Ο χρόνος σύγκλισης εξαρτάται από το δέντρο για $1 \leq \lambda < 2$.

Επίσης μελετούμε την πολυπλοκότητα ακριβούς και προσεγγιστικού υπολογισμού του Z_λ^S .

Για τα πλήρη δέντρα όπως και για τα μονοπάτια το Z_λ^S μπορεί να υπολογιστεί ακριβώς για κάθε λ . Στη χειρότερη περίπτωση αποδεικνύεται ότι ο ακριβής υπολογισμός του Z_λ^S είναι αδύνατος εκτός αν $\text{NP}=\text{P}$, αντίστοιχα πιθανοτικός ακριβής υπολογισμός είναι αδύνατος εκτός αν $\text{NP}=\text{RP}$.

Όσον αφορά στην προσεγγισσιμότητα του Z_λ^S , προκύπτει ότι εξαρτάται με πολύ ουσιαστικό τρόπο από το αν μας δίνεται το ακριβές ύψος του δέντρου ή ένα άνω φράγμα αυτού.

Όταν το ύψος του δέντρου είναι γνωστό, τότε για κάθε $\lambda \leq 1$ η προσέγγιση του Z_λ^S είναι αδύνατη εκτός αν $\text{NP}=\text{RP}$, ενώ για κάθε $\lambda \geq 2$ υπάρχει FPRAS για το Z_λ^S . Επομένως υπάρχει αλλαγή φάσης από μη προσεγγίσιμο σε προσεγγίσιμο στο διάστημα $[1, 2]$.

Όταν το ύψος του δέντρου δεν είναι γνωστό, τότε το Z_λ^S είναι μη προσεγγίσιμο για κάθε $\lambda > 0$.

Επιπλέον προσδιορίζουμε μια οικογένεια δύσκολων στιγμιότυπων για το πρόβλημα προσέγγισης του Z_λ^S όταν το ύψος δεν είναι γνωστό. Για τα παραπάνω δύσκολα στιγμιότυπα του προβλήματος προσέγγισης του Z_λ^S , ο χρόνος σύγκλισης της αλυσίδας παρουσιάζει αλλαγή φάσης επίσης στο $\lambda = 2$. Παρόλο όμως που για $\lambda \geq 2$ έχουμε sampling σε πολυωνυμικό χρόνο, δεν μπορούμε να έχουμε FPRAS για το Z_λ^S σε αυτή την περίπτωση.

Σημασία των αποτελεσμάτων Η καινοτομία αυτού του κεφαλαίου συνίσταται σε δύο σημεία.

Πρώτον ανακαλύπτουμε φαινόμενα αλλαγής φάσης που δεν ήταν ήδη γνωστά, και αποδεικνύουμε αυστηρά την ύπαρξή τους.

Ένα αξιοσημείωτο συμπέρασμα των αποτελεσμάτων μας είναι ότι για τα σταθμισμένα προβλήματα η δειγματοληψία δεν συνεπάγεται απαραίτητα και σταθμι-

σμένη μέτρηση, αντίθετα με τα μη σταθμισμένα προβλήματα όπου ομοιόμορφη δειγματοληψία συνεπάγεται προσεγγιστική μέτρηση. Αυτό προκύπτει από το τελευταίο αποτέλεσμα που αναφέραμε, ότι όταν το ύψος του δέντρου δεν είναι γνωστό, για $\lambda \geq 2$ έχουμε sampling σε πολυωνυμικό χρόνο, ενώ δεν μπορούμε να έχουμε FPRAS για το Z_λ^S σε αυτή την περίπτωση.

Είναι επίσης ενδιαφέρον ότι για την περίπτωση που το ύψος του δέντρου είναι γνωστό, ο αλγόριθμος τύπου Metropolis είναι αντιπροσωπευτικός της πολυπλοκότητας χειρότερης περίπτωσης του Z_λ^S για $\lambda \leq 1$ και $\lambda \geq 2$. Αποτελεί ανοιχτό ερώτημα το αν ισχύει το ίδιο για $\lambda \in (1, 2)$: Ξέρουμε ότι υπάρχει αλλαγή φάσης ως προς την πολυπλοκότητα του Z_λ^S στο $[1, 2]$, όπως ξέρουμε ότι και για κάθε στιγμίοτυπο ο αλγόριθμος τύπου Metropolis εμφανίζει αλλαγή φάσης ως προς το χρόνο εκτέλεσης στο ίδιο διάστημα, αλλά δεν ξέρουμε την ακριβή τιμή στην οποία αυτές οι αλλαγές φάσης συμβαίνουν και αν ταυτίζονται στα στιγμίοτυπα χειρότερης περίπτωσης.

Δεύτερον βρίσκουμε σε όρους σχετικούς με την έρευνα πάνω σε μετρητική πολυπλοκότητα και με τη σχέση της με μαρκοβιανές αλυσίδες, νέες ισοδύναμες διατυπώσεις του προβλήματος NP vs. RP, το οποίο αποτελεί ένα από τα σημαντικότερα ανοικτά προβλήματα της θεωρητικής πληροφορικής με πολλές θεωρητικές και πρακτικές συνέπειες.

5.4 Η μαρκοβιανή αλυσίδα

Αναλύουμε την μαρκοβιανή αλυσίδα που ακολουθεί τον κανόνα του Metropolis: Για κάθε S και λ , από κάθε κόμβο x , επιλέγουμε ένα γείτονα y του x με πιθανότητα $1/3$, και πηγαίνουμε στο y με πιθανότητα $\min\{1, \frac{P_\lambda^S(y)}{P_\lambda^S(x)}\}$. Οπότε συνολικά οι πιθανότητα μετάβασης από το x στο y είναι $p(x, y) = \min\{1, \frac{P_\lambda^S(y)}{P_\lambda^S(x)}\} \cdot \frac{1}{3}$.

Για απλοποίηση του συμβολισμού, όταν είναι ξεκάθαρο από τα συμφραζόμενα, παραλείπουμε τα λ και S από τους δείκτες και γράφουμε απλά $P(u)$, $p(x, y)$, Z για τη στάσιμη κατανομή, τις πιθανότητες μετάβασης και τον συντελεστή κανονικοποίησης αντίστοιχα.

Αν u είναι ο γονέας του v τότε

$$P(u) = \frac{\lambda^{n-\text{depth}(u)}}{Z},$$

και

$$P(v) = \frac{\lambda^{n-\text{depth}(v)}}{Z} = \frac{\lambda^{n-\text{depth}(u)-1}}{Z} = \frac{P(u)}{\lambda}.$$

Οπότε $\frac{P(u)}{P(v)} = \lambda$ και οι πιθανότητες μετάβασης είναι ως εξής.

Ορισμός 41. Έστω S ένα δυαδικό δέντρο ύψους n , και έστω $\lambda > 0$. Ορίζουμε μια μαρκοβιανή αλυσίδα M_λ^S της οποίας ο χώρος καταστάσεων είναι το σύνολο των κόμβων $V(S)$ του δέντρου. Οι πιθανότητες μετάβασης είναι

- $\lambda > 1$

$$p(x, y) = \frac{1}{3\lambda} \text{ αν } y \text{ είναι παιδί του } x$$

$$p(x, y) = \frac{1}{3} \text{ αν } y \text{ είναι ο γονιός του } x$$

$$p(x, y) = 0 \text{ για κάθε άλλο } y \neq x$$

$$p(x, x) = 1 - \sum_{y \neq x} p(x, y).$$
- $0 < \lambda < 1$

$$p(x, y) = \frac{1}{3} \text{ αν } y \text{ είναι παιδί του } x$$

$$p(x, y) = \frac{\lambda}{3} \text{ αν } y \text{ είναι ο γονιός του } x$$

$$p(x, y) = 0 \text{ για κάθε άλλο } y \neq x$$

$$p(x, x) = 1 - \sum_{y \neq x} p(x, y).$$

Θεώρημα 33. Για κάθε S, λ , η στάσιμη κατανομή της M_λ^S είναι η P_λ^S .

Απόδειξη. Για κάθε $u \in V(S)$ $P_\lambda^S(u) = \sum_{v \in V(S)} P_\lambda^S(v)p(v, u)$. □

5.5 Ο χρόνος σύγκλισης

Για να αναλύσουμε το χρόνο σύγκλισης, θα εξετάσουμε την τεμπέλικη έκδοση της μαρκοβιανής αλυσίδας, δηλαδή με πιθανότητα $1/2$ δεν κάνουμε τίποτα και με πιθανότητα $1/2$ ακολουθούμε τον κανόνα Metropolis όπως περιγράφηκε προηγουμένως.

Θα φράξουμε την αγωγιμότητα της μαρκοβιανής αλυσίδας και θα χρησιμοποιήσουμε τα λήμματα 1 και 2 για να φράξουμε το χρόνο σύγκλισης. Για να δείξουμε αργή σύγκλιση αρκεί να βρεθεί ένα υποσύνολο του χώρου καταστάσεων με επαρκώς μικρή αγωγιμότητα. Για να δείξουμε ταχεία σύγκλιση πρέπει να αποδείξουμε ότι για κάθε υποσύνολο του χώρου καταστάσεων η αγωγιμότητα είναι αρκετά μεγάλη.

Η ανάλυση διαφοροποιείται για $\lambda < 1$, $1 < \lambda < 2$ και $\lambda \geq 2$.

Θεώρημα 34. Για κάθε δυαδικό δέντρο S ύψους n , και για κάθε $\lambda \geq 2$ ο χρόνος σύγκλισης της M_λ^S είναι πολωνυμικός στο n .

Απόδειξη. Πρώτα απ' όλα, θα εξετάσουμε την τεμπέλικη έκδοση της μαρκοβιανής αλυσίδας, δηλαδή σε κάθε βήμα, με πιθανότητα $1/2$ δεν κάνουμε τίποτα και με πιθανότητα $1/2$ ακολουθούμε τους κανόνες όπως στον ορισμό 41. Ο χρόνος σύγκλισης του P φράσσεται από το χρόνο σύγκλισης της τεμπέλικης έκδοσης. Η στάσιμη κατανομή είναι η ίδια. Η μαρκοβιανή αλυσίδα είναι χρονικά αναστρέψιμη, και το υποστηρίζον γράφημα είναι δέντρο με βάρη στις ακμές

$$w_{uv} = P_\lambda^S(u)p(u, v) = \frac{\lambda^{n-\text{depth}(u)}}{Z_\lambda^S} \cdot \frac{1}{6\lambda} = \frac{\lambda^{n-\text{depth}(u)-1}}{6Z_\lambda^S}$$

όταν u είναι ο γονέας του v .

Ισχυρισμός: Για κάθε $u \in V(S)$ η ποσότητα $\log(P_\lambda^S(u))^{-1}$ είναι πολωνυμική στο n .

Απόδειξη ισχυρισμού: Θεωρήστε το πλήρες πλήρες δυαδικό δέντρο T ύψους n . Ισχύει

$$\begin{aligned} \log(P_\lambda^S(u))^{-1} &\leq \log Z_\lambda^S = \log \sum_{u \in V(S)} \lambda^{n-\text{depth}(u)} \leq \\ \log \sum_{u \in V(T)} \lambda^{n-\text{depth}(u)} &= \log \sum_{i=0}^n 2^i \lambda^{n-i} \leq \log \sum_{i=0}^n \lambda^i \lambda^{n-i} = \\ \log(\lambda^n(n+1)) &= n \log \lambda + \log(n+1). \end{aligned}$$

Τώρα αρκεί να δείξουμε ότι το $1/\Phi(H)$ είναι πολυωνυμικό στο n .

Θα θεωρήσουμε όλα τα δυνατά $Y \subseteq V(S)$ με $0 \leq P_\lambda^S(Y) \leq 1/2$. Για καθένα από αυτά θα φράξουμε την ποσότητα $\Phi(Y) = \frac{\sum_{i \in Y, j \notin Y} w_{ij}}{\sum_{i \in Y} P_\lambda^S(i)}$.

Αν το Y είναι συνεκτικό και δεν περιέχει τη ρίζα του S , τότε είναι ένα υποδέντρο του S , με ρίζα ας πούμε u , και $P_\lambda^S(u) = \lambda^k/Z_\lambda^S$ για κάποιο $k \in \{0, \dots, n\}$. Έχουμε

$$\sum_{i \in Y, j \notin Y} w_{ij} \geq w_{u, \text{father}(u)} = \frac{\lambda^k}{6Z_\lambda^S}.$$

Έστω Y' το τέλει δυαδικό δέντρο με ρίζα u και ύψος k . Έχουμε

$$\begin{aligned} \sum_{i \in Y} P_\lambda^S(i) &\leq \sum_{i \in Y'} P_\lambda^S(i) = \sum_{j=0}^k \frac{\lambda^{k-j}}{Z_\lambda^S} \times 2^j \leq \\ \frac{\lambda^k(k+1)}{Z_\lambda^S} &\leq \frac{\lambda^k(n+1)}{Z_\lambda^S} \end{aligned}$$

όπου αυτό προκύπτει αν αθροίσουμε πάνω σε όλα τα επίπεδα του δέντρου Y' . Οπότε ισχύει

$$\frac{\sum w_{ij}}{\sum P_\lambda^S(i)} \geq \frac{\lambda^k}{6\lambda^k(n+1)} = \frac{1}{6(n+1)}$$

Αν Y είναι η ένωση δύο υποδέντρων του S , που δεν περιέχουν τη ρίζα του S , και η ρίζα του ενός είναι πρόγονος της ρίζας του άλλου, τότε τα ίδια επιχειρήματα ισχύουν, όπου τώρα παίρνουμε ως u τη ρίζα του πρώτου υποδέντρου.

Αν Y είναι η ένωση από m υποδέντρα που δεν περιέχουν τη ρίζα του S , για τα οποία ισχύει ότι κανενός η ρίζα δεν είναι πρόγονος της ρίζας κάποιου άλλου, τότε μπορούμε να αποδείξουμε παρόμοιο φράγμα ως εξής. Έστω Y_1, \dots, Y_m τα υποδέντρα, και έστων k_1, k_2, \dots, k_m , οι αντίστοιχοι εκθέτες στις πιθανότητες των ριζών αυτών, στη στάσιμη κατανομή. Τότε

$$\sum w_{ij} \geq (\lambda^{k_1} + \lambda^{k_2} + \dots + \lambda^{k_m})/6Z_\lambda^S$$

και

$$\sum_{i \in Y} P_\lambda^S(i) = \sum_{j=1 \dots m} \sum_{i \in Y_j} P_\lambda^S(i) \leq \sum_{j=1 \dots m} \lambda^{k_j}(n+1)/Z_\lambda^S$$

άρα

$$\frac{\sum w_{ij}}{\sum P_\lambda^S(i)} \geq \frac{Z_\lambda^S \sum_{j=1\dots m} \lambda^{k_j}}{6Z_\lambda^S(n+1) \sum_{j=1\dots m} \lambda^{k_j}} = \frac{1}{6(n+1)}.$$

Αν Y είναι ένα υποδέντρο του S που περιέχει την ρίζα του S , τότε το συμπλήρωμα του Y , δηλ το $S \setminus Y$ είναι ένωση από m υποδέντρα της προηγούμενης μορφής. Οπότε αν θεωρήσουμε Y_i, k_i όπως πριν, τότε

$$\sum w_{ij} = \sum_{j=1\dots m} \lambda^{k_j} / 6Z_\lambda^S$$

και αφού από την υπόθεση $P_\lambda^S(Y) \leq 1/2$, έχουμε

$$\sum_{i \in Y} P_\lambda^S(i) \leq \sum_{i \in S \setminus Y} P_\lambda^S(i) \leq \sum_{j=1\dots m} \lambda^{k_j}(n+1) / Z_\lambda^S$$

οπότε το ίδιο φράγμα ισχύει ξανά.

Τέλος παρόμοια επιχειρήματα συνεπάγονται το ίδιο φράγμα όταν το Y είναι αυθαίρετο υποσύνολο των κόμβων του S δηλ αυθαίρετη ένωση υποδέντρων του S .

Συνολικά έχουμε $1/\Phi(H) \leq 6(n+1)$. □

Θεώρημα 35. Για κάθε n και κάθε $1 < \lambda < 2$, υπάρχει ένα δέντρο ύψους n για το οποίο ο χρόνος σύγκλισης της M_λ^S είναι εκθετικός στο n .

Απόδειξη. Αρκεί να δείξουμε ότι για το πλήρες δυαδικό δέντρο T ύψους n , ο χρόνος σύγκλισης είναι εκθετικός στο n . Ωστόσο, τα ίδια επιχειρήματα ισχύουν και για άλλα δέντρα, π.χ. τα λεγόμενα "χριστουγεννιάτικα δέντρα". Έστω $Y \subset V(T)$ το αριστερό υποδέντρο του T . Θα δείξουμε ότι το $\Phi(Y)^{-1}$ είναι εκθετικό στο n . Έχουμε

$$Z_\lambda^T \sum_{u \in Y} P_\lambda^T(u) = Z_\lambda^T \sum_{u \in Y} \lambda^{n - \text{depth}(u)} = \sum_{i=0}^{n-1} 2^i \lambda^{n-i-1}$$

και

$$Z_\lambda^T \sum_{i \in Y, j \notin Y} w_{ij} = \lambda^{n-1} / 6$$

οπότε

$$\Phi(Y)^{-1} = \frac{\sum_{u \in Y} P_\lambda^T(u)}{\sum_{i \in Y, j \notin Y} w_{ij}} = 6 \sum_{i=0}^{n-1} \left(\frac{2}{\lambda}\right)^i = 6 \frac{\left(\frac{2}{\lambda}\right)^n - 1}{\frac{2}{\lambda} - 1}.$$

Εφόσον $1 < \lambda < 2$ είναι $2/\lambda > 1$ άρα η παραπάνω ποσότητα είναι εκθετική στο n , και άρα ο χρόνος σύγκλισης είναι επίσης εκθετικός στο n . □

Πόρισμα 9. Ο χρόνος σύγκλισης της M_λ^T παρουσιάζει αλλαγή φάσης στο $\lambda = 2$ από εκθετικό σε πολυωνυμικό.

Θεώρημα 36. Για κάθε n και κάθε $0 < \lambda < 1$, υπάρχει ένα δέντρο ύψους n για το οποίο ο χρόνος σύγκλισης της M_λ^S είναι εκθετικός στο n .

Απόδειξη. Θεωρούμε ξανά την τεμπέλικη εκδοχή της μαρκοβιανής αλυσίδας, και δείχνουμε ότι για το πλήρες δυαδικό δέντρο T ύψους n , ο χρόνος σύγκλισης είναι εκθετικός.

Για $u, v \in V(T)$ όπου u είναι ο γονέας του v , ισχύει

$$w_{uv} = \frac{\lambda^{n-\text{depth}(v)+1}}{6Z_\lambda^T}.$$

Έστω $Y \subset V(T)$ το αριστερό υποδέντρο του T .

$$Z_\lambda^T \sum_{u \in Y} P_\lambda^T(u) = Z_\lambda^T \sum_{u \in Y} \lambda^{n-\text{depth}(u)} = \sum_{i=0}^{n-1} 2^i \lambda^{n-i-1}$$

και

$$Z_\lambda^T \sum_{i \in Y, j \notin Y} w_{ij} = \lambda^n / 6$$

οπότε

$$\frac{1}{6} \Phi(T)^{-1} = \frac{1}{6} \frac{\sum_{u \in Y} P_\lambda^T(u)}{\sum_{i \in Y, j \notin Y} w_{ij}} = \left(\frac{1}{\lambda} + \frac{2}{\lambda^2} + \dots + \frac{2^{n-1}}{\lambda^n} \right) = \left(\frac{2}{\lambda} \right)^n \left(\frac{1}{2-\lambda} \right) - \left(\frac{1}{2-\lambda} \right).$$

Εφόσον $\lambda < 1 \Rightarrow 2/\lambda > 2$ η αντίστροφη αγωγιμότητα, και συνεπώς και ο χρόνος σύγκλισης, είναι εκθετικά στο n . \square

Θα αποδείξουμε ένα άλλο γεγονός που μας φαίνεται ενδιαφέρον. Αν και στη χειρότερη περίπτωση, δηλ. για το τέλειο δυαδικό δέντρο, καθώς και για ένα "χριστουγεννιάτικο δέντρο", ο χρόνος σύγκλισης υφίσταται μια αλλαγή φάσης στο $\lambda = 2$, η κατάσταση δεν είναι η ίδια για κάθε δέντρο. Συγκεκριμένα, για την άλλη ακραία περίπτωση του προβλήματος, δηλαδή για το μονοπάτι μήκους n , η αλλαγή φάσης από εκθετικό σε πολυωνυμικό χρόνο σύγκλισης εμφανίζεται στο $\lambda = 1$.

Πρόταση 7. Έστω S το μονοπάτι μήκους n , ο χρόνος σύγκλισης της M_λ^S υφίσταται αλλαγή φάσης στο $\lambda = 1$.

Απόδειξη. Για $\lambda = 1$ η Metropolis μαρκοβιανή αλυσίδα είναι ένας απλός τυχαίος περίπατος στους κόμβους του δέντρου. Είναι γνωστό ότι ο χρόνος σύγκλισης του τυχαίου περιπάτου σε μονοπάτι είναι πολυωνυμικός στο n .

Θα δείξουμε ότι για $\lambda < 1$ ο χρόνος σύγκλισης είναι εκθετικός.

Έστω $Y = S \setminus \{\text{root}(S)\}$.

$$\frac{1}{6} \Phi(Y)^{-1} = \frac{1}{6} \frac{\sum_{u \in Y} P_\lambda^S(u)}{\sum_{i \in Y, j \notin Y} w_{ij}} = \frac{1}{6} \frac{1 + \lambda + \dots + \lambda^{n-1}}{\lambda^n / 6} = \left(\frac{1}{\lambda} \right)^n \left(\frac{1}{1-\lambda} \right) - \left(\frac{1}{1-\lambda} \right).$$

Εφόσον $\lambda < 1 \Rightarrow 1/\lambda > 1$ η αντίστροφη αγωγιμότητα και συνεπώς και ο χρόνος σύγκλισης, είναι εκθετικά στο n . \square

Πόρισμα 10. Για κάθε S ύψους n και $0 < \lambda < 1$, ο χρόνος σύγκλισης της M_λ^S είναι εκθετικός στο n .

Απόδειξη. Έστω Y το αριστερό υποδέντρο του S , παρατηρούμε ότι το $\sum_{u \in Y} P_\lambda^S(u)$ είναι τουλάχιστον τόσο όσο για την προηγούμενη περίπτωση όπου S ήταν μονοπάτι μήκους n . \square

5.6 Η πολυπλοκότητα υπολογισμού του συντελεστή κανονικοποίησης

Η πολυπλοκότητα υπολογισμού του συντελεστή κανονικοποίησης εξαρτάται με πολύ ουσιαστικό τρόπο από το αν το ύψος του δέντρου είναι γνωστό ή όχι. Όταν λέμε ότι είναι γνωστό εννοούμε ότι δίνεται στην είσοδο, ενώ όταν δεν είναι γνωστό εννοούμε ότι δίνεται στην είσοδο ένα άνω φράγμα αυτού.

Ο αρχικός ορισμός του Size-of-Subtree υποθέτει ότι μας δίνεται ένα άνω φράγμα του ύψους του δέντρου, και αυτό το πρόβλημα αποδεικνύεται ότι είναι TotP-πλήρες υπό φειδωλές αναγωγές (βλ. κεφ. 2). Η δεύτερη εκδοχή του προβλήματος όπου δίνεται το ακριβές ύψος του δέντρου, είναι πάλι TotP-πλήρες, όμως υπό AP-αναγωγές. Αυτό μπορεί να το δει κανείς αν παρατηρήσει ότι το #IS ανάγεται με φειδωλές αναγωγές στο Size-of-Subtree όπου το δέντρο που προκύπτει μέσω της αναγωγής έχει ύψος n τόσο όσο και το πλήθος των κόμβων του γραφήματος που δίνεται ως είσοδος στο #IS: οι διακλαδώσεις αντιστοιχούν στην μη ντετερμινιστική επιλογή "παίρνω ή δεν παίρνω" τον τάδε κόμβο στο ανεξάρτητο σύνολο. Επειδή το #IS είναι TotP-πλήρες (και #P-πλήρες επίσης) υπό AP-αναγωγές, το ίδιο προκύπτει και για το Size-of-Subtree όταν δίνεται το ακριβές ύψος του δοσμένου δέντρου.

5.6.1 Όταν το ύψος είναι γνωστό

Θα αναλύσουμε πρώτα την πολυπλοκότητα υπολογισμού του Z_λ^S για την περίπτωση που το ακριβές ύψος του δέντρου είναι γνωστό. Αποδεικνύουμε ότι υπάρχει αλλαγή φάσης για κάποια τιμή του λ στο διάστημα $[1, 2]$. Για κάθε $\lambda \leq 1$ ο υπολογισμός του Z_λ^S είναι μη προσεγγίσιμος εκτός αν $NP=RP$. Αντιθέτως, για $\lambda \geq 2$ το Z_λ^S για οποιοδήποτε S επιδέχεται FPRAS. Ο ακριβής του υπολογισμός είναι αδύνατος για κάθε $\lambda > 0$ εκτός αν $NP=P$.

Θεώρημα 37. Για κάθε $\lambda > 0$ ο ακριβής υπολογισμός του Z_λ^S είναι αδύνατος (στη χειρότερη περίπτωση), εκτός αν $NP=P$ (ή $NP=RP$ για πιθανοτικό υπολογισμό). Επιπλέον για $\lambda \leq 1$ το Z_λ^S είναι μη προσεγγίσιμο με πολλαπλασιαστικό πολυωνυμικό σφάλμα εκτός αν $NP=RP$.

Απόδειξη. Έστω $\lambda > 0$, έστω S ένα μη κενό δέντρο δοσμένο ως είσοδος και n το ύψος του, επίσης δοσμένο ως είσοδος.

Θα ανάγουμε το πρόβλημα Size-of-Subtree με δοσμένο ύψος δέντρου, δλδ. τον υπολογισμό του μεγέθους ενός δέντρου $|S|$ ύψους n , ο οποίος είναι #P-complete

υπό AP-αναγωγές, στον υπολογισμό του $Z_\lambda^R = \sum_{u \in R} \lambda^{n-\text{depth}(u)}$ ενός δυαδικού δέντρου R . Η αναγωγή εμπλέκει τον υπολογισμό του Z_λ^R για πολυωνυμικά πολλά κατάλληλα ορισμένα δέντρα R , όχι μόνο για ένα.

Στα εξής τα λ και S θα είναι φελαρισμένα και θα παραλείπονται από τους δείκτες εκτός αν χρειάζεται.

Έστω m_i το πλήθος των κόμβων του S σε βάθος i , και έστω S_i το υποδέντρο του S που περιέχει όλους τους κόμβους μέχρι βάθος i . Έστω Z_i ο συντελεστής κανονικοποίησης που αντιστοιχεί στην $P_\lambda^{S_i}$. Δλδ.

$$Z_i = \sum_{u \in S_i} \lambda^{i-\text{depth}(u)}.$$

Για κάθε $i = 1, \dots, n$ ισχύει

$$Z_i = \lambda Z_{i-1} + m_i$$

και $Z_0 = 1$ οπότε

$$\begin{aligned} |S| &= m_1 + \dots + m_n = \\ &= (Z_\lambda^S - \lambda Z_{n-1}) + (Z_{n-1} - \lambda Z_{n-2}) + \dots + (Z_1 - \lambda Z_0) + Z_0 \Rightarrow \\ |S| &= Z_\lambda^S + (1 - \lambda) \sum_{i=0}^{n-1} Z_i. \end{aligned}$$

Αυτό ολοκληρώνει την απόδειξη ότι το Z_λ^S δεν μπορεί να υπολογιστεί ακριβώς εκτός αν $\text{NP}=\text{RP}$, αφού ο υπολογισμός του $|S|$ όταν το ύψος του S είναι γνωστό, είναι επίσης $\#P$ -complete υπό AP-αναγωγές. Έτσι αν μπορούσαμε να υπολογίσουμε ακριβώς το Z_λ^S για κάθε S , θα μπορούσαμε να υπολογίσουμε ακριβώς και το $|S|$, οπότε θα είχαμε $\text{NP}=\text{RP}$. Επιπλέον όμως ισχύει το ισχυρότερο αποτέλεσμα ότι αν $\text{NP} \neq \text{P}$ (αντίστοιχα $\text{NP} \neq \text{RP}$) τότε $\#IS$ δεν επιδέχεται FPTAS (αντίστοιχα FPRAS) [67, 25]. Οπότε παίρνουμε και το ισχυρότερο αποτέλεσμα ότι το Z_λ^S δεν μπορεί να υπολογιστεί ντετερμινιστικά ακριβώς εκτός αν $\text{NP}=\text{P}$.

Τώρα παρατηρήστε ότι αν $\lambda \leq 1$ τότε το $(1 - \lambda)$ είναι θετικό, οπότε ο υπολογισμός του $|S|$ στην παραπάνω αναγωγή είναι μια πρόσθεση θετικών ποσοτήτων. Ένα FPRAS για το Z_λ^S για κάθε δέντρο S συνεπάγεται έτσι ένα FPRAS για το $|S|$. Άρα ο υπολογισμός του Z_λ^S σε αυτή την περίπτωση είναι $\#P$ -hard υπό AP-αναγωγές.

Δεν ισχύει το ίδιο για $\lambda > 1 \Leftrightarrow (1 - \lambda) < 0$ διότι η αφαίρεση θετικών ποσοτήτων δεν διατηρεί το πολλαπλασιαστικό σφάλμα: το συνολικό σφάλμα μπορεί να είναι εκθετικά μεγάλο σε αυτή την περίπτωση. \square

Θεώρημα 38. Για $\lambda \geq 2$ ο υπολογισμός του Z_λ^S επιδέχεται FPRAS.

Απόδειξη. Αρκεί να προσεγγίσουμε την πιθανότητα της ρίζας του S , αφού είναι ίση με λ^n / Z_λ^S .

Προσεγγίζουμε την πιθανότητα της ρίζας τρέχοντας την μαρκοβιανή αλυσίδα και λαμβάνοντας δείγματα $m = \text{poly}(n)$ στο πλήθος.

Πολυωνυμικά πολλά δείγματα επαρκούν, επειδή η πιθανότητα της ρίζας είναι πάντα μεγαλύτερη από $1/(n+1)$: Θεωρήστε την πιθανότητα να βρίσκεται η αλυσίδα σε βάθος i του δέντρου, στη στάσιμη κατανομή. Αυτή η πιθανότητα είναι το πολύ $2^i \lambda^{n-i}$. Αφού $\lambda \geq 2$, η πιθανότητα της ρίζας είναι πάντα μεγαλύτερη από την πιθανότητα να βρίσκεται σε οποιοδήποτε άλλο βάθος. Όλα τα επίπεδα του δέντρου είναι $(n+1)$, έτσι έχουμε το συμπέρασμα. \square

Πόρισμα 11. Για $\lambda \geq 2$ ο υπολογισμός του Z_λ^S δεν είναι #P-complete κάτω από approximation preserving reductions, εκτός αν $NP=RP$.

Τώρα θα αποδείξουμε ότι για κάθε $\lambda \geq 1$, ασχέτως αν δεν είναι εφικτή η δειγματοληψία με τη χρήση της συγκεκριμένης μαρκοβιανής αλυσίδας τύπου Metropolis που αναλύσαμε σε αυτό το κεφάλαιο, εάν είναι εφικτή σε πολυωνυμικό χρόνο η δειγματοληψία (με οποιονδήποτε αλγόριθμο) σύμφωνα με την P_λ^R για κάθε δέντρο R , τότε μπορούμε να έχουμε FPRAS για τον υπολογισμό του Z_λ^S για κάθε S .

Θεώρημα 39. Για κάθε $\lambda \geq 1$ αν είναι εφικτή η δειγματοληψία σε πολυωνυμικό χρόνο σύμφωνα με την P_λ^S για οποιοδήποτε στιγμιότυπο S , τότε έχουμε FPRAS για το Z_λ^S για οποιοδήποτε στιγμιότυπο S .

Απόδειξη. Έστω $\lambda \geq 1$ και S ένα δυαδικό δέντρο ύψους n . Έστω $\forall i = 0, 1, \dots, n$ S_i το υποδέντρο του S που περιέχει όλους τους κόμβους μέχρι και βάθος i , και έστω $A_i = \sum_{u \in S_i} w(u)$ το άθροισμα των βαρών των κόμβων του S_i , όπου $w(u) = \lambda^{n-\text{depth}(u)}$. Οπότε $A_0 = \lambda^n$ και $A_n = Z_\lambda^S$.

Παρατηρούμε ότι

$$Z_\lambda^S = \frac{A_n}{A_{n-1}} \cdot \frac{A_{n-1}}{A_{n-2}} \cdot \dots \cdot \frac{A_2}{A_1} \cdot \frac{A_1}{A_0} \cdot A_0 \quad (5.1)$$

Για να προσεγγίσω το Z_λ^S αρκεί να μπορώ να προσεγγίσω τους λόγους $\frac{A_i}{A_{i+1}}$.

$$A_{i+1} = A_i + \sum_{\{u | \text{depth}(u)=i+1\}} w(u).$$

Το πλήθος των κόμβων σε βάθος $i+1$ είναι το πολύ 2 φορές το πλήθος των κόμβων σε βάθος μέχρι και i .

Το βάρος κάθε κόμβου σε βάθος $i+1$ είναι το πολύ ίσο με το βάρος οποιουδήποτε κόμβου σε βάθος μέχρι και i , αφού $\lambda \geq 1$.

$$\text{Άρα } \sum_{\{u | \text{depth}(u)=i+1\}} w(u) \leq 2A_i \Rightarrow A_{i+1} \leq 3A_i \Rightarrow \frac{A_i}{A_{i+1}} \geq \frac{1}{3}.$$

Τέλος αν θεωρήσουμε την κατανομή $P_\lambda^{S_{i+1}}$ πάνω στο δέντρο S_{i+1} , με $w_\lambda^{S_{i+1}}(u) = \lambda^{i+1-\text{depth}(u)}$, τότε έστω $\forall j = 0, 1, \dots, i+1$ $B_j = \sum_{u \in S_j} w_\lambda^{S_{i+1}}(u)$. Παρατηρούμε ότι για κάθε $j = 0, 1, \dots, i+1$ $A_j = B_j \cdot \lambda^k$ για κάποιο $k \in \mathbb{N}$, οπότε ισχύει

$$\frac{B_j}{B_{j+1}} = \frac{A_j}{A_{j+1}}.$$

Έτσι αν μπορούμε να κάνουμε δειγματοληψία σύμφωνα με την P_λ^S για κάθε S σε πολυωνυμικό χρόνο, τότε μπορούμε να προσεγγίσουμε κάθε λόγο $\frac{B_j}{B_{j+1}}$ με

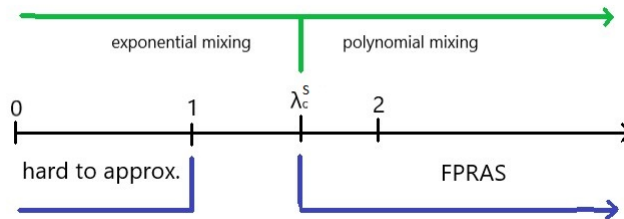
5.6. Η ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΥΠΟΛΟΓΙΣΜΟΥ ΤΟΥ ΣΥΝΤΕΛΕΣΤΗ ΚΑΝΟΝΙΚΟΠΟΙΗΣΗΣ 133

δειγματοληψία από την $P_\lambda^{S_{j+1}}$. Πολυωνμικά δείγματα αρκούν αφού κάθε τέτοιος λόγος είναι τουλάχιστον ίσος με $1/3$.

Κατ' επέκταση μπορούμε να προσεγγίσουμε τους λόγους $\frac{A_j}{A_{j+1}}$ και άρα και το Z_λ^S σύμφωνα με την εξίσωση [5.1](#). \square

Πόρισμα 12. Για κάθε δυαδικό δέντρο S , το Z_λ^S επιδέχεται FPRAS για κάθε $\lambda \geq \lambda_c^{mix} \geq 1$, όπου λ_{mix} είναι το σημείο αλλαγής φάσης του χρόνου σύγκλισης της αλυσίδας τύπου Metropolis του παρόντος κεφαλαίου.

Συνοπτικά τα αποτελέσματα όσον αφορά τις αλλαγές φάσης του χρόνου σύγκλισης της μαρκοβιανής αλυσίδας που παρουσιάσαμε και της πολυπλοκότητας προσέγγισης του Z_λ^S , παρουσιάζονται στο εξής διάγραμμα.



Θεώρημα 40. Αν $NP=RP$ τότε για κάθε $\lambda > 0$ και S το Z_λ^S υπολογίζεται με FPRAS.

Απόδειξη. Το ερώτημα "ποιό είναι το πλήθος των κόμβων ενός δέντρου S που βρίσκονται σε βάθος i ;" όταν δίνεται ως είσοδος το i , και το S σε συμπαγή αναπαράσταση, αποτελεί πρόβλημα στη #P. Άρα αν $NP=RP$, τότε δεδομένου του S , το πλήθος των κόμβων σε κάθε βάθος μπορεί να προσεγγιστεί με FPRAS, άρα και το Z_λ^S επίσης. \square

Πόρισμα 13. $NP=RP$ αν και μόνο αν $\exists \lambda \leq 1 \forall S$ το Z_λ^S επιδέχεται FPRAS. Επίσης $NP=RP$ αν και μόνο αν $\forall \lambda \leq 1 \forall S$ το Z_λ^S επιδέχεται FPRAS.

5.6.2 Όταν το ύψος δεν είναι γνωστό

Σε αυτή την υποενότητα αναλύουμε την πολυπλοκότητα για την περίπτωση που το ακριβές ύψος του δέντρου δεν είναι γνωστό, παρά μόνο ένα άνω φράγμα αυτού. Δείχνουμε ότι το πρόβλημα είναι #P-hard υπό Cook αναγωγές και μη προσεγγίσιμο για κάθε $\lambda > 0$, αλλά η ανάλυση διαφέρει για $\lambda \leq 1$ και $\lambda > 1$. Παρατηρούμε επίσης ότι το FPRAS της προηγούμενης υποενότητας δεν ισχύει αν το ακριβές ύψος n δεν είναι γνωστό.

Θεώρημα 41. Για κάθε $\lambda > 0$ ο υπολογισμός του Z_λ^S είναι #P-hard υπό Cook αναγωγές. Επιπλέον για $\lambda \leq 1$ το Z_λ^S είναι μη προσεγγίσιμο με πολλαπλασιαστικό πολυωνυμικό σφάλμα εκτός αν $NP=RP$.

Απόδειξη. Έστω $\lambda > 0$, έστω S ένα μη κενό δέντρο δοσμένο ως είσοδος και n' ένα άνω φράγμα για το ύψος του, επίσης δοσμένο ως είσοδος.

Θα ανάγουμε το πρόβλημα Size-of-Subtree, δλδ. τον υπολογισμό του μεγέθους ενός δέντρου $|S|$ ύψους το πολύ n' , ο οποίος είναι #P-complete υπό αναγωγές Cook, στον υπολογισμό του $Z_\lambda^R = \sum_{u \in R} \lambda^{n - \text{depth}(u)}$ ενός δυαδικού δέντρου R . Η αναγωγή εμπλέκει τον υπολογισμό του Z_λ^R για πολυωνυμικά πολλά κατάλληλα ορισμένα δέντρα R , όχι μόνο για ένα.

Στα εξής τα λ και S θα είναι φιξαρισμένα και θα παραλείπονται από τους δείκτες εκτός αν χρειάζεται.

Έστω ότι το ύψος του δέντρου είναι n . Το n δεν δίνεται, αλλά δείχνουμε στο τέλος της απόδειξης πώς μπορούμε να το ανακαλύψουμε.

Έστω m_i το πλήθος των κόμβων του S σε βάθος i , και έστω S_i το υποδέντρο του S που περιέχει όλους τους κόμβους μέχρι βάθος i . Έστω Z_i ο συντελεστής κανονικοποίησης που αντιστοιχεί στην $P_\lambda^{S_i}$. Δλδ.

$$Z_i = \sum_{u \in S_i} \lambda^{i - \text{depth}(u)}.$$

Για κάθε $i = 1, \dots, n$ ισχύει

$$Z_i = \lambda Z_{i-1} + m_i$$

και $Z_0 = 1$ οπότε

$$\begin{aligned} |S| &= m_1 + \dots + m_n = \\ &= (Z_\lambda^S - \lambda Z_{n-1}) + (Z_{n-1} - \lambda Z_{n-2}) + \dots + (Z_1 - \lambda Z_0) + Z_0 \Rightarrow \\ |S| &= Z_\lambda^S + (1 - \lambda) \sum_{i=0}^{n-1} Z_i. \end{aligned}$$

Μένει να δείξουμε πώς μπορούμε να ανακαλύψουμε το ακριβές ύψος n του S . Αρκεί να παρατηρήσουμε ότι για κάθε $i \geq n$ ισχύει $Z_i = Z_{i+1}$ και δεν ισχύει για κανένα $i < n$. Επομένως αν μπορούσαμε να υπολογίσουμε το Z_λ^R για κάθε δέντρο R ύψους το πολύ n' , θα μπορούσαμε να ανακαλύψουμε το ύψος του S βρίσκοντας για ποιά i ισχύει $Z_{i-1} \neq Z_i = Z_{i+1}$.

Αυτό ολοκληρώνει την απόδειξη ότι το Z_λ είναι #P-complete κάτω από Cook αναγωγές, αφού ο υπολογισμός του $|S|$ είναι επίσης #P-complete κάτω από Cook αναγωγές.

Για $\lambda \leq 1$ το Z_λ^S είναι μη προσεγγίσιμο, διότι το ίδιο συμβαίνει όταν γνωρίζουμε το n , οπότε αν είχαμε FPRAS μη γνωρίζοντας το n προφανώς θα είχαμε FPRAS και γνωρίζοντάς το. □

Θεώρημα 42. Για $\lambda > 1$ το Z_λ^S δεν επιδέχεται FPRAS (στη χειρότερη περίπτωση), εκτός αν $NP=RP$.

Απόδειξη. Ανάγουμε το SAT στον υπολογισμό του Z_λ^S . Για κάθε τύπο boolean με n μεταβλητές, κατασκευάζουμε μια συνοπτική περιγραφή ενός δέντρου S , έτσι ώστε αν μπορούσαμε να προσεγγίσουμε το Z_λ^S τότε θα μπορούσαμε να αποφασίσουμε με μεγάλη πιθανότητα αν ο τύπος είναι ικανοποιήσιμος ή όχι.

Υπάρχει μια τετριμμένη NPTM M για το SAT: το αντίστοιχο δέντρο στην είσοδο ϕ είναι ένα πλήρες δυαδικό δέντρο ύψους n . Κάθε φύλλο αντιστοιχεί σε μια ανάθεση στις μεταβλητές n και επιστρέφει "ναι" αν η ανάθεση ικανοποιεί τη φόρμουλα. Ορίζουμε μια άλλη NPTM M' που προσομοιώνει τη M και αν το M επιστρέφει "ναι" τότε η M' σταματά, αλλιώς η M' κάνει άλλες n μη ντετερμινιστικές επιλογές (δηλαδή άλλα 2^n δυνατά μονοπάτια) και σταματά. Αυτός ο υπολογισμός ορίζει ένα δέντρο που αποτελείται από ένα πλήρες δυαδικό δέντρο ύψους n από κάποια φύλλα του οποίου κρέμονται μερικά ακόμη πλήρη δυαδικά δένδρα ύψους n .

Οι μη ικανοποιήσιμοι τύποι αντιστοιχούν στο πλήρες δυαδικό δένδρο ύψους n , που συμβολίζουμε με T , ενώ οι ικανοποιήσιμες που έχουν ακριβώς μία ικανοποιητική ανάθεση, αντιστοιχούν σε ένα δέντρο ύψους $2n$, που συμβολίζουμε με S , αποτελούμενο από το πλήρες δυαδικό δένδρο ύψους n με ένα άλλο πλήρες δυαδικό δέντρο ύψους n να κρέμεται από ένα φύλλο του πρώτου.

Αφού $\lambda > 1$ ισχύει

$$Z_\lambda^S = Z_\lambda^T + \lambda^n Z_\lambda^T - \lambda^n = Z_\lambda^T + \lambda^n (Z_\lambda^T - 1) \Rightarrow \\ Z_\lambda^S \geq 2Z_\lambda^T - 1$$

Άρα αν μπορούσαμε να προσεγγίσουμε το Z_λ^R για κάθε R , τότε θα μπορούσαμε να διακρίνουμε μεταξύ των S και T , άρα θα μπορούσαμε επίσης να αποφασίσουμε αν η δοσμένη φόρμουλα είναι ικανοποιήσιμη ή όχι.

Αν η φόρμουλα έχει περισσότερες από μία ικανοποιητικές αναθέσεις, τότε ο συντελεστής κανονικοποίησης για το αντίστοιχο δέντρο θα ήταν ακόμα μεγαλύτερος από το Z_λ^S , οπότε το ίδιο επιχείρημα θα ίσχυε ξανά. \square

Πόρισμα 14. Μια οικογένεια δύσκολων στιγμιοτύπων για την προσέγγιση του Z_λ^S , για $\lambda > 1$, είναι η οικογένεια δέντρων που για κάθε n ένα δέντρο ύψους $2n$ αποτελείται από ένα πλήρες δυαδικό δέντρο ύψους n από κάποια φύλλα του οποίου κρέμονται μερικά ακόμη πλήρη δυαδικά δένδρες ύψους n .

Απόδειξη. Προκύπτει από την προηγούμενη απόδειξη. \square

Θεώρημα 43. Αν $NP=RP$ τότε για κάθε λ και S το Z_λ^S υπολογίζεται με FPRAS.

Απόδειξη. Το ερώτημα "ποιοί είναι το πλήθος των κόμβων ενός δέντρου S που βρίσκονται σε βάθος i ;" όταν δίνεται ως είσοδος το i , και το S σε συμπαγή αναπαράσταση, αποτελεί πρόβλημα στη #P. Άρα αν $NP=RP$, τότε δεδομένου του S , το πλήθος των κόμβων σε κάθε βάθος μπορεί να προσεγγιστεί με FPRAS, άρα και το Z_λ^S επίσης. \square

Πόρισμα 15. $NP=RP$ αν και μόνο αν $\exists \lambda > 0 \forall S$ το Z_λ^S επιδέχεται FPRAS. Επίσης $NP=RP$ αν και μόνο αν $\forall \lambda > 0 \forall S$ το Z_λ^S επιδέχεται FPRAS.

5.7 Συζήτηση

Ο αλγόριθμος τύπου Metropolis για το μοντέλο μας επιδεικνύει μια διαφορετική συμπεριφορά για $\lambda \leq 1$ και $\lambda > 1$. Στην πρώτη περίπτωση έχει τάση προς τα κάτω, δηλαδή για οποιαδήποτε ακμή η πιθανότητα να μετάβασης από πάνω προς τα κάτω είναι μεγαλύτερη από την πιθανότητα μετάβασης από κάτω προς τα πάνω. Στη δεύτερη περίπτωση ($\lambda > 1$) το αντίθετο ισχύει. Αυτό αρχικά οδήγησε στην εικασία ότι η αλλαγή φάσης θα έπρεπε να εμφανιστεί στο $\lambda = 1$. Πράγματι, ο χρόνος σύγκλισης αυτής της μαρκοβιανής αλυσίδας είναι εκθετικός για όλα τα δέντρα για $\lambda < 1$.

Ωστόσο, όπως φαίνεται, η αλλαγή φάσης εξαρτάται από το δέντρο. Για το τέλει δυαδικό δέντρο έχουμε μια μετάβαση από εκθετικό σε πολυωνυμικό χρόνο σύγκλισης στο $\lambda = 2$, ενώ για το μονοπάτι ύψους n η μετάβαση συμβαίνει στο $\lambda = 1$. Επίσης, για τις δύσκολες περιπτώσεις του Size of-Subtree, η μετάβαση συμβαίνει επίσης στο $\lambda = 2$.

Μια δεύτερη παρατήρηση είναι ότι ο χρόνος σύγκλισης του αλγορίθμου τύπου Metropolis για το μοντέλο tree-depth στο διάστημα $(0, \infty) \setminus (1, 2)$, μετάβαίνει από εκθετικό σε πολυωνυμικό, και αυτό συμπίπτει με τη μετάβαση ως προς την πολυπλοκότητα προσέγγισης του Z_λ^S (όταν το ύψος του δέντρου είναι γνωστό) από NP-hard σε προσεγγίσιμο με FPRAS. Με άλλα λόγια ο αλγόριθμος Metropolis αντιπροσωπεύει κατά κάποιο τρόπο την πολυπλοκότητα της προσέγγισης της partition function αυτού του μοντέλου στο διάστημα $(0, \infty) \setminus (1, 2)$. (Αυτό είναι κάτι που δεν ισχύει γενικά για οποιοδήποτε πρόβλημα σταθμισμένης μέτρησης).

Όμως παρατηρούμε ότι ίδιος αλγόριθμος δεν είναι αντιπροσωπευτικός της πολυπλοκότητας για διάφορα εύκολα στιγμιότυπα του προβλήματος, όπως είναι τα μονοπάτια, για τα οποία το Z_λ^S μπορεί να υπολογιστεί εύκολα για κάθε $\lambda > 0$, ενώ η μαρκοβιανή αλυσίδα συγκλίνει σε εκθετικό χρόνο για $\lambda < 1$.

Εξάλλου αποτελεί ανοιχτό ερώτημα η πολυπλοκότητα προσέγγισης του Z_λ^S στη χειρότερη περίπτωση, για $\lambda \in (1, 2)$ και όταν το ύψος δεν είναι γνωστό, όπως είναι ανοιχτό ερώτημα και το ακριβές σημείο όπου συμβαίνει αλλαγή φάσης.

Οπότε το μεγάλο ερώτημα είναι κατά πόσο ο αλγόριθμος τύπου Metropolis έχει κάποια ενδογενή σχέση με το πρόβλημα ώστε να είναι αντιπροσωπευτικός της πολυπλοκότητας για τα δύσκολα στιγμιότυπα του προβλήματος. Εάν αποδειχθεί ότι είναι αντιπροσωπευτικός και ότι μια ενδογενής σχέση όντως υπάρχει, τότε $\text{NP} \neq \text{RP}$. (Το τελευταίο ισχύει επειδή αν $\text{NP} = \text{RP}$ τότε για κάθε $\lambda > 0$ το πρόβλημα θα έπρεπε να προσεγγίζεται εύκολα, αλλά για $\lambda < 1$ η αλυσίδα Metropolis συγκλίνει σε εκθετικό χρόνο.)

Ένα άλλο ζήτημα ενδιαφέροντος είναι το κατά πόσο για σταθμισμένα αθροίσματα ισχύει η ισοδυναμία μεταξύ σταθμισμένης δειγματοληψίας και σταθμισμένης μέτρησης. Για μη σταθμισμένα προβλήματα η σχεδόν ομοιόμορφη δειγματοληψία είναι ισοδύναμη με προσεγγιστική μέτρηση [69]. Είναι εύκολο να γενικεύσουμε την μία πλευρά του θεωρήματος του [69] ως εξής. Αν ένα πρόβλημα σταθμισμένου αθροίσματος είναι πολυωνυμικά αυτοαναγόμενο, τότε η ύπαρξη FPRAS για το πρόβλημα συνεπάγεται δειγματοληψία σε πολυωνυμικό χρόνο της αντίστοι-

χης κατανομής. Το αντίθετο όμως δεν ισχύει όπως προκύπτει από τα αποτελέσματά μας, διότι για παράδειγμα για κάθε $\lambda > 0$ το Z_λ^S όταν το ύψος του δέντρου δεν είναι γνωστό δεν επιδέχεται FPRAS, παρ' όλα αυτά για $\lambda \geq 2$ η δειγματοληψία είναι εφικτή μέσω της μαρκοβιανής αλυσίδας που παρουσιάσαμε.

5.7.1 Ανοιχτά προβλήματα

Για $\lambda \in (1, 2)$ ποιά είναι η πολυπλοκότητα προσέγγισης του Z_λ^S στη χειρότερη περίπτωση, όταν το ύψος του δέντρου δεν είναι γνωστό; Ποιά είναι μια οικογένεια δύσκολων στιγμιοτύπων για αυτήν την περίπτωση;

Είναι ο υπολογισμός του Z_λ^S AP-αλληλοαναγόμενος με το #SAT, με το #BIS, (ή με κανένα από τα δύο);

5.7.2 Σχετικές εργασίες

Σχετικά με την TotP, ιδιότητες και πληρότητα, δείτε το κεφάλαιο 1. Σχετικά με προβλήματα σταθμισμένης μέτρησης, μαρκοβιανές αλυσίδες και αλλαγές φάσης δείτε επίσης στο κεφάλαιο 1. Σχετικά με το Size-of-Subtree δείτε τις σχετικές εργασίες στο κεφάλαιο 4.

Βιβλιογραφία

- [1] Dimitris Achlioptas: Random Satisfiability. *Handbook of Satisfiability 2009*: 245-270
- [2] Dimitris Achlioptas, Amin Coja-Oghlan, Federico Ricci-Tersenghi: On the solution-space geometry of random constraint satisfaction problems. *Random Struct. Algorithms* 38(3): 251-268 (2011)
- [3] Dimitris Achlioptas, Cristopher Moore: Random k-SAT: Two Moments Suffice to Cross a Sharp Threshold. *SIAM J. Comput.* 36(3): 740-762 (2006)
- [4] Dimitris Achlioptas, Federico Ricci-Tersenghi: Random Formulas Have Frozen Variables. *SIAM J. Comput.* 39(1): 260-280 (2009)
- [5] Mikhail Alekhnovich and Eli Ben-Sasson. Linear upper bounds for random walk on small density random 3-CNFs. *SIAM J. Comput.*, 36(5):1248–1263, (2007)
- [6] Carme Alvarez, Birgit Jenner: A Very Hard log-Space Counting Class. *Theor. Comput. Sci.* 107(1): 3-30 (1993)
- [7] Andris Ambainis, Martins Kokainis: Quantum algorithm for tree size estimation, with applications to backtracking and 2-player games. *STOC 2017*: 989-1002
- [8] Marcelo Arenas, Martin Muñoz, Cristian Riveros: Descriptive Complexity for counting complexity classes. *LICS 2017*: 1-12
- [9] Sanjeev Arora, Boaz Barak: *Computational Complexity - A Modern Approach*. Cambridge University Press 2009, ISBN 978-0-521-42426-4, pp. I-XXIV, 1-579
- [10] Eleni Bakali: On Markov chains for #Clustered-Monotone-SAT and other hard counting problems with easy decision version, *Inter. Jour. Sci. Engin. Research* 9(3): 1203-1211 (2018)
- [11] Eleni Bakali, Aggeliki Chalki, Aris Pagourtzis, Petros Pantavos, Stathis Zachos: Completeness Results for Counting Problems with Easy Decision. *CIAC 2017*: 55-66

- [12] Evangelos Bampas, Andreas-Nikolas Göbel, Aris Pagourtzis, Aris Tentes: On the connection between interval size functions and path counting. In Proc. of TAMC'09, LNCS 5532: 108–117, Springer, 2009.
- [13] Evangelos Bampas, Andreas-Nikolas Göbel, Aris Pagourtzis, Aris Tentes: On the connection between interval size functions and path counting. *Computational Complexity* 26(2): 421-467 (2017)
- [14] Jean Barbier, Florent Krzakala, Lenka Zdeborova and Pan Zhang : The hardcore model on random graphs revisited. *J. Phys.: Conf. Ser.* 473 : 012021 (2013)
- [15] Gleb Belov, Samuel Esler, Dylan Fernando, Pierre Le Bodic, George L. Nemhauser: Estimating the size of search trees by sampling with domain knowledge. *IJCAI 2017*: 473-479
- [16] Nayantara Bhatnagar, Allan Sly, Prasad Tetali: Reconstruction Threshold for the Hardcore Model. *APPROX-RANDOM 2010*: 434-447
- [17] Magnus Bordewich: On the Approximation Complexity Hierarchy. *WAOA 2010*: 37-46
- [18] G. Brightwell and P. Winkler: Hard constraints and the Bethe lattice: adventures at the interface of combinatorics and statistical physics. In Proc. Int'l. Congress of Mathematicians, volume III : 605–624 (2002)
- [19] Andrei A. Bulatov, Víctor Dalmau, Marc Thurley: Descriptive complexity of approximate counting CSPs. *CSL 2013*: 149-164
- [20] Peter C. Cheeseman, Bob Kanefsky, William M. Taylor: Where the Really Hard Problems Are. *IJCAI 1991*: 331-340
- [21] Pang C. Chen: Heuristic Sampling: A Method for Predicting the Performance of Tree Searching Programs. *SIAM J. Comput.* 21(2): 295-315 (1992)
- [22] Víctor Dalmau: Linear datalog and bounded path duality of relational structures. *Logical Methods in Computer Science* 1(1) (2005)
- [23] Holger Dell, John Lapinskas: Fine-grained reductions from approximate counting to decision. *CoRR abs/1707.04609* (2017)
- [24] Martin E. Dyer: Approximate counting by dynamic programming. *STOC 2003*: 693-699
- [25] Martin E. Dyer, Alan M. Frieze, Mark Jerrum: On Counting Independent Sets in Sparse Graphs. *SIAM J. Comput.* 31(5): 1527-1541 (2002)
- [26] Martin E. Dyer, Alan M. Frieze, Ravi Kannan: A Random Polynomial Time Algorithm for Approximating the Volume of Convex Bodies. *J. ACM* 38(1): 1-17 (1991)

- [27] Martin E. Dyer, Leslie Ann Goldberg, Catherine S. Greenhill, Mark Jerrum: The Relative Complexity of Approximate Counting Problems. *Algorithmica* 38(3): 471-500 (2004)
- [28] Stephen A. Fenner, Lance Fortnow, Stuart A. Kurtz: Gap-Definable Counting Classes. *J. Comput. Syst. Sci.* 48(1): 116-148 (1994)
- [29] Martin Fürer, Shiva Prasad Kasiviswanathan: An Almost Linear Time Approximation Algorithm for the Permanent of a Random (0-1) Matrix. *FSTTCS 2004*: 263-274
- [30] Andreas Galanis, Leslie Ann Goldberg, Mark Jerrum: Approximately Counting H-Colourings is # BIS -Hard. *ICALP (1) 2015*: 529-541
- [31] Gallavotti, G. (1999), *Statistical mechanics, Texts and Monographs in Physics*, Berlin: Springer-Verlag, ISBN 3-540-64883-6, MR 1707309
- [32] Stuart Geman, Donald Geman: Stochastic Relaxation, Gibbs Distributions, and the Bayesian Restoration of Images. *IEEE Trans. Pattern Anal. Mach. Intell.* 6(6): 721-741 (1984)
- [33] Leslie Ann Goldberg, Mark Jerrum: The Complexity of Ferromagnetic Ising with Local Fields. *Combinatorics, Probability and Computing* 16(1): 43-61 (2007)
- [34] Oded Goldreich: *Computational complexity - a conceptual perspective*. Cambridge University Press 2008, ISBN 978-0-521-88473-0, pp. I-XXIV, 1-606
- [35] Carla P. Gomes, Ashish Sabharwal, Bart Selman: Model Counting: A New Strategy for Obtaining Good Bounds. *AAAI 2006*: 54-61
- [36] Parikshit Gopalan, Adam R. Klivans, Raghu Meka, Daniel Stefankovic, Santosh Vempala, Eric Vigoda: An FPTAS for # Knapsack and Related Counting Problems. *FOCS 2011*: 817-826
- [37] Parikshit Gopalan, Raghu Meka, Omer Reingold: DNF sparsification and a faster deterministic counting algorithm. *Computational Complexity* 22(2): 275-310 (2013)
- [38] Hastings, W.: Monte Carlo sampling methods using Markov chains and their application. *Biometrika*, 57: 97-109 (1970)
- [39] Lane A. Hemaspaandra, Christopher M. Homan, Sven Kosub, Klaus W. Wagner: The Complexity of Computing the Size of an Interval. *SIAM J. Comput.* 36(5): 1264-1300 (2007)
- [40] Russell Impagliazzo, William Matthews, Ramamohan Paturi: A satisfiability algorithm for AC0. *SODA 2012*: 961-972

- [41] Russell Impagliazzo, Ramamohan Paturi, Francis Zane: Which Problems Have Strongly Exponential Complexity? *J. Comput. Syst. Sci.* 63(4): 512-530 (2001)
- [42] Ising, E. *Z. Physik* (1925) 31: 253. <https://doi.org/10.1007/BF02980577>
- [43] Mark Jerrum, Alistair Sinclair: The Markov chain Monte-Carlo method: an approach to approximate counting and integration. *Approximation Algorithms for NP-hard Problems* (Dorit Hochbaum, ed.), PWS, : 482–520 (1996)
- [44] Mark Jerrum, Alistair Sinclair: Approximating the Permanent. *SIAM J. Comput.* 18(6): 1149-1178 (1989)
- [45] Mark Jerrum, Alistair Sinclair, Eric Vigoda: A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries. *J. ACM* 51(4): 671–697 (2004)
- [46] Richard M. Karp, Michael Luby, Neal Madras: Monte-Carlo Approximation Algorithms for Enumeration Problems. *J. Algorithms* 10(3): 429-448 (1989)
- [47] Aggelos Kiayias, Aris Pagourtzis, Kiron Sharma, Stathis Zachos: Acceptor-Definable Counting Classes. *Panhellenic Conference on Informatics 2001*: 453-463
- [48] Aggelos Kiayias, Aris Pagourtzis, Kiron Sharma, Stathis Zachos: The complexity of determining the order of solutions. In *Proceedings of the First Southern Symposium on Computing*, Hattiesburg, Mississippi, 1998
- [49] Aggelos Kiayias, Aris Pagourtzis, Stathis Zachos: Cook reductions blur structural differences between functional complexity classes. *Panhellenic Logic Symposium 1999*: 132-137
- [50] Philip Kilby, John K. Slaney, Sylvie Thiébaux, Toby Walsh: Estimating Search Tree Size. *AAAI 2006*: 1014-1019
- [51] Donald E. Knuth. 1974. Estimating the Efficiency of Backtrack Programs. Technical Report. Stanford University, Stanford, CA, USA.
- [52] Johannes Köbler, Uwe Schöning, Jacobo Torán: On Counting and Approximation. *Acta Inf.* 26(4): 363-379 (1989)
- [53] Florent Krzakala, Andrea Montanari, Federico Ricci-Tersenghi, Guilhem Semerjian, and Lenka Zdeborová: Gibbs states and the set of solutions of random constraint satisfaction problems. *Proc. Natl. Acad. Sci. USA*, 104(25):10318–10323 (electronic) (2007)

- [54] Frank R. Kschischang, Brendan J. Frey, Hans-Andrea Loeliger: Factor graphs and the sum-product algorithm. *IEEE Trans. Information Theory* 47(2): 498-519 (2001)
- [55] David A. Levin, Yuval Peres, Elizabeth L. Wilmer: Markov chains and mixing times. AMS (2009), Electronic ISBN: 978-1-4704-1204-3
- [56] László Lovász, Santosh Vempala: Simulated annealing in convex bodies and an $O^*(n^4)$ volume algorithm. *J. Comput. Syst. Sci.* 72(2): 392-417 (2006)
- [57] Michael Luby and Boban Velickovic. On deterministic approximation of DNF. *Algorithmica*, 16(4/5):415–433 (1996)
- [58] Martinelli, F. and Olivieri, E.: Approach to equilibrium of Glauber dynamics in the one phase region. I. The attractive case. *Communications in Mathematical Physics*, 161(3): 447-486, (1994)
- [59] Nicholas Metropolis, Arianna W. Rosenbluth, Marshall N. Rosenbluth, Augusta H. Teller, and Edward Teller: Equations of state calculations by fast computing machines. *J. Chem. Phys.*, 21(6): 1087–1092 (1953)
- [60] David G. Mitchell, Bart Selman, Hector J. Levesque: Hard and Easy Distributions of SAT Problems. *AAAI 1992*: 459-465
- [61] Aris Pagourtzis: On the complexity of hard counting problems with easy decision version. 3rd Panhellenic Logic Symposium 2001
- [62] Aris Pagourtzis, Stathis Zachos: The Complexity of Counting Functions with Easy Decision Version. *MFCS 2006*: 741-752
- [63] Christos H. Papadimitriou: *Computational Complexity*. Addison-Wesley, 1994
- [64] Peierls, R. : On Ising's model of ferromagnetism. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32(3): 477-481 (1936)
- [65] Paul Walton Purdom Jr.: Tree Size by Partial Backtracking. *SIAM J. Comput.* 7(4): 481-491 (1978)
- [66] Sanjeev Saluja, K. V. Subrahmanyam, Madhukar N. Thakur: Descriptive Complexity of #P Functions. *J. Comput. Syst. Sci.* 50(3): 493-505 (1995)
- [67] Alistair Sinclair, CS294 Markov Chain Monte Carlo: Foundations and Applications, lecture notes, Fall 2009, <https://people.eecs.berkeley.edu/sinclair/cs294/f09.html>
- [68] Alistair Sinclair, CS271 Randomness and Computation, lecture notes, Fall 2011, <https://people.eecs.berkeley.edu/sinclair/cs271/n10.pdf>

- [69] Alistair Sinclair, Mark Jerrum: Approximate Counting, Uniform Generation and Rapidly Mixing Markov Chains. *Inf. Comput.* 82(1): 93-133 (1989)
- [70] Alan D. Sokal: Chromatic polynomials, Potts models and all that. *Physica A: Statistical Mechanics and its Applications*, 279(1): 324–332 (2000)
- [71] Larry J. Stockmeyer: On Approximation Algorithms for #P. *SIAM J. Comput.* 14(4): 849-861 (1985)
- [72] Marc Thurley: An Approximation Algorithm for #k-SAT. *STACS 2012*: 78-87
- [73] Seinosuke Toda: PP is as Hard as the Polynomial-Time Hierarchy. *SIAM J. Comput.* 20(5): 865-877 (1991)
- [74] Patrick Traxler: The Relative Exponential Time Complexity of Approximate Counting Satisfying Assignments. *Algorithmica* 75(2): 339-362 (2016).
- [75] Radislav Vaisman and Dirk P. Kroese: Stochastic Enumeration Method for Counting Trees. *Methodol. Comput. Appl. Probab.* 19(1): 31-73 (2017)
- [76] Leslie G. Valiant: The Complexity of Computing the Permanent. *Theor. Comput. Sci.* 8: 189-201 (1979)
- [77] Leslie G. Valiant: The Complexity of Enumeration and Reliability Problems. *SIAM J. Comput.* 8(3): 410-421 (1979)
- [78] Leslie G. Valiant, Vijay V. Vazirani: NP is as Easy as Detecting Unique Solutions. *Theor. Comput. Sci.* 47(3): 85-93 (1986)
- [79] Dror Weitz: Counting independent sets up to the tree threshold. *STOC 2006*: 140-149
- [80] D. J. Welsh and C. Merino: The Potts model and the Tutte polynomial. *Journal of Mathematical Physics*, 41(3):1127–1152 (2000)
- [81] Ryan Williams: Improving Exhaustive Search Implies Superpolynomial Lower Bounds. *SIAM J. Comput.* 42(3): 1218-1244 (2013)
- [82] Ryan Williams: Algorithms for Circuits and Circuits for Algorithms. *IEEE Conference on Computational Complexity 2014*: 248-261
- [83] F.-Y. Wu: The Potts model. *Reviews of modern physics*, 54(1):235 (1982)
- [84] David Zuckerman: On Unapproximable Versions of NP-Complete Problems. *SIAM J. Comput.* 25(6): 1293-1304 (1996)