

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ
ΕΠΙΣΤΗΜΩΝ

Η Αλλαγή Φάσης στο Τυχαίο Πρόβλημα K-SAT

Διπλωματική Εργασία

Νίκου Γεωργουδιού

Επιβλέπων

Μιχαήλ Λουλάκης, Καθηγητής ΣΕΜΦΕ

Τριμελής Επιτροπή

Μιχαήλ Λουλάκης, Καθηγητής ΣΕΜΦΕ
Αριστέιδης Παγουρτζής, Καθηγητής ΣΗΜΜΥ
Πέτρος Στεφανέας, Καθηγητής ΣΕΜΦΕ



Αθήνα 2022

Περίληψη

Ένα στιγμιότυπο του τυχαίου προβλήματος K-SAT με N μεταβλητές και M περιορισμούς είναι με ψηλή πιθανότητα ικανοποιήσιμο αν ο λόγος $\alpha = M/N$ επαληθεύει $\alpha < 2^K \log 2 - \frac{1}{2}(1 + \log 2) + o_K(1)$, ενώ είναι με ψηλή πιθανότητα μη ικανοποιήσιμο για τιμές του α πάνω από αυτό το κατώφλι. Στην παρούσα εργασία θα χρησιμοποιήσουμε την ευρετική μέθοδο Cavity της στατιστικής φυσικής για να εκτιμήσουμε το παραπάνω κατώφλι, ενώ θα δούμε επίσης πως η μέθοδος αυτή έχει εμπνεύσει την απόδειξη αυτής της εικασίας.

Λέξεις κλειδιά: Ικανοποιησιμότητα, K-SAT, Αλλαγή Φάσης, Μέθοδος Cavity, Belief Propagation, Survey Propagation, Πολυπλοκότητα Μέσης Περίπτωσης

Abstract

An instance of the random K-SAT problem with N variables and M constraints is with high probability satisfiable if the quotient $\alpha = M/N$ satisfies $\alpha < 2^K \log 2 - \frac{1}{2}(1 + \log 2) + o_K(1)$, and with high probability unsatisfiable for values of α above this threshold. In this thesis, we are going to conjecture the existence and value of the above threshold via the non-rigorous and heuristic Cavity Method, and we will explore the connection between this method and the rigorous proof of the conjecture.

Keywords: Satisfiability, K-SAT, Phase Transition, Cavity Approach, Belief Propagation Survey Propagation, Average Case Complexity

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής αυτής εργασίας κύριο Λουλάκη Μιχαήλ, ο οποίος με έφερε σε επαφή με το παρόν θέμα και την πλούσια και ιδιαίτερα ενδιαφέρουσα σχετική βιβλιογραφία, ενώ μου πρόσφερε επίσης πολύτιμη βοήθεια και καθοδήγηση κατά τη διάρκεια εκπόνησης της.

Θα ήθελα επίσης να ευχαριστήσω ιδιαίτερα την οικογένεια μου για την στήριξη που μου παρείχε καθ' όλη τη διάρκεια των προπτυχιακών σπουδών μου.

Νίκος Γεωργουδίδης

© (2022) Εθνικό Μετσόβιο Πολυτεχνείο. All rights Reserved. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς το συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σ' αυτό το έγγραφο εκφράζουν το συγγραφέα και δεν πρέπει να ερμηνευτεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περιεχόμενα

Εισαγωγή	2
0.1 Ορισμός και Ιστορική Αναδρομή του Προβλήματος	2
0.2 Μοντέλα Γραφημάτων Παραγόντων	6
0.3 Η Μέθοδος RS Cavity και ο Αλγόριθμος Belief Propagation	8
1 Αλγόριθμοι για το Πρόβλημα SAT και η Μέθοδος 1RSB Cavity	14
1.1 Ο Αλγόριθμος Warning Propagation για το Πρόβλημα SAT	14
1.2 Η Μέθοδος RS Cavity και ο Αλγόριθμος Belief Propagation για το Πρόβλημα SAT	18
1.3 Η Μέθοδος 1RSB Cavity και ο Αλγόριθμος Survey Propagation για το Πρόβλημα SAT	22
1.4 Οι Αλγόριθμοι WID και SID για την Εύρεση Satisfying Assignments .	29
2 Η Εκτίμηση του Κατωφλιού Ικανοποίησης για το Τυχαίο Πρόβλημα K-SAT	31
2.1 Η Συνάρτηση Πολυπλοκότητας του Αλγορίθμου Survey Propagation .	31
2.2 Αριθμητική Εκτίμηση του Κατωφλιού Ικανοποίησης για μικρά K	37
2.3 Η Εικασία του Κατωφλιού Ικανοποίησης	40
2.4 Η Απόδειξη της Εικασίας	45

Εισαγωγή

0.1 Ορισμός και Ιστορική Αναδρομή του Προβλήματος

Στην εισαγωγική αυτή ενότητα θα ορίσουμε το τυχαίο πρόβλημα SAT και θα παρουσιάσουμε της φάσεις που προβλέπει η μέθοδος Cavity για τον χώρο λύσεων αυτού. Θα δώσουμε επίσης ένα ιστορικό σχεδιάγραμμα της εξέλιξης το προβλήματος εύρεσης του κατωφλιού ικανοποιησιμότητας. Αρχίζουμε με τον ορισμό του προβλήματος SAT.

Ορισμός 1. Έστω X ένα σύνολο από N το πλήθος μεταβλητές και έστω επίσης M το πλήθος περιορισμοί (διαζεύξεις) των λογικών αυτών μεταβλητών καθώς και των αρνήσεων τους. Το πρόβλημα SAT είναι ο προσδιορισμός της ύπαρξης ή μη μιας ανάθεσης αληθοτιμών των N μεταβλητών ώστε κάθε διάζευξη να ικανοποιείται, δηλαδή να λάβει την τιμή Αληθής. Αν αυτή υπάρχει, το αντίστοιχο στιγμιότυπο του προβλήματος ονομάζεται *Satisfiable* (Ικανοποίηση) και η αντίστοιχη ανάθεση *Satisfying Assignment*. Αν κάθε περιορισμός περιέχει σταθερό πλήθος μεταβλητών ίσο με K , τότε αναφερόμαστε στο $K - SAT$.

Για παράδειγμα, το στιγμιότυπο

$$(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (\neg x_1 \vee \neg x_3)$$

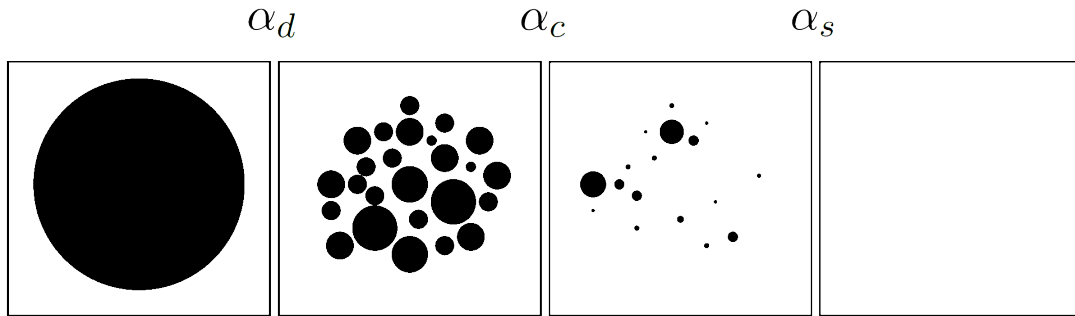
είναι ικανοποιήσιμο στιγμιότυπο του προβλήματος 2-SAT με $N = 3$ μεταβλητές και $M = 4$ περιορισμούς, και μια ανάθεση που ικανοποιεί όλους τους περιορισμούς είναι η

$$x_1 : \text{Ψευδής} \quad x_2 : \text{Ψευδής} \quad x_3 : \text{Αληθής}$$

Από εδώ και στο εξής θεωρούμε την αντιστοιχία

$$0 \rightarrow \text{Αληθής} \quad 1 \rightarrow \text{Ψευδής}$$

Το τυχαίο πρόβλημα $K - SAT$ διαφέρει στο ότι δεδομένων των N, M , για κάθε περιορισμό επιλέγουμε τυχαία και ομοιόμορφα K από τις N μεταβλητές και έπειτα επιλέγουμε



Σχήμα 1: Οι Φάσεις του τυχαίου προβλήματος K-SAT [1]

τυχαία και ομοιόμορφα τα πρόσημα τους, δηλαδή αν στον περιορισμό θα εμφανίζονται με ή χωρίς άρνηση.

Έστω τώρα $\alpha = \frac{M}{N}$. Το τυχαίο πρόβλημα K-SAT υπόκειται σε αλλαγή φάσης. Καθώς $N \rightarrow \infty$ παρατηρείται η ύπαρξη ενός κρίσιμου σημείου $\alpha_s = \alpha_s(K)$ τέτοιο, ώστε ένα στιγμιότυπο του τυχαίου προβλήματος K-SAT να είναι ασυμπτωτικά στο N σχεδόν βέβαια ικανοποιήσιμο για $\alpha < \alpha_s$ ενώ σχεδόν βέβαια μη ικανοποιήσιμο για $\alpha > \alpha_s$. Συγκεκριμένα, η μέθοδος Cavity προβλέπει τις εξής φάσεις.

- $0 < \alpha < \alpha_d$: Replica Symmetric Phase
Στην φάση αυτή έχουμε πολλές λύσεις του αντίστοιχου στιγμιότυπου K-SAT και δεν έχουμε συσχετίσεις μεγάλης απόστασης. Συγκεκριμένα, περιμένουμε ότι η αληθοτιμές δύο μεταβλητών του ίδιου περιορισμού στα Satisfying Assignments να είναι σχεδόν ασυσχέτιστες αν αυτός ο περιορισμός δεν υπήρχε, όπως θα δούμε παρακάτω.
- $\alpha_d < \alpha < \alpha_c$: Dynamic Replica Symmetry Breaking Phase
Στην φάση αυτή έχουμε εκθετικό πλήθος συστάδων λύσεων με εκθετικά μικρό κλάσμα των Satisfying Assignments σε κάθε μια από αυτές. Συστάδες λύσεων είναι υποσύνολα του συνόλου λύσεων, τα στοιχεία του οποίου έχουν μικρή απόσταση Hamming, δηλαδή αναθέσεις αληθοτιμών που διαφέρουν σε λίγες θέσεις. Λύσεις διαφορετικών συστάδων διαφέρουν σε πολλές θέσεις. Συσχετίσεις μεγάλων αποστάσεων είναι μικρές.
- $\alpha_c < \alpha < \alpha_s$: Static Replica Symmetry Breaking Phase
Στην φάση αυτή έχουμε εκθετικό πλήθος συστάδων λύσεων, αλλά ορισμένες από αυτές περιέχουν σταθερό κλάσμα των Satisfying Assignments, με αποτέλεσμα να έχουμε συσχετίσεις μεγάλης απόστασης.
- $\alpha > \alpha_s$: UNSAT Phase
Στην φάση αυτή δεν έχουμε πλέον Satisfying Assignments. Το κατώφλι α_s είναι το κατώφλι ικανοποιησιμότητας.

Σημαντικό ρόλο στην εύρεση φραγμάτων για το α_s , αλλά και τον ασυμπτωτικό προσδιορισμό του, έπαιξαν οι μέθοδοι της πρώτης και δεύτερης ροπής, τις οποίες δίνουμε παρακάτω:

Λήμμα 1 (Μέθοδος Πρώτης Ροπής). Έστω X μια μη αρνητική τυχαία μεταβλητή που παίρνει ακέραιες τιμές, τότε

$$\mathbb{P}[X > 0] \leq \mathbb{E}[X] \quad (1)$$

Λήμμα 2 (Μέθοδος Δεύτερης Ροπής). Έστω X μια μη αρνητική τυχαία μεταβλητή που παίρνει ακέραιες τιμές, τότε

$$\mathbb{P}[X > 0] \geq \frac{\mathbb{E}[X]^2}{\mathbb{E}[X^2]} \quad (2)$$

Η μέθοδος πρώτης ροπής είναι συμπέρασμα της ανισότητας Markov με την παρατήρηση ότι για μη αρνητικές ακέραιες μεταβλητές είναι $\mathbb{P}[X > 0] = \mathbb{P}[X \geq 1] < \frac{\mathbb{E}[X]}{1}$ ενώ η μέθοδος δεύτερης ροπής προκύπτει αν εφαρμόσουμε την ανισότητα Cauchy, η οποία δίνει $\mathbb{E}[X] = \mathbb{E}[X \mathbb{1}\{X > 0\}] \leq \mathbb{E}[X^2]^{1/2} \mathbb{P}[X > 0]^{1/2}$.

Το 1982 οι Franco και Paull [2] έδειξαν μέσω της μεθόδου πρώτης ροπής ότι ένα στιγμιότυπο του τυχαίου προβλήματος K-SAT είναι σχεδόν βέβαια μη ικανοποιήσιμο αν $\alpha > 2^k \log 2$, δίνοντας ένα άνω φράγμα για το α_s . Το επιχείρημα τους ήταν το εξής: Κάθε περιορισμός ικανοποιείται με πιθανότητα $1 - 2^{-K}$, οπότε το αναμενόμενο πλήθος από Satisfying Assignments ισούται με $2^N (1 - 2^{-K})^{\alpha N}$ το οποίο είναι τάξης $o(1)$ για $\alpha > 2^k \log 2$.

Το 1990 οι Chao και Franco [3] έδωσαν έναν αλγόριθμο, ο οποίος σε γραμμικό χρόνο εντοπίζει με γνήσια θετική πιθανότητα ένα Satisfying Assignment για $\alpha < \frac{2^k}{K}$, δίνοντας ένα κάτω φράγμα για το α_s .

Το 1992 ο Goerdts [4] απέδειξε ότι για το τυχαίο 2-SAT το όριο ικανοποίησης είναι $\alpha_s(2) = 1$, ενώ αριθμητική παρατήρηση της ύπαρξης του κατωφλιού ικανοποίησης για $K = 3$ είχε γίνει το 1994 από τους Kirkpatrick και Selmon [5] οι οποίοι επίσης παρατήρησαν την ύπαρξη «δύσκολων στιγμιότυπων» κοντά στο κατώφλι.

Το 1997 οι Dubois και Boufkhad [6] βελτίωσαν το άνω φράγμα και έδειξαν, επίσης με εφαρμογή της μεθόδου πρώτης ροπής, ότι $\alpha_s \leq 2^k \log 2 - \frac{1 + \log 2}{2} - o(1)$.

Το 1999, ο Friedgut [7] απέδειξε το εξής βασικό θεώρημα, στο οποίο στηρίχτηκαν επόμενα αποτελέσματα.

Θεώρημα 1 (Friedgut). Έστω $P_N(K, \alpha)$ η πιθανότητα ένα στιγμιότυπο του τυχαίου προβλήματος K -SAT με N μεταβλητές και αN περιορισμούς να είναι ικανοποιήσιμο, τότε υπάρχει ακολουθία $\alpha_c^{(N)}(K)$ τέτοια ώστε, για κάθε $\varepsilon > 0$

$$\lim_{N \rightarrow \infty} P_N(K, \alpha) = \begin{cases} 1, & \text{αν } \alpha < \alpha_c^{(N)}(K) - \varepsilon \\ 0, & \text{αν } \alpha > \alpha_c^{(N)}(K) + \varepsilon \end{cases}$$

Δηλαδή, η μετάβαση από την φάση ικανοποιησιμότητας στη φάση μη ικανοποιησιμότητας γίνεται ολόένα και πιο απότομη. Για την εικασία του κατωφλιού ικανοποίησης, ωστόσο, χρειάζεται επίσης η $\alpha_c^{(N)}(K)$ να συγχλίνει.

Το 2002, οι Achlioptas και Moore [8] εφάρμοσαν την μέθοδο δεύτερης ροπής πάνω σε Satisfying Assignments, η άρνηση των οποίων είναι επίσης Satisfying Assignment και βελτίωσαν το κάτω φράγμα, δείχνοντας ότι $\alpha_s \leq 2^{K-1} \log 2 - \frac{1+\log 2}{2} - o(1)$. Μια χρονιά αργότερα οι Achlioptas και Peres [9] βελτίωσαν περαιτέρω το κάτω φράγμα, εφαρμόζοντας την μέθοδο δεύτερης ροπής πάνω σε ισορροπημένα Satisfying Assignments, τα οποία δηλαδή ικανοποιούν περίπου τις μισές των kM συνολικών εμφανίσεων των μεταβλητών στο στιγμιότυπο. Το αποτέλεσμα τους ήταν ότι $\alpha_s \geq 2^K \log 2 - (K+1) \frac{\log 2}{2} - 1 - o(1)$, το οποίο μαζί με το παραπάνω άνω φράγμα δίνει ότι το α_s είναι της τάξης $\alpha_s = 2^K \log 2 + O(K)$. Θα χρησιμοποιήσουμε το αποτέλεσμα αυτό ως αφετηρία στην παρουσίαση της εικασίας. Το 2006 οι Achlioptas και Ricci-Tersenghi [10] απέδειξαν τη ύπαρξη συστάδων στο τυχαίο K -SAT για $K \geq 8$.

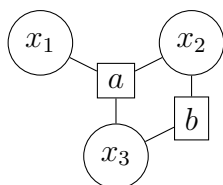
Το 2002 οι Mezard και Zecchina [11] εφάρμοσαν την μέθοδο 1RSB Cavity στο τυχαίο πρόβλημα K -SAT και εισήγαγαν τον αλγόριθμο Survey Propagation, ενώ το 2006 οι Mertens, Mezard και Zecchina [12] εκτίμησαν μέσω αυτού το όριο ικανοποίησης ίσο με $\alpha_s = 2^K \log 2 - \frac{1-\log 2}{2} - o_K(1)$. Η εικασία αυτή θα αποτελέσει το κύριο μέρος της εργασίας.

Το 2014, οι Coja Oghlan και Panagiotou [13] απέδειξαν την παραπάνω εικασία. Εμπνευσμένοι από την μέθοδο 1RSB Cavity εφάρμοσαν την μέθοδο δεύτερης ροπής πάνω σε 'καλύμματα' από Satisfying Assignments, τα οποία θα ορίσουμε αργότερα.

Τέλος, το 2022 οι Ding, Sly και Sun [1] γενίκευσαν το παραπάνω αποτέλεσμα, δείχνοντας ότι ισχύει γενικότερα για $K \geq K_0$, όπου K_0 επαρκώς μεγάλο.

0.2 Μοντέλα Γραφημάτων Παραγόντων

Στην παράγραφο αυτή θα ορίσουμε αρχικά τα μοντέλα γραφημάτων παραγόντων στην γενική τους μορφή και θα τα χρησιμοποιήσουμε στη συνέχεια για να απεικονίσουμε στιγμιότυπα του προβλήματος SAT. Η απεικόνιση αυτή θα είναι πολύ εύχρηστη στον ορισμό της μεθόδου Cavity και των σχετικών αλγορίθμων στο επόμενο κεφάλαιο.



Σχήμα 2: Απεικόνιση μιας κατανομής της μορφής $p(x_1, x_2, x_3) = \psi_a(x_1, x_2, x_3)\psi_b(x_2, x_3)$

Ορίζουμε τώρα τα μοντέλα γραφημάτων παραγόντων.

Έστω μια συνάρτηση πυκνότητας πιθανότητας $p(x)$, όπου x διάνυσμα τυχαίων μεταβλητών, η οποία παραγοντοποιείται ως εξής:

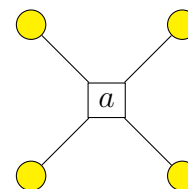
$$p(x) = \frac{1}{Z} \prod_{a \in A} \psi_a(x_a) \quad (3)$$

όπου ψ_a συναρτήσεις που εξαρτώνται μόνο από ένα υποσύνολο x_a των μεταβλητών του x .

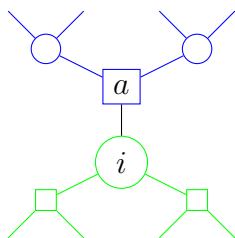
Μια τέτοια κατανομή μπορεί να απεικονιστεί μέσω ενός διμερούς γραφήματος $G(A, V, E)$ όπου A και V είναι σύνολα κορυφών και E είναι σύνολο ακμών ως εξής:

Σε κάθε παράγοντα αντιστοιχούμε μια κορυφή $a \in A$ και σε κάθε μεταβλητή αντιστοιχούμε μια κορυφή $i \in V$. Ενώνουμε με ακμή τις $a \in A$ και $i \in V$ αν και μόνο αν ψ_a εξαρτάται από την μεταβλητή i .

Για κάθε μεταβλητή $i \in V$, το σύνολο $V(i)$ αποτελείται από τις κορυφές παραγόντων του A που συνορεύουν στο i . Αντίστοιχα ορίζονται τα $V(a)$ για $a \in A$. Ειδικότερα, αν το G είναι δέντρο, για κάθε ακμή $ia \in E$ ορίζουμε τα υπόδεντρα $T_{i \rightarrow a}, T_{a \rightarrow i}$ του G που προκύπτουν αν από το δέντρο αφαιρέσουμε την ακμή ia και πάρουμε την συνιστώσα που περιέχει το i και a αντίστοιχα.



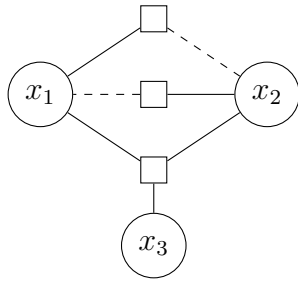
Σχήμα 3: Το σύνολο $V(a)$ (χίτρινο)



Σχήμα 4: Τα υπόδεντρα $T_{i \rightarrow a}$ (πράσινο) και $T_{a \rightarrow i}$ (μπλε)

Για ένα στιγμιότυπο του προβλήματος SAT, μπορούμε τώρα να απεικονίσουμε την ομοιόμορφη κατανομή πάνω στα Satisfying Assignments. Αν Z είναι το πλήθος αυτών, και A το σύνολο περιορισμών, τότε η κατανομή αυτή γράφεται στην μορφή (3) ως εξής:

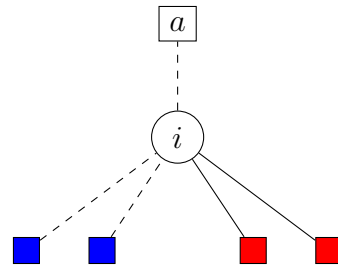
$$p(x) = \frac{1}{Z} \prod_{a \in A} \mathbb{1}\{a \text{ satisfied}\} \quad (4)$$



Σχήμα 5: Απεικόνιση του στιγμιότυπου SAT $(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2) \wedge (x_1 \vee x_2 \vee x_3)$

Επομένως μπορεί κανείς να απεικονίσει ένα στιγμιότυπο του προβλήματος SAT μέσω ενός γραφήματος παραγόντων, εισάγοντας διακεκομμένες ακμές στην περίπτωση που η άρνηση μιας μεταβλητής εμφανίζεται σε έναν περιορισμό. Θα κλείσουμε την σύντομη αυτή εισαγωγή με ορισμούς ποσοτήτων που θα χρησιμοποιούμε στη συνέχεια. Από εδώ και στο εξής, θα χρησιμοποιήσουμε τις έννοιες του στιγμιότυπου και του γραφήματος του εναλλασσόμενα, πχ όταν λέμε «περιορισμός» θα εννοούμε στο γράφημα την αντίστοιχη κορυφή του και αντίστροφα.

Για a κορυφή του γραφήματος, ήδη ορίσαμε $V(a)$ το σύνολο των κορυφών που είναι γειτονικοί της a , όπου a μπορεί να είναι παράγοντας ή μεταβλητή. Με $V_+(a)$ και $V_-(a)$ συμβολίζουμε αντίστοιχα τους θετικούς και αρνητικούς γείτονες του a . Για κάθε ακμή $i - a$ ορίζουμε $V_a^u(i)$ και $V_a^s(i)$ τους γείτονες του i εκτός από τον a στους οποίους το i εμφανίζεται με το αντίθετο, αντίστοιχα ίδιο πρόσημο με τον περιορισμό a . Ο βαθμός μιας κορυφής i συμβολίζεται n_i . Τέλος, ορίζουμε J_i^a το αντίθετο πρόσημο της ακμής ia . Έτσι είναι $J_i^a = -1$ για πλήρη ακμή και $J_i^a = 1$ για διακεκομμένη ακμή.



Σχήμα 6: Τα σύνολα $V_a^s(i)$ (μπλε) και $V_a^u(i)$ (κόκκινο) για $i - a$ διακεκομμένη ακμή, $n_i = 5$

0.3 Η Μέθοδος RS Cavity και ο Αλγόριθμος Belief Propagation

Στην τρίτη αυτή εισαγωγική ενότητα θα παρουσιάσουμε την μέθοδο Cavity, η οποία εκφράζεται μέσω του αλγόριθμου Belief Propagation, και θα δούμε πως μέσω αυτής μπορούμε να εκτιμήσουμε τις περιθώριες κατανομές των μεταβλητών μιας κατανομής $P(X) = \frac{1}{Z} \prod_{a \in A} \psi_a(x_a)$, όπως ορίσαμε στην προηγούμενη ενότητα, καθώς και την σταθερά κανονικοποίησης της Z . Εάν το αντίστοιχο γράφημα παραγόντων της κατανομής είναι δέντρο, τότε τα αποτελέσματα είναι ακριβή. Εάν το γράφημα είναι τοπικά δέντρο, και οι συσχετίσεις μεγάλης απόστασης είναι πολύ μικρές, τότε η μέθοδος μπορεί να χρησιμοποιηθεί για εκτίμηση, χωρίς όμως να υπάρχει εγγύηση ορθότητας. Στο κεφάλαιο αυτό, υποθέτουμε ότι δουλεύουμε με γραφήματα δέντρων, και θα ακολουθήσουμε το σχεδιάγραμμα απόδειξης που περιγράφεται στο [14].

Κύριο συστατικό του αλγόριθμου είναι τα μηνύματα $\mu_{i \rightarrow a}(x_i), \mu_{a \rightarrow i}(x_i)$ κατά μήκος των ακμών $ia \in E$ και προς τις δύο κατευθύνσεις, τα οποία ορίζονται ως εξής:

- $\mu_{i \rightarrow a}(x_i)$ είναι η κατανομή της μεταβλητής i στο υπογράφημα που προκύπτει αν αφαιρέσουμε τον περιορισμό a . Για δέντρα αυτό θα είναι το $T_{i \rightarrow a}$.
- $\mu_{a \rightarrow i}(x_i)$ είναι η αναμενόμενη τιμή του $\psi_a(x_a)$ εάν η μεταβλητή i λάβει την τιμή x_i .

Ο αλγόριθμος Belief Propagation αρχικοποιεί τυχαία τα μηνύματα αυτά και σε κάθε επανάληψη τα ενημερώνει ως εξής:

$$\begin{aligned}
 & \bullet \mu_{i \rightarrow a}(x_i) \cong \prod_{b \in V(i) \setminus a} \mu_{b \rightarrow i}(x_i) \\
 & \text{Αν } V(i) \setminus a = \emptyset \text{ τότε } \mu_{i \rightarrow a}(x_i) \text{ είναι ομοιόμορφη κατανομή} \\
 & \bullet \mu_{a \rightarrow i}(x_i) = \sum_{x_a \setminus x_i} \psi_a(x_a) \prod_{j \in V(a) \setminus i} \mu_{j \rightarrow a}(x_j) \\
 & \text{Αν } V(a) \setminus i = \emptyset \text{ τότε } \mu_{a \rightarrow i}(x_i) = \psi_a(x_i)
 \end{aligned} \tag{5}$$

Το παρακάτω θεώρημα συνοψίζει τα αποτελέσματα αυτής της ενότητας.

Θεώρημα 2. Έστω κατανομή $P(X) = \frac{1}{Z} \prod_{a \in A} \psi_a(x_a)$ το γράφημα παραγόντων της οποίας είναι δέντρο. Τότε:

- Ο αλγόριθμος Belief Propagation συγκλίνει σε ένα μοναδικό σύνολο σταθερών μηνυμάτων $\{\mu_{a \rightarrow i}^*(x_i), \mu_{i \rightarrow a}^*(x_i)\}_{ia \in E}$.

ii) Η κατανομή της x_i ισούται με:

$$p_i(x_i) \cong \prod_{b \in V(i)} \mu_{b \rightarrow i}^*(x_i) \quad (6)$$

iii) Η σταθερά κανονικοποίησης Z ικανοποιεί:

$$\log Z = \sum_{a \in A} \log c_a + \sum_{i \in V} \log c_i - \sum_{ia \in E} \log c_{ia} \quad (7)$$

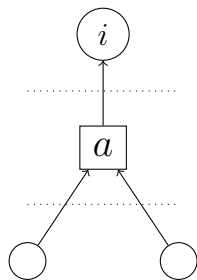
όπου

$$\begin{aligned} c_i &= \log \left(\sum_{x_i} \prod_{b \in V(i)} \mu_{b \rightarrow i}^*(x_i) \right) \\ c_a &= \log \left(\sum_{x_a} \psi_a(x_a) \prod_{i \in V(a)} \mu_{i \rightarrow a}^*(x_i) \right) \\ c_{ia} &= \log \left(\sum_{x_i} \mu_{i \rightarrow a}^*(x_i) \mu_{a \rightarrow i}^*(x_i) \right) \end{aligned} \quad (8)$$

Θα αποδείξουμε το παραπάνω θεώρημα μέσω μιας σειράς ισχυρισμών.

Ισχυρισμός 1. Τα μηνύματα $\mu_{a \rightarrow i}$ (αντίστοιχα $\mu_{j \rightarrow b}$) συγκλίνουν μετά από $r + 1$ επαναλήψεις, όπου r είναι το βάθος του υπόδεντρου $T_{a \rightarrow i}$ (αντίστοιχα $T_{j \rightarrow b}$).

Απόδειξη. Χωρίς βλάβη της γενικότητας μελετάμε μηνύματα από παράγοντες σε μεταβλητές. Το ζητούμενο προκύπτει επαγωγικά ως εξής:



$r = k + 1$

$r = k$

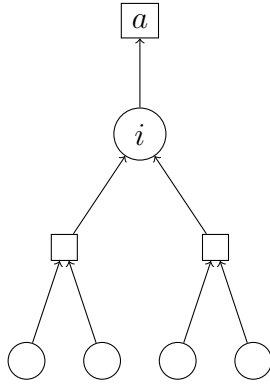
Μηνύματα από φύλλα σε γονείς τους είναι εξ ορισμού σταθερά, άρα για $r = 0$ έχουμε σύγκλιση σε μία επανάληψη. Αν τώρα το ζητούμενο ισχύει για όλα τα μηνύματα μέχρι και βάθους k και μία ακμή $a - i$ είναι τέτοια ώστε $T_{a \rightarrow i}$ έχει βάθος $k + 1$. Επειδή τα υπόδεντρα $T_{j \rightarrow a}$ για $j \in V(a) \setminus i$ έχουν βάθος $\leq k$ με ένα τουλάχιστον να έχει βάθος ακριβώς k , τα μηνύματα $\mu_{j \rightarrow a}$ θα έχουν όλα συγκλίνει μετά από $k + 1$ επαναλήψεις. Επειδή το $\mu_{a \rightarrow i}$ εξαρτάται μόνο από αυτά, θα έχει συγκλίνει μετά από $k + 2$ επαναλήψεις. \square

Για τους επόμενους ισχυρισμούς, υποθέτουμε ότι τα μηνύματα έχουν συγκλίνει.

Ισχυρισμός 2. Το μήνυμα $\mu_{i \rightarrow a}$ ισούται με την κατανομή της μεταβλητής i στο $T_{i \rightarrow a}$, αγνοώντας την σταθερά κανονικοποίησης.

Απόδειξη. Θα αποδείξουμε το ζητούμενο επίσης με επαγωγή στο βάθος r του υπόδεικτου. Οι περιπτώσεις $r = 0, r = 1$ είναι τετριμμένες και δίνουμε το επαγωγικό βήμα. Θεωρούμε $X_{i \rightarrow a}$ τις μεταβλητές του $T_{j \rightarrow b}$ εκτός τις j και $A_{j \rightarrow b}$ τους παράγοντες του $T_{i \rightarrow a}$, για κάθε $(j, b) \in E$. Θεωρούμε για το επαγωγικό βήμα ακμή (ia) τέτοια ώστε το $T_{i \rightarrow a}$ έχει βάθος $r = k + 2$.

Η κατανομή της x_i στο $T_{i \rightarrow a}$, έστω $p_{i \rightarrow a}(x_i)$, επαληθεύει



$$\begin{aligned}
 p_{i \rightarrow a}(x_i) &= \sum_{X_{i \rightarrow a}} \prod_{b \in A_{i \rightarrow a}} \psi_b(x_b) \\
 &= \sum_{X_{i \rightarrow a}} \prod_{b \in V(i) \setminus a} \psi_b(x_b) \prod_{j \in V(b) \setminus i} \prod_{c \in A_{j \rightarrow b}} \psi_c(x_c) \\
 &\cong \prod_{b \in V(i) \setminus a} \sum_{x_b} \psi_b(x_b) \prod_{j \in V(b) \setminus i} \sum_{X_{j \rightarrow b}} \prod_{c \in A_{j \rightarrow b}} \psi_c(x_c) \\
 &\cong \prod_{b \in V(i) \setminus a} \sum_{x_b} \psi_b(x_b) \prod_{j \in V(b) \setminus i} \mu_{j \rightarrow b}(x_j) \\
 &\cong \mu_{i \rightarrow a}(x_i)
 \end{aligned}$$

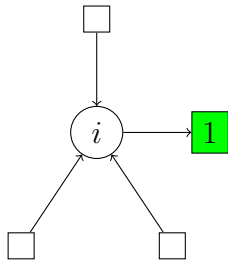
Το οποίο ολοκληρώνει την απόδειξη. □

Ισχυρισμός 3. Η κατανομή $p(x_i)$ της x_i ισούται με:

$$p(x_i) = \frac{1}{c_i} \prod_{b \in V(i)} \mu_{b \rightarrow i}(x_i)$$

όπου $c_i = \sum_{x_i} \prod_{b \in V(i)} \mu_{b \rightarrow i}(x_i)$ σταθερά κανονικοποίησης.

Απόδειξη.



Η απόδειξη προκύπτει άμεσα από τον προηγούμενο ισχυρισμό αν θεωρήσουμε έναν επιπλέον σταθερό και μοναδιαίο παράγοντα ο οποίος πάντα ικανοποιείται και ενώνεται με το i . Ένας τέτοιος παράγοντας προφανώς δεν μεταβάλλει την κατανομή $P(X)$, αλλά ούτε τα μηνύματα του γραφήματος, καθώς αυτός εξ ορισμού στέλνει μοναδιαίο μήνυμα στο i . Το μήνυμα $\mu_{i \rightarrow 1}$ τώρα ισούται και με τα δύο μέλη της παραπάνω εξίσωσης. □

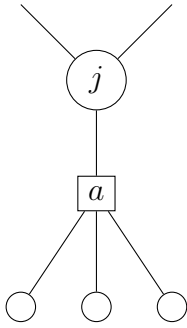
Ισχυρισμός 4. Η απο κοινού πιθανότητα των μεταβλητών του μοντέλου γράφεται επίσης:

$$p(x) = \prod_{a \in A} p_a(x_a) \prod_{i \in V} p_i(x_i)^{1-n_i} \quad (9)$$

όπου $p_a(x_a)$ η απο κοινού πιθανότητα των μεταβλητών που συμμετέχουν στον περιορισμό a .

Απόδειξη.

Θα αποδείξουμε το ζητούμενο με επαγωγή στο πλήθος των παραγόντων. Αν το μοντέλο μας αποτελείται από έναν μόνο παράγοντα, το αποτέλεσμα είναι τετριμμένο. Θεωρούμε τώρα ένα μοντέλο με $M + 1$ παράγοντες. Επειδή αυτό είναι δέντρο, θα υπάρχει ένας παράγοντας a ο οποίος, εκτός από μία μεταβλητή j , θα συνορεύει μόνο σε φύλλα.



Έστω G το γράφημα μας και G' το γράφημα που προκύπτει αν τώρα αφαιρέσουμε τον παράγοντα a και τους γειτονικούς του κόμβους εκτός τον j . Αν X οι μεταβλητές του G' και X οι μεταβλητές του G , τότε για την κατανομή του X ισχύει:

$$P(X) = p_a(x_a|G')P(G') = p_a(x_a|x_j)P(G')$$

Η επαγωγική υπόθεση και ο νόμος Bayes δίνουν:

$$\begin{aligned} P(X) &= p_a(x_a|x_j) \prod_{b \in G'} p_b(x_b) \prod_{i \in G'} p_i(x_i)^{1-\tilde{n}_i} \\ &= \frac{p(x_j|x_a)p_a(x_a)}{p_j(x_j)} \prod_{b \in G'} p_b(x_b) \prod_{i \in G'} p_i(x_i)^{1-\tilde{n}_i} \end{aligned}$$

Όπου \tilde{n}_i είναι ο βαθμός της κορυφής i στο G' . Για την μεταβλητή j αυτός είναι κατά ένα μεγαλύτερος στο G ενώ για τις υπόλοιπες γειτονικές μεταβλητές του a ο βαθμός θα είναι 1. Επειδή το x_j είναι συνιστώσα του x_a , το ζητούμενο έπεται.

□

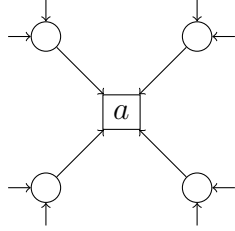
Ισχυρισμός 5. Ως προς τα μηνύματα *Belief Propagation* είναι:

$$p_a(x_a) = \frac{1}{c_a} \psi_a(x_a) \prod_{i \in V(a)} \mu_{i \rightarrow a}(x_i)$$

όπου c_a σταθερά κανονικοποίησης ίση με:

$$c_a = \sum_{x_a} \psi_a(x_a) \prod_{i \in V(a)} \mu_{i \rightarrow a}(x_i)$$

Απόδειξη.



Εργαζόμαστε ανάλογα όπως στον Ισχυρισμό 3. Έχουμε:

$$\begin{aligned} p_a(x_a) &= \sum_{X \setminus x_a} \prod_{b \in A} \psi_b(x_b) = \psi_a(x_a) \sum_{X \setminus x_a} \prod_{i \in V(a)} \prod_{b \in A_{i \rightarrow a}} \psi_b(x_b) \\ &\cong \psi_a(x_a) \prod_{i \in V(a)} \sum_{X_{i \rightarrow a}} \prod_{b \in A_{i \rightarrow a}} \psi_b(x_b) \cong \psi_a(x_a) \prod_{i \in V(a)} \mu_{i \rightarrow a}(x_i) \end{aligned}$$

Το οποίο ολοκληρώνει την απόδειξη. \square

Ισχυρισμός 6. Η Σταθερά Κανονικοποίησης Z ικανοποιεί:

$$\log Z = \sum_{a \in A} \log c_a + \sum_{i \in V} (1 - n_i) \log c_i + \sum_{ia \in E} \log c_{i \rightarrow a}$$

όπου $c_{i \rightarrow a} = \sum_{x_i} \prod_{b \in V(i) \setminus a} \mu_{b \rightarrow i}(x_i)$

Απόδειξη. Από τον Ισχυρισμό 4 έχουμε:

$$\begin{aligned} \frac{1}{Z} \prod_{a \in A} \psi_a(x_a) &= \prod_{a \in A} p_a(x_a) \prod_{i \in V} p_i(x_i)^{1-n_i} \\ \implies \log Z &= \sum_{a \in A} \log \left(\frac{\psi_a(x_a)}{p_a(x_a)} \right) + \sum_{i \in V} (n_i - 1) \log p_i(x_i) \end{aligned}$$

Χωρίς βλάβη μπορούμε να αθροίσουμε τα παραπάνω για όλους τους συνδυασμούς τιμών των μεταβλητών. Θα έχουμε:

$$\sum_X P(X) \log Z = \log Z = \sum_{a \in A} \sum_{x_a} p_a(x_a) \log \left(\frac{\psi_a(x_a)}{p_a(x_a)} \right) + \sum_{i \in V} (n_i - 1) \sum_{x_i} p_i(x_i) \log p_i(x_i) \quad (10)$$

Έχουμε τώρα $p_a(x_a) = \frac{1}{c_a} \prod_{i \in V(a)} \mu_{i \rightarrow a}(x_i)$ και άρα:

$$\begin{aligned} \sum_{a \in A} \sum_{x_a} p_a(x_a) \log \left(\frac{\psi_a(x_a)}{p_a(x_a)} \right) &= \sum_{a \in A} \log c_a - \sum_{a \in A} \sum_{i \in V(a)} \sum_{x_i} p_i(x_i) \log \mu_{i \rightarrow a}(x_i) \\ &= \sum_{a \in A} \log c_a - \sum_{a \in A} \sum_{i \in V(a)} \sum_{x_i} p_i(x_i) \log \left(\frac{1}{c_{i \rightarrow a}} \prod_{b \in V(i) \setminus a} \mu_{b \rightarrow i}(x_i) \right) \\ &= \sum_{a \in A} \log c_a + \sum_{ia \in E} \log c_{i \rightarrow a} - \sum_{i \in V} (n_i - 1) \sum_{b \in V(i)} \sum_{x_i} p_i(x_i) \log \mu_{b \rightarrow i}(x_i) \end{aligned} \quad (11)$$

Όπου θέσαμε $c_{i \rightarrow a} = \sum_{x_i} \prod_{b \in V(i) \setminus a} \mu_{b \rightarrow i}(x_i)$. Τώρα $p_i(x_i) = \frac{1}{c_i} \prod_{b \in V(i)} \mu_{b \rightarrow i}(x_i)$ και άρα:

$$\sum_{i \in V} (n_i - 1) \sum_{x_i} p_i(x_i) \log p_i(x_i) = \sum_{i \in V} (1 - n_i) \log c_i + \sum_{i \in V} (n_i - 1) \sum_{b \in V(i)} \sum_{x_i} p_i(x_i) \log \mu_{b \rightarrow i}(x_i) \quad (12)$$

Αντικατάσταση των (11) και (12) στην (10) δίνει το ζητούμενο □

Κεφάλαιο 1

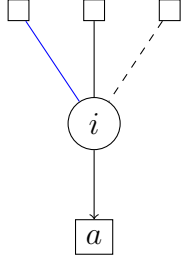
Αλγόριθμοι για το Πρόβλημα SAT και η Μεθοδος 1RSB Cavity

1.1 Ο Αλγόριθμος Warning Propagation για το Πρόβλημα SAT

Ο πρώτος Αλγόριθμος τον οποίο θα παρουσιάσουμε είναι ο αλγόριθμος Warning Propagation. Ο αλγόριθμος αυτός είναι εξαιρετικά απλός και μας δίνει πληροφορία για το πως συμπεριφέρονται κάποιες μεταβλητές στα Satisfying Assignments, κατασκευάζοντας μια απεικόνιση από αυτές στο σύνολο $\{0, 1, *\}$ με την εξής ερμηνεία:

- $x_i \mapsto 0$: Για όλα τα Satisfying Assignments ισχύει $x_i = 0$, άρα η μεταβλητή x_i είναι περιορισμένη να πάρει την τιμή 0.
- $x_i \mapsto 1$: Για όλα τα Satisfying Assignments ισχύει $x_i = 1$, άρα η μεταβλητή x_i είναι περιορισμένη να πάρει την τιμή 1.
- $x_i \mapsto *$: Υπάρχουν Satisfying Assignments και για τις δύο αληθοτιμές της μεταβλητής x_i , άρα αυτή δεν περιορίζεται.

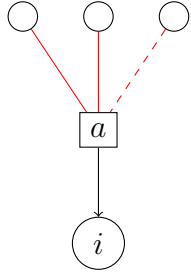
Κύριο συστατικό του αλγορίθμου είναι τα μηνύματα κατά μήκος των ακμών του γραφικού μοντέλου, $E_{a \rightarrow i}$ από τους περιορισμούς στις μεταβλητές και $E_{i \rightarrow a}$ από τις μεταβλητές στους περιορισμούς. Τα μηνύματα αυτά είναι δίτιμες μεταβλητές και οι ερμηνείες τους είναι οι εξής:



Σχήμα 1.1: $E_{i \rightarrow a} = \{1, 0\}$, μπλε ακμή δηλώνει μη μηδενικό warning

Μηνύματα από μεταβλητές προς περιορισμούς:

- $E_{i \rightarrow a} = \{1, 0\}$: Οι γείτονες του i εκτός από τον a χρειάζονται το i να πάρει την τιμή 0 παρά την τιμή 1.
- $E_{i \rightarrow a} = \{0, 1\}$: Οι γείτονες του i εκτός από τον a χρειάζονται το i να πάρει την τιμή 1 παρά την τιμή 0.
- $E_{i \rightarrow a} = \{1, 0\}$: Οι γείτονες του i εκτός από τον a δεν χρειάζονται το i να πάρει κάποια αληθοτιμή ενάντια της άλλης.



Σχήμα 1.2: $E_{a \rightarrow i} = \{1, 0\}$, κόκκινη ακμή δηλώνει $h_{j \rightarrow a} J_j^a > 0$

Μηνύματα από περιορισμούς προς μεταβλητές:

- $E_{a \rightarrow i} = \{1, 0\}$: Ο περιορισμός a απαιτεί από την μεταβλητή i να πάρει την τιμή 0 για να ικανοποιηθεί.
- $E_{a \rightarrow i} = \{0, 1\}$: Ο περιορισμός a απαιτεί από την μεταβλητή i να πάρει την τιμή 1 για να ικανοποιηθεί.
- $E_{a \rightarrow i} = \{1, 0\}$: Ο περιορισμός a δεν απαιτεί από την μεταβλητή i να πάρει κάποια συγκεκριμένη τιμή για να ικανοποιηθεί.

Επειδή μόνο για πλήρη ακμή $a - i$ μπορούμε να έχουμε $E_{a \rightarrow i} = \{1, 0\}$ και μόνο για διακεκομμένη ακμή $E_{a \rightarrow i} = \{0, 1\}$, τα μηνύματα $E_{a \rightarrow i}$ παραμετροποιούνται με μια μεταβλητή $w_{a \rightarrow i} \in \{0, 1\}$ πχ $E_{a \rightarrow i} = \{w_{a \rightarrow i}, 0\}$ για πλήρη ακμή. Ο Αλγόριθμος αρχικοποιεί τυχαία και ομοιόμορφα τα μηνύματα και τα ενημερώνει ως εξής:

1. Για κάθε $j \in V(a) \setminus i$ υπολογίζει το:

$$h_{j \rightarrow a} = \sum_{b \in V_+(j) \setminus a} w_{b \rightarrow j} - \sum_{b \in V_-(j) \setminus a} w_{b \rightarrow j} \quad (1.1)$$

Αν $V(i) \setminus a$ κενό, τότε $h_{j \rightarrow a} = 0$. Τότε:

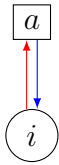
$$E_{j \rightarrow a} = \begin{cases} \{1, 0\} & \text{για } h_{j \rightarrow a} > 0, \\ \{0, 1\} & \text{για } h_{j \rightarrow a} < 0, \\ \{0, 0\} & \text{για } h_{j \rightarrow a} = 0. \end{cases}$$

2. Το $w_{a \rightarrow i}$ για $a - i$ πλήρης ακμή ενημερώνεται ως εξής:

$$w_{a \rightarrow i} = \begin{cases} 1 & \text{αν για κάθε } j \in V(a) \setminus i \text{ είναι } h_{j \rightarrow a} J_j^a > 0, \\ 0 & \text{διαφορετικά.} \end{cases} \quad (1.2)$$

Αν $V(a) \setminus i$ κενό, τότε $w_{j \rightarrow a} = 1$. Στα σχήματα που ακολουθούν απεικονίζουμε μηνύματα με $h * J > 0$ κε κόκκινο χρώμα ενώ μηνύματα με $w > 0$ απεικονίζονται με μπλε χρώμα.

Ισχυρισμός 7. Έστω στιγμιότυπο του προβλήματος SAT για το οποίο το γραφικό μοντέλο είναι δέντρο. Τότε τα μηνύματα συγκλίνουν, ανεξάρτητα από την αρχικοποίηση.



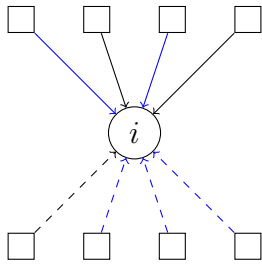
Σχήμα 1.3: Αντίφαση στην ακμή $a - i$.

Η απόδειξη του ισχυρισμού αυτού είναι ανάλογη με την απόδειξη της σύγκλισης του αλγόριθμου Belief Propagation και την αναβάλλουμε για την επόμενη ενότητα.

Ας μελετήσουμε τώρα την σχέση μεταξύ των μηνυμάτων και της ύπαρξης ή μη από Satisfying Assignments στην περίπτωση δέντρου. Για κάθε ακμή $i - a$ ορίζουμε την ποσότητα:

$$F_{ai} = \mathbf{1}\{E_{a \rightarrow i} + E_{i \rightarrow a} = \{1, 1\}\} \quad (1.3)$$

Η τελευταία ισούται με 1 αν ο a χρειάζεται την i να λάβει την τιμή που τον ικανοποιεί, ενώ πιο πολλοί είναι οι γείτονες της i που χρειάζονται αυτήν να λάβει την αντίθετη τιμή ώστε να ικανοποιηθούν.



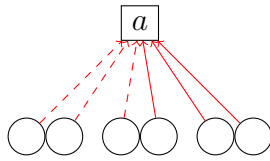
Σχήμα 1.4: Αντίφαση στην μεταβλητή i , $F_i = 2$.

Θα ορίσουμε τώρα τις αντιφάσεις των μεταβλητών ως εξής:

$$F_i = \min \sum_{b \in V(i)} E_{b \rightarrow i} = \min(n_0, n_1) \quad (1.4)$$

Όπου n_0 το πλήθος των εισερχόμενων $\{1, 0\}$ μηνυμάτων και n_1 το πλήθος των εισερχόμενων $\{0, 1\}$ μηνυμάτων.

Τέλος, θα ορίσουμε και αντιφάσεις παραγόντων. Θεωρούμε $F_a = 0$ αν υπάρχει τρόπος να τεθούν τιμές στις γειτονικές μεταβλητές που στέλνουν στο a μηδενικό μήνυμα, έτσι ώστε οι υπόλοιπες γειτονικές μεταβλητές να λάβουν τις τιμές που χρειάζονται σύμφωνα με τα μηνύματα που στέλνουν στον a ενώ αυτός να ικανοποιείται.



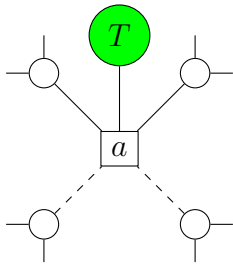
Σχήμα 1.5: Αντίφαση στον περιορισμό a

Αν αυτό δεν είναι δυνατόν, τότε θεωρούμε $F_a = 1$. Παρατηρήστε ότι αυτό είναι ισοδύναμο με το να είναι όλα τα εισερχόμενα στο a μηνύματα κόκκινα. Συμβολικά:

$$F_a = \min_{x_a} \left[\mathbf{1}\{a \text{ satisfied}\} + \sum_{j \in V(a)} E_{j \rightarrow a}(1 - x_j) \right] \quad (1.5)$$

Ισχυρισμός 8. Έστω στιγμότυπο του προβλήματος SAT για το οποίο το γράφημα είναι δέντρο. Το ελάχιστο πλήθος περιορισμών που παραβιάζεται, U^* ικανοποιεί:

$$U^* = \sum_{a \in F} F_a + \sum_{i \in V} F_i - \sum_{(ia) \in E} F_{ia} \quad (1.6)$$



Απόδειξη. Θα αποδείξουμε τον παραπάνω ισχυρισμό με επαγωγή στο πλήθος M των παραγόντων. Η περίπτωση $M = 1$ είναι τετριμμένη ενώ για το επαγωγικό βήμα θα θεωρήσουμε ότι επιτρέπουμε σε έναν περιορισμό να μην ικανοποιείται, πχ μέσω πρόσθεσης μιας εικονικής μεταβλητής σε αυτόν μόνο που να τον ικανοποιεί. Θα δούμε την επίδραση αυτού στην ποσότητα U^* . Αρχικά ήταν $F_a = 1$ και οπότε και $F_{ai} = 1 \quad \forall i \in V(a)$. Οι αντιφάσεις αυτές τώρα δεν θα υπάρχουν καθώς ο a ικανοποιείται και δεν στέλνει warning στους γείτονες του. Παράλληλα,

επειδή η γείτονες δεν ικανοποιούσαν το a , η αληθοτιμή που αυτό απαιτούσε είναι αυτή που αντιστοιχούσε στο $\arg \min(n_0, n_1)$ του ορισμού του F_i και άρα το τελευταίο θα έχει μειωθεί τώρα κατά μια μονάδα για κάθε $i \in V(a)$. Συνολικά το U^* ελαττώθηκε λοιπόν κατά μια μονάδα το οποίο ολοκληρώνει το επαγωγικό βήμα. \square

1.2 Η Μέθοδος RS Cavity και ο Αλγόριθμος Belief Propagation για το Πρόβλημα SAT

Έχουμε ήδη παρουσιάσει στην εισαγωγή την μέθοδο RS Cavity και την υλοποίηση της μέσω του αλγορίθμου Belief Propagation. Θα εφαρμόσουμε τώρα την μέθοδο αυτή στο πρόβλημα SAT. Έχουμε ορίσει την κατανομή:

$$P(X) = \frac{1}{Z} \prod_{a \in A} \mathbb{1}\{a \text{ satisfied}\} \quad (1.7)$$

Η οποία είναι ομοιόμορφη πάνω στο σύνολο των Satisfying Assignments και η σταθερά κανονικοποίησης της Z ισούται με το συνολικό πλήθος αυτών. Για την κατανομή αυτή και το αντίστοιχο γράφημα παραγόντων, η μέθοδος RS Cavity ορίζει τα εξής μηνύματα:

$$\begin{aligned} \bullet \mu_{i \rightarrow a}(x_i) &\cong \prod_{b \in V(i) \setminus a} \mu_{b \rightarrow i}(x_i) \\ \bullet \mu_{a \rightarrow i}(x_i) &= \sum_{x_a \setminus x_i} \mathbb{1}\{a \text{ satisfied}\} \prod_{j \in V(a) \setminus i} \mu_{j \rightarrow a}(x_j) \end{aligned} \quad (1.8)$$

και η ερμηνεία τους είναι η εξής:

- $\mu_{i \rightarrow a}(x_i) \in [0, 1]$ είναι η κατανομή της μεταβλητής i στο μοντέλο εάν δεν υπήρχε ο περιορισμός a .
- $\mu_{a \rightarrow i}(x_i) \in [0, 1]$ είναι η πιθανότητα να ικανοποιείται ο περιορισμός a αν η μεταβλητή i λάβει την τιμή x_i .

Η ύπαρξη δύο ειδών ακμών στην γενική περίπτωση περιπλέκει την κατανομή. Στην περίπτωση του προβλήματος SAT οι μεταβλητές είναι δίτιμες και το θέμα αυτό αντιμετωπίζεται μέσω παραμετρικοποίησης. Συγκεκριμένα, τα μηνύματα $\mu_{i \rightarrow a}$ μπορούν να περιγράφονται πλήρως από μια παράμετρο $\gamma_{i \rightarrow a}$ η οποία θα ισούται με την πιθανότητα η μεταβλητή i να μην ικανοποιεί τον περιορισμό a αν αυτός δεν υπήρχε (πχ $\mu_{i \rightarrow a} = (\gamma_{i \rightarrow a}, 1 - \gamma_{i \rightarrow a})$ για πλήρη ακμή). Ορίζουμε επίσης $\delta_{a \rightarrow i} = \prod_{j \in V(a) \setminus i} \gamma_{j \rightarrow a}$ την πιθανότητα κανέναν γείτονα του a εκτός από την i να τον ικανοποιεί. Θα είναι τότε, για παράδειγμα, $\mu_{a \rightarrow i} = (1, 1 - \delta_{a \rightarrow i})$ για πλήρη ακμή.

Ο αλγόριθμος θα ενημερώνει τις μεταβλητές που ορίσαμε ως εξής:

1.

$$\gamma_{j \rightarrow a} = \frac{P_{j \rightarrow a}^u}{P_{j \rightarrow a}^u + P_{j \rightarrow a}^s}$$

$$\text{όπου } P_{j \rightarrow a}^u = \prod_{b \in V_a^s(i)} (1 - \delta_{b \rightarrow j}) \quad (1.9)$$

$$P_{j \rightarrow a}^s = \prod_{b \in V_a^u(i)} (1 - \delta_{b \rightarrow j})$$

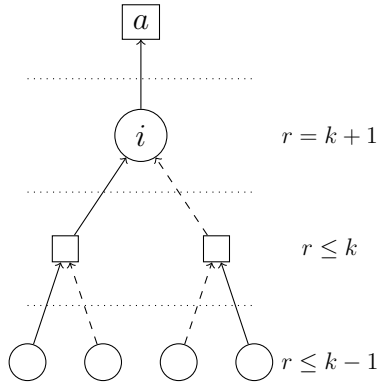
2.

$$\delta_{a \rightarrow i} = \prod_{j \in V(a) \setminus i} \gamma_{j \rightarrow a} \quad (1.10)$$

Θα αποδείξουμε τώρα εκ νέου τον Ισχυρισμό 2 της εισαγωγικής ενότητας για το πρόβλημα SAT μέσω των παραμέτρων που ορίσαμε παραπάνω.

Ισχυρισμός 9. Κατόπιν συγκλίσεως, το μήνυμα $\gamma_{i \rightarrow a}$ ισούται με την πιθανότητα σε ένα τυχαίο και ομοιόμορφα επιλεγμένο *Satisfying Assignment* η μεταβλητή i να λάβει την τιμή που δεν ικανοποιεί τον περιορισμό a .

Απόδειξη.



Η απόδειξη αυτή είναι επίσης επαγωγική στο βάθος του υπόδεντρου $T_{i \rightarrow a}$. Για βάθος 0 ή 1 ισχύει εξ ορισμού. Υποθέτουμε ότι ισχύει για βάθος $\leq k$ του $T_{i \rightarrow a}$. Χωρίς βλάβη θα υποθέσουμε ότι η ακμή $i - a$ είναι πλήρης. Η απόδειξη στην αντίθετη περίπτωση είναι όμοια. Από την επαγωγική υπόθεση, για $j \in V(b) \setminus i : b \in V(i) \setminus a$ τα μηνύματα $\gamma_{j \rightarrow b}$ μετράνε το κλάσμα των *Satisfying Assignments* στο υπόδεντρο $T_{j \rightarrow b}$ για τα οποία το b δεν θα ικανοποιείται. Για να επεκταθούν τα *Satisfying Assignments* του $\bigcup T_{j \rightarrow b}$ σε *Satisfying Assignments* του $T_{i \rightarrow a}$ θα πρέπει τα $b \in V(i) \setminus a$ να ικανοποιηθούν. Διακρίνουμε περιπτώσεις:

1. Κάποιο από τα $b \in V_a^s(i)$ δεν ικανοποιείται από κανέναν απόγονο του ενώ τα $b \in V_a^u(i)$ έχουν ήδη ικανοποιηθεί. Αυτό συμβαίνει για κλάσμα των *Satisfying Assignments* του $\bigcup T_{j \rightarrow b}$ ίσο με:

$$\left[1 - \prod_{b \in V_a^s(i)} (1 - \delta_{b \rightarrow i}) \right] \prod_{b \in V_a^u(i)} (1 - \delta_{b \rightarrow i}) = (1 - P_{i \rightarrow a}^u) P_{i \rightarrow a}^s$$

Θέτοντας $i = 0$ λαμβάνουμε ένα Satisfying Assignment του $T_{i \rightarrow a}$.

2. Κάποιο από τα $b \in V_a^u(i)$ δεν ικανοποιείται από κανέναν απόγονο του ενώ τα $b \in V_a^s(i)$ έχουν ήδη ικανοποιηθεί. Αυτό συμβαίνει για κλάσμα των Satisfying Assignments του $\bigcup T_{j \rightarrow b}$ ίσο με:

$$\left[1 - \prod_{b \in V_a^u(i)} (1 - \delta_{b \rightarrow i}) \right] \prod_{b \in V_a^s(i)} (1 - \delta_{b \rightarrow i}) = (1 - P_{i \rightarrow a}^s) P_{i \rightarrow a}^u$$

Θέτοντας $i = 0$ λαμβάνουμε ένα Satisfying Assignment του $T_{i \rightarrow a}$.

3. Όλα τα $b \in V(i) \setminus a$ έχουν ήδη ικανοποιηθεί από τους απογόνους τους. Αυτό συμβαίνει για κλάσμα των Satisfying Assignments του $\bigcup T_{j \rightarrow b}$ ίσο με:

$$\prod_{b \in V_a^u(i)} (1 - \delta_{b \rightarrow i}) \prod_{b \in V_a^s(i)} (1 - \delta_{b \rightarrow i}) = P_{i \rightarrow a}^s P_{i \rightarrow a}^u$$

Για οποιαδήποτε αληθοτιμή της i λαμβάνουμε ένα Satisfying Assignment του $T_{i \rightarrow a}$, άρα συνολικά δύο από αυτά.

4. Για κάθε ένα από τα σύνολα $V_a^s(i), V_a^u(i)$ υπάρχει περιορισμός που δεν ικανοποιείται ήδη. Αυτό συμβαίνει για το υπόλοιπο κλάσμα των Satisfying Assignments του $\bigcup T_{j \rightarrow b}$ ίσο με:

$$\left[1 - \prod_{b \in V_a^u(i)} (1 - \delta_{b \rightarrow i}) \right] \left[1 - \prod_{b \in V_a^s(i)} (1 - \delta_{b \rightarrow i}) \right] = (1 - P_{i \rightarrow a}^s)(1 - P_{i \rightarrow a}^u)$$

Αυτά δέν μπορούν να επεκταθούν σε Satisfying Assignment του $T_{i \rightarrow a}$.

Επομένως, το κλάσμα των Satisfying Assignments στο $T_{i \rightarrow a}$ με $x_i = 1$ ισούται με:

$$\mu_i(x_i = 1) = \frac{(1 - P_{i \rightarrow a}^s) P_{i \rightarrow a}^u + P_{i \rightarrow a}^s P_{i \rightarrow a}^u}{(1 - P_{i \rightarrow a}^s) P_{i \rightarrow a}^u + (1 - P_{i \rightarrow a}^u) P_{i \rightarrow a}^s + 2 P_{i \rightarrow a}^s P_{i \rightarrow a}^u} = \frac{P_{i \rightarrow a}^u}{P_{i \rightarrow a}^u + P_{i \rightarrow a}^s}$$

το οποίο ολοκληρώνει την απόδειξη. □

Μπορούμε τώρα να υπολογίσουμε τις σταθερές κανονικοποίησης c_i, c_a, c_{ia} που ορίσαμε στην (8) στην εισαγωγική ενότητα ως προς τα μηνύματα αυτά. Συγκεκριμένα, ισχύει το παρακάτω:

Ισχυρισμός 10. για το πλήθος Z των *Satisfying Assignments* ισχύει:

$$\log Z = \sum_{a \in A} \mathbb{F}_a + \sum_{i \in V} (n_i - 1) \mathbb{F}_i \quad (1.11)$$

όπου

$$\begin{aligned} \mathbb{F}_a &= \log \left[\prod_{j \in V(a)} (P_{j \rightarrow a}^u + P_{j \rightarrow a}^s) - \prod_{j \in V(a)} P_{j \rightarrow a}^u \right] \\ \mathbb{F}_i &= \log [P_i^+ + P_i^-] \\ P_i^+ &= \prod_{b \in V_+(i)} (1 - \delta_{b \rightarrow i}) \\ P_i^- &= \prod_{b \in V_-(i)} (1 - \delta_{b \rightarrow i}) \end{aligned} \quad (1.12)$$

Απόδειξη. Το αποτέλεσμα προκύπτει άμεσα από τον Ισχυρισμό 6 αν υπολογίσουμε τις σταθερές κανονικοποίησης $c_a, c_i, c_{i \rightarrow a}$ της (8) για την συγκεκριμένη περίπτωση αυτή του αλγορίθμου Belief Propagation. Έχουμε:

$$c_a = \sum_{x_a} \mathbb{1}\{a \text{ satisfied}\} \prod_{i \in V(a)} \mu_{i \rightarrow a}(x_i) = 1 - \prod_{i \in V(a)} \gamma_{i \rightarrow a} = 1 - \prod_{i \in V(a)} \frac{P_{i \rightarrow a}^u}{P_{i \rightarrow a}^u + P_{i \rightarrow a}^s} \quad (1.13)$$

αφού η μόνη ανάθεση αληθοτιμών των x_a που μηδενίζει την δείκτρια είναι αυτή για την οποία κανένας γείτονας δεν ικανοποιεί το a . Επιπλέον, όπως ήδη δείξαμε:

$$c_{i \rightarrow a} = P_{i \rightarrow a}^u + P_{i \rightarrow a}^s \quad (1.14)$$

και επίσης:

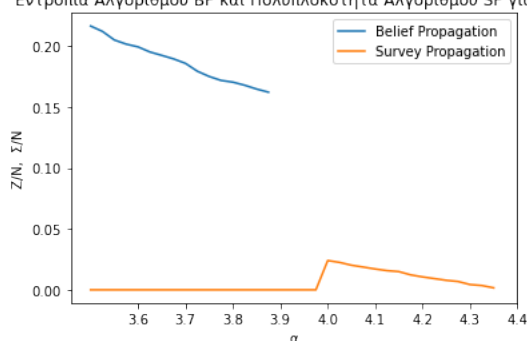
$$c_i = P_i^+ + P_i^- \quad (1.15)$$

Συνδυάζοντας κάθε c_a με τα $c_{i \rightarrow a}$ για $i \in V(a)$ προκύπτει το ζητούμενο. □

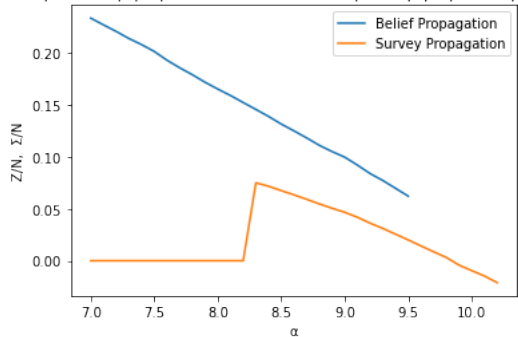
1.3 Η Μέθοδος 1RSB Cavity και ο Αλγόριθμος Survey Propagation για το Πρόβλημα SAT

Καθώς εκτελεί κανείς τους παραπάνω αλγόριθμους σε τυχαία στιγμιότυπα του k -SAT, θα παρατηρήσει ότι, κρατώντας τον αριθμό N των μεταβλητών σταθερό και αυξάνοντας τον αριθμό M των περιορισμών, ο αλγόριθμος γίνεται ασταθής, δεν συγκλίνει συχνά και υπάρχει δυνατότητα ύπαρξης περισσότερων του ενός σταθερών συνόλων μνηυμάτων για αυτά.

Εντροπία Αλγόριθμου BP και Πολυπλοκότητα Αλγόριθμου SP για $K=3$



Εντροπία Αλγόριθμου BP και Πολυπλοκότητα Αλγόριθμου SP για $K=4$



Εν γένει, οι αλγόριθμοι αυτοί δίνουν ακριβή αποτελέσματα σε μοντέλα δέντρων. Όταν εφαρμόζονται σε γραφήματα με κύκλους, κάνουν την παραδοχή ότι αφαιρώντας έναν περιορισμό, η γειτονικές του μεταβλητές έχουν χαμηλή συσχέτιση. Ωστόσο, το γράφημα μας για μεγάλο N και για σταθερό λόγο $\alpha = \frac{M}{N}$ είναι τοπικά δέντρο, επομένως για να παραβιάζεται η παραπάνω παραδοχή, θα πρέπει να υπάρχουν συσχετίσεις μεγάλης απόστασης (Long range correlations).

Αυτό που έχει δείχτεί στο [10] ότι συμβαίνει για μεγάλα k είναι ότι για ένα συγκεκριμένο εύρος του α , καθώς $N \rightarrow \infty$, υπάρχουν με ψηλή πιθανότητα λύσεις του προβλήματος και αυτές είναι οργανωμένες σε συστάδες, με τρόπο ώστε η απόσταση Hamming (το πλήθος των μεταβλητών των οποίων η αληθοτιμή διαφέρει)

δύο λύσεων της ίδιας συστάδας είναι μικρή, ενώ αυτή δύο λύσεων από διαφορετικές συστάδες είναι μεγάλη. Οι πιο πολλές μεταβλητές σε κάθε συστάδα είναι «παγωμένες», δηλαδή λαμβάνουν μία μόνο τιμή για κάθε Satisfying Assignment της συστάδας αυτής.

Λόγω της γεωμετρίας αυτής του χώρου λύσεων, δύο Satisfying Assignments από την ίδια συστάδα θα έχουν ψηλή συσχέτιση, και άρα δημιουργούνται γενικά συσχετίσεις μέσω της «κρυμμένης» μεταβλητής (latent variable) η οποία δηλώνει την συστάδα στην οποία ανήκει κάθε λύση, το οποίο δικαιολογεί την αστάθεια των παραπάνω αλγορίθμων. Επειδή ο αλγόριθμος Warning Propagation κατασκευάζει ακριβώς μια απεικόνιση από τις μεταβλητές στο σύνολο $\{0, 1, *\}$ ανάλογα με το αν μια μεταβλητή είναι 'παγωμένη' ή όχι, και επειδή εάν δεσμεύσουμε τον χώρο των λύσεων σε μία μόνο συστάδα, τότε

δεν περιμένουμε ψηλές συσχετίσεις, πιστεύουμε ότι υπάρχει αντιστοιχία ανάμεσα στα σταθερά σύνολα μηνυμάτων του αλγόριθμου Warning Propagation και τις συστάδες λύσεων. Η ιδέα της μεθόδου 1RSB Cavity είναι να μετρήσουμε το πλήθος των σταθερών αυτών συνόλων (και άρα να εκτιμήσουμε το πλήθος συστάδων λύσεων) αντί να εκτιμήσουμε το πλήθος των λύσεων.

Θεωρούμε μεταβλητές τώρα τα μηνύματα, και θα θεωρήσουμε κατανομή πάνω στα σταθερά σύνολα του αλγόριθμου Warning Propagation. Προφανώς αυτά θα πρέπει να επαληθεύουν τις εξισώσεις του αλγόριθμου. Υπενθυμίζουμε ότι, για κάθε περιορισμό $a \in A$ θα πρέπει να έχουμε:

$$w_{a \rightarrow i} = \prod_{j \in V(a) \setminus i} \mathbb{1}\{h_{j \rightarrow a} J_j^a > 0\}, \quad \forall i \in V(a)$$

και για κάθε μεταβλητή $i \in V$ θα πρέπει να έχουμε:

$$h_{i \rightarrow a} = \sum_{b \in V_+(i) \setminus a} w_{b \rightarrow i} - \sum_{b \in V_-(i) \setminus a} w_{b \rightarrow i}, \quad \forall a \in V(i)$$

Για την αποφυγή σύγχυσης, θα συμβολίζουμε τα μηνύματα αυτά w_{ai} , h_{ia} και τις παραπάνω εξισώσεις ως:

$$\begin{aligned} w_{ai} &= f_a(\{h_{ja}\}_{j \in V(a) \setminus i}) \\ h_{ia} &= f_i(\{w_{bi}\}_{b \in V(i) \setminus a}) \end{aligned} \quad (1.16)$$

Επίσης, θυμίζουμε ότι το πλήθος περιορισμών που μπορεί να ικανοποιηθεί από ένα σταθερό σύνολο μηνυμάτων είναι:

$$U^* = \sum_{a \in A} \mathbb{F}_a + \sum_{i \in V} \mathbb{F}_i - \sum_{ia \in E} \mathbb{F}_{ia}$$

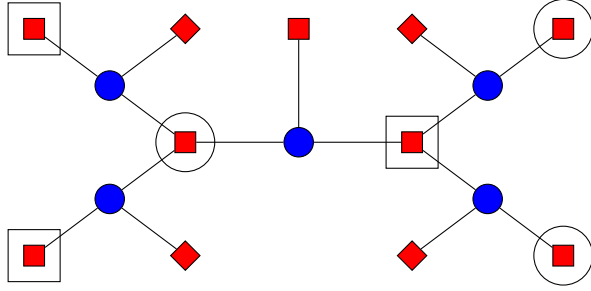
Θα ορίσουμε τώρα κατανομή πάνω στα σταθερά σύνολα μηνυμάτων, με τρόπο ώστε να επιτρέπεται η παραβίαση περιορισμών, αλλά κάθε παραβίαση ενός τέτοιου να μειώνει την πιθανότητα του αντίστοιχου σταθερού συνόλου μηνυμάτων κατά έναν παράγοντα e^{-x} , $x > 0$.

Η κατανομή είναι η εξής:

$$\begin{aligned} P[\{h_{ia}, w_{ai}\}] &= \frac{1}{N_c} \prod_{a \in A} \left[\prod_{i \in V(a)} \mathbb{1}\{w_{ai} = f_a(\{h_{ja}\}_{j \in V(a) \setminus i})\} \right] \prod_{i \in V} \left[\prod_{a \in V(i)} \mathbb{1}\{h_{ia} = f_i(\{w_{bi}\}_{b \in V(i) \setminus a})\} \right] \\ &\times e^{-x(\sum_{a \in A} \mathbb{F}_a + \sum_{i \in V} \mathbb{F}_i - \sum_{ia \in E} \mathbb{F}_{ia})} \\ &= \frac{1}{N_c} \prod_{a \in A} \Psi_a(\{h_{ia}, w_{ai}\}_{i \in V(a)}) \prod_{i \in V} \Psi_i(\{h_{ia}, w_{ai}\}_{a \in V(i)}) \prod_{ia \in E} \Psi_{ia}(\{h_{ia}, w_{ai}\}) \end{aligned} \quad (1.17)$$

Όπου

$$\begin{aligned}
 \Psi_a(\{h_{ia}, w_{ai}\}_{i \in V(a)}) &= \prod_{i \in V(a)} \mathbb{1}\{w_{ai} = f_a(\{h_{ja}\}_{j \in V(a) \setminus i})\} e^{-x \mathbb{F}_a} \\
 \Psi_i(\{h_{ia}, w_{ai}\}_{a \in V(i)}) &= \prod_{a \in V(i)} \mathbb{1}\{h_{ia} = f_i(\{w_{bi}\}_{b \in V(i) \setminus a})\} e^{-x \mathbb{F}_i} \\
 \Psi_{ia}(\{h_{ia}, w_{ai}\}) &= e^{x \mathbb{F}_{ia}}
 \end{aligned} \tag{1.18}$$

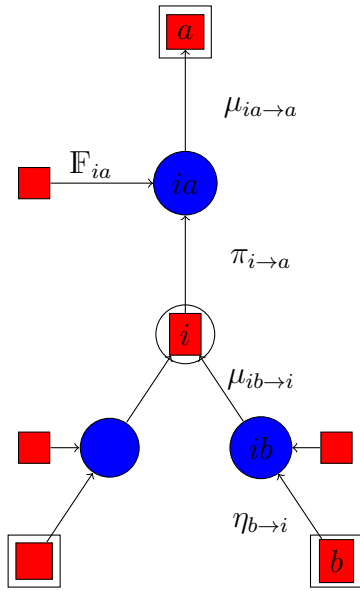


Σχήμα 1.6: Το νέο μοντέλο (έγχρωμοι κόμβοι) πάνω στο αρχικό μοντέλο (λευκοί κόμβοι)

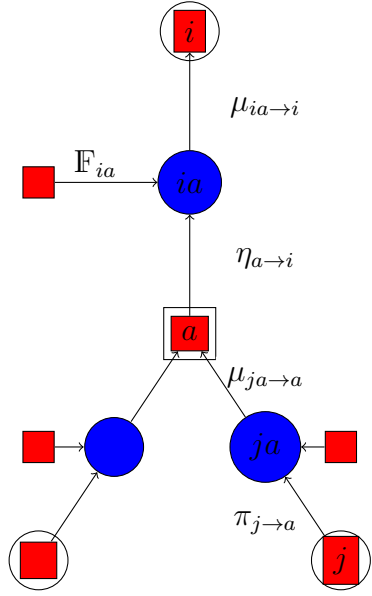
Η παραγοντοποίηση αυτή ορίζει γραφικό μοντέλο με παρόμοια μορφή όπως αυτό του αρχικού προβλήματος SAT. Συγκεκριμένα, για κάθε μεταβλητή και για κάθε παράγοντα του αρχικού μοντέλου έχουμε έναν παράγοντα Ψ όπως ορίσαμε, ενώ για κάθε ακμή, που αντιστοιχεί σε ζεύγος μηνυμάτων, έχουμε τώρα μια μεταβλητή. Έχοντας ορίσει το μοντέλο ως μοντέλο γραφήματος παραγόντων, μπορούμε τώρα να εφαρ-

μόσουμε τον γενικό αλγόριθμο Belief Propagation για να εκτιμήσουμε τις κατανομές των μηνυμάτων.

Θα ονομάσουμε $\pi_{i \rightarrow a}$ το μήνυμα $\mu_{i \rightarrow ia}$ και $\eta_{b \rightarrow i}$ το μήνυμα $\mu_{b \rightarrow ib}$. Οι εξισώσεις Belief Propagation (5) δίνουν:



$$\begin{aligned}
 \pi_{i \rightarrow a}(h_{ia}) &\cong \prod_{b \in V(i) \setminus a} \mu_{ib \rightarrow i}(w_{bi}) \Psi_i \\
 &\cong \prod_{b \in V(i) \setminus a} \eta_{b \rightarrow i}(w_{bi}) \Psi_i \Psi_{ib} \\
 &\cong \prod_{b \in V(i) \setminus a} \mathbb{1}\{h_{ia} = f_i(\{w_{bi}\}_{b \in V(i) \setminus a})\} \eta_{b \rightarrow i}(w_{bi}) \\
 &\quad \times e^{-x(\mathbb{F}_i - \mathbb{F}_{ib})}
 \end{aligned}$$



Θα υπολογίσουμε τώρα μια παρόμοια σχέση για τα μηνύματα $\eta_{a \rightarrow i}$ συναρτήσει των μηνυμάτων $\pi_{j \rightarrow a}$.

Οι εξισώσεις Belief Propagation (5) δίνουν:

$$\begin{aligned}
 \eta_{a \rightarrow i}(w_{ia}) &\cong \prod_{j \in V(a) \setminus i} \mu_{ja \rightarrow a}(h_{ja}) \Psi_a \\
 &\cong \prod_{j \in V(a) \setminus i} \pi_{j \rightarrow a}(h_{ja}) \Psi_a \Psi_{ja} \\
 &\cong \prod_{j \in V(a) \setminus i} \mathbb{1} \{w_{ai} = f_a(\{h_{ja}\}_{j \in V(a) \setminus i})\} \pi_{j \rightarrow a}(h_{ja}) \\
 &\quad \times e^{-x(\mathbb{F}_a - \mathbb{F}_{ja})}
 \end{aligned}$$

Έχουμε λοιπόν τις εξής εξισώσεις για τα $\pi_{i \rightarrow a}(h_{ia})$, $\eta_{a \rightarrow i}(w_{ai})$, οι οποίες ονομάζονται εξισώσεις 1RSB Cavity:

$$\begin{aligned}
 \pi_{i \rightarrow a}(h_{ia}) &\cong \prod_{b \in V(i) \setminus a} \mathbb{1} \{h_{ia} = f_i(\{w_{bi}\}_{b \in V(i) \setminus a})\} \eta_{b \rightarrow i}(w_{bi}) e^{-x(\mathbb{F}_i - \mathbb{F}_{ib})} \\
 \eta_{a \rightarrow i}(w_{ia}) &\cong \prod_{j \in V(a) \setminus i} \mathbb{1} \{w_{ai} = f_a(\{h_{ja}\}_{j \in V(a) \setminus i})\} \pi_{j \rightarrow a}(h_{ja}) e^{-x(\mathbb{F}_a - \mathbb{F}_{ja})}
 \end{aligned} \tag{1.19}$$

Για τον αλγόριθμο Warning Propagation που ορίσαμε σε προηγούμενη ενότητα, είδαμε ότι είναι $\mathbb{F}_a = 1 \Leftrightarrow \mathbb{F}_{ia} = 1 \quad \forall i \in V(a)$. επομένως θα είναι πάντοτε $\mathbb{F}_a - \mathbb{F}_{ia} = 0$. Επίσης, εύκολα παρατηρεί κανείς ότι:

$$u_{ia} := \mathbb{F}_i - \mathbb{F}_{ia} = \min\{\hat{n}_0, \hat{n}_1\} \tag{1.20}$$

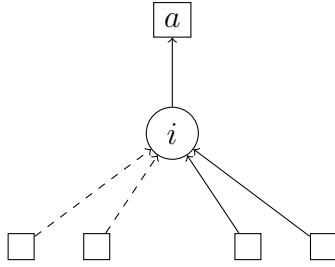
Όπου

$$\begin{aligned}
 \hat{n}_0 &= \sum_{b \in V_+(i) \setminus a} w_{b \rightarrow i} \\
 \hat{n}_1 &= \sum_{b \in V_-(i) \setminus a} w_{b \rightarrow i}
 \end{aligned}$$

Παίρνοντας τώρα το όριο $x \rightarrow \infty$ λαμβάνουμε τις εξισώσεις Survey Propagation.

$$\begin{aligned}
\pi_{i \rightarrow a}(h_{ia}) &\cong \sum_{w_{bi}} \mathbf{1} \{h_{ia} = f_i(\{w_{bi}\}_{b \in V(i) \setminus a})\} \mathbf{1} \{u_{ia} = 0\} \prod_{b \in V(i) \setminus a} \eta_{b \rightarrow i}(w_{bi}) \\
\eta_{a \rightarrow i}(w_{ia}) &\cong \sum_{h_{ja}} \mathbf{1} \{w_{ia} = f_a(\{h_{ja}\}_{j \in V(a) \setminus i})\} \prod_{j \in V(a) \setminus i} \pi_{j \rightarrow a}(h_{ja})
\end{aligned} \tag{1.21}$$

Όπου θυμίζουμε ότι $h_{ia} \in \{0, 1, *\}$, $w_{ai} \in \{1, 0\}$. Θα υπολογίσουμε τώρα τις τιμές των μηνυμάτων για τις διάφορες τιμές των h_{ia}, w_{ai} .



Η συνθήκη $\mathbf{1}\{u_{ia} = 0\}$ αντιστοιχεί στο να μην έχουμε warning από περιορισμούς των συνόλων $V_a^u(i), V_a^s(i)$ ταυτόχρονα. Θα παραμετροποιήσουμε το $\pi_{i \rightarrow a}(h_{ia})$ με την βοήθεια των παραμέτρων $\Pi_{i \rightarrow a}^u, \Pi_{i \rightarrow a}^s, \Pi_{i \rightarrow a}^*$, ώστε $\pi_{i \rightarrow a}(0, 1, *) = (\Pi_{i \rightarrow a}^s, \Pi_{i \rightarrow a}^u, \Pi_{i \rightarrow a}^*)$ για πλήρη ακμή ai , και $\pi_{i \rightarrow a}(0, 1, *) = \Pi_{i \rightarrow a}^u, \Pi_{i \rightarrow a}^s, \Pi_{i \rightarrow a}^*$ για διακεκομμένη ακμή ai . Παραμετροποιούμε επίσης το $\eta_{a \rightarrow i}(w_{ai})$ ως $(\eta_{a \rightarrow i}(0), \eta_{a \rightarrow i}(1)) = (1 - \eta_{a \rightarrow i}, \eta_{a \rightarrow i})$.

Οι εξισώσεις τότε γίνονται:

$$\begin{aligned}
\Pi_{i \rightarrow a}^u &= \left[1 - \prod_{b \in V_a^u(i)} (1 - \eta_{b \rightarrow i}) \right] \prod_{b \in V_a^s(i)} (1 - \eta_{b \rightarrow i}) \\
\Pi_{i \rightarrow a}^s &= \left[1 - \prod_{b \in V_a^s(i)} (1 - \eta_{b \rightarrow i}) \right] \prod_{b \in V_a^u(i)} (1 - \eta_{b \rightarrow i}) \\
\Pi_{i \rightarrow a}^* &= \prod_{b \in V(j) \setminus a} (1 - \eta_{b \rightarrow i}) \\
\eta_{a \rightarrow i} &= \prod_{j \in V(a) \setminus i} \frac{\Pi_{j \rightarrow a}^u}{\Pi_{j \rightarrow a}^u + \Pi_{j \rightarrow a}^s + \Pi_{j \rightarrow a}^*}
\end{aligned} \tag{1.22}$$

Οι οποίες με την συνθήκη ότι γινόμενα πάνω σε κενά σύνολα ισούνται με 1 δίνουν τον αλγόριθμο Survey Propagation, στον οποίο ενημερώνουμε διαδοχικά τα μηνύματα όλων των ακμών μέσω των εξισώσεων αυτών, όπως και στους προηγούμενους αλγόριθμους.

Για να λάβουμε την εξίσωση για το $\Pi_{i \rightarrow a}^u$, για παράδειγμα, αθροίσαμε πάνω σε όλα τα ενδεχόμενα των $w_{a \rightarrow i}$ για τα οποία έχουμε τουλάχιστον ένα μη μηδενικό warning από το σύνολο $V_a^u(i)$ και κανένα μη μηδενικό warning από το $V_a^s(i)$, αφού διαφορετικά θα ήταν $u_{ia} > 0$. Κάθε ένας από αυτούς τους γείτονες στέλνει μη μηδενικό warning με πιθανότητα $\eta_{b \rightarrow i}$. Έτσι παίρνουμε τις ερμηνείες των $\Pi_{i \rightarrow a}$. Συγκεκριμένα, διαλέγοντας

τυχαία ένα σύνολο σταθερών μηνυμάτων του αλγόριθμου Warning Propagation με πιθανότητα ανάλογη του πλήθους Satisfying Assignments που ορίζουν αντικαθιστώντας αληθοτιμές στις μη παγωμένες μεταβλητές,

- $\Pi_{i \rightarrow a}^u$ είναι η πιθανότητα στον αλγόριθμο Warning Propagation να είναι $h_{i \rightarrow a} J_i^a > 0$
- $\Pi_{i \rightarrow a}^s$ είναι η πιθανότητα στον αλγόριθμο Warning Propagation να είναι $h_{i \rightarrow a} J_i^a < 0$
- $\Pi_{i \rightarrow a}^0$ είναι η πιθανότητα στον αλγόριθμο Warning Propagation να είναι $h_{i \rightarrow a} J_i^a = 0$
- $\eta_{a \rightarrow i}$ είναι η πιθανότητα στον αλγόριθμο Warning Propagation να είναι $w_{a \rightarrow i} = 1$

Παρατηρείστε την ομοιότητα των εξισώσεων Survey Propagation και Belief Propagation. Φαίνεται πως η διαφορά τους είναι απλά ότι στις πρώτες ορίσαμε ξεχωριστή κατάσταση για την περίπτωση 3 στον ισχυρισμό 9, θεωρώντας ότι η περίπτωση αυτή δίνει Satisfying Assignment. Ουσιαστικά, οι εξισώσεις Survey Propagation αποτελούν εξισώσεις Belief Propagation για το γράφημα του αρχικού προβλήματος, με την επιπλέον παρουσία της κατάστασης * (: μη δέσμευση) πέραν των αληθοτιμών 0, 1 των μεταβλητών. (Δείτε [15] για αναλυτική απόδειξη αυτού). Δίνοντας αυτήν την ερμηνεία στις εξισώσεις, μπορεί κανείς να λάβει άμεσα την εντροπία του αλγορίθμου Survey Propagation, την οποία για την αποφυγή σύγχυσης με την εντροπία του αλγορίθμου Belief Propagation θα ονομάζουμε συνάρτηση πολυπλοκότητας από εδώ και στο εξής. Τα αποτελέσματα (1.11), (1.12) της προηγούμενης παραγράφου γενικεύονται άμεσα:

Ισχυρισμός 11. Το πλήθος συστάδων λύσεων για ένα στιγμιότυπο του προβλήματος SAT, N_c , ικανοποιεί

$$\log N_c = \sum_{a \in A} \Sigma_a + \sum_{i \in V} (n_i - 1) \Sigma_i \quad (1.23)$$

όπου

$$\begin{aligned}
\Sigma_a &= \log \left[\prod_{j \in V(a)} (\Pi_{j \rightarrow a}^u + \Pi_{j \rightarrow a}^s + \Pi_{j \rightarrow a}^*) - \prod_{j \in V(a)} \Pi_{j \rightarrow a}^u \right] \\
\Sigma_i &= \log [\Pi_i^+ + \Pi_i^- + \Pi_i^*] \\
\Pi_i^+ &= \left[1 - \prod_{b \in V_+(i)} (1 - \eta_{b \rightarrow i}) \right] \prod_{b \in V_-(i)} (1 - \eta_{b \rightarrow i}) \\
\Pi_i^- &= \left[1 - \prod_{b \in V_-(i)} (1 - \eta_{b \rightarrow i}) \right] \prod_{b \in V_+(i)} (1 - \eta_{b \rightarrow i}) \\
\Pi_i^* &= \prod_{b \in V(j)} (1 - \eta_{b \rightarrow i})
\end{aligned} \tag{1.24}$$

1.4 Οι Αλγόριθμοι WID και SID για την Εύρεση Satisfying Assignments

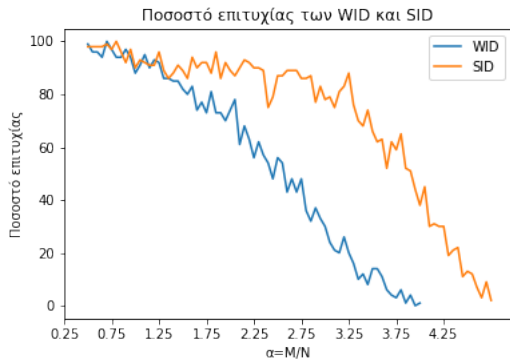
Θα κλείσουμε το πρώτο αυτό κεφάλαιο με μια σύντομη αναφορά στους αλγόριθμους WID (Warning Propagation Inspired Decimation και SID (Survey Propagation Inspired Decimation οι οποίοι εκμεταλλεύονται τους παραπάνω αλγορίθμους για να αναζητήσουν Satisfying Assignment σε στιγμιότυπα του προβλήματος SAT. Οι αλγόριθμοι αυτή μοιάζουν και δίνουμε περιγραφή τους

WID :

1. Τρέξε τον αλγόριθμο Warning Propagation στο τρέχον στιγμιότυπο του προβλήματος SAT
2. Αν ο Αλγόριθμος δεν συγκλίνει ή αν υπάρχουν αντιφάσεις, επέστρεψε UNSAT
3. Αν δεν υπάρχουν αντιφάσεις, δώσε σε κάθε μεταβλητή που δέχεται μη μηδενικά Warning την αληθοτιμή που αυτά απαιτούν. Αν όλα τα Warnings είναι μηδενικά, θέσε τυχαία μια αληθοτιμή σε κάποια μεταβλητή.
4. Καθάρισε το γράφημα. Αν το γράφημα που προκύπτει είναι κενό, επέστρεψε τις αληθοτιμές που τέθηκαν. Διαφορετικά επέστρεψε στο 1

SID :

1. Τρέξε τον αλγόριθμο Survey Propagation στο τρέχον στιγμιότυπο του προβλήματος SAT
2. Αν ο Αλγόριθμος δεν συγκλίνει επέστρεψε UNSAT
3. Υπολόγισε για κάθε μεταβλητή την μεροληψία $|\Pi_i^+ - \Pi_i^-|$. Δώσε στην μεταβλητή με την μεγαλύτερη μεροληψία την επιθυμητή αληθοτιμή. Αν όλα τα Surveys είναι μηδενικά, θέσε τυχαία μια αληθοτιμή σε κάποια μεταβλητή.
4. Καθάρισε το γράφημα. Αν το γράφημα που προκύπτει είναι κενό, επέστρεψε τις αληθοτιμές που τέθηκαν. Διαφορετικά επέστρεψε στο 1



Σχήμα 1.7: Ποσοστά επιτυχίας των W-ID και SID για $N = 100$ μεταβλητές

ακόμη και κοντά στο κατώφλι ικανοποίησης, όπου εκεί εκτιμάται γενικότερα η ύπαρξη φάσης «δύσκολων στιγμιότυπων». Περισσότερα πειράματα με τους αλγόριθμους μπορούν να βρεθούν στο [16]

Θα ορίσουμε τώρα την πράξη καθαρισμού που αναφέραμε παραπάνω. Αν τεθεί αληθοτιμή σε κάποια μεταβλητή, τότε την διαγράφουμε από το γράφημα, και διαγράφουμε επίσης τους γειτονικούς περιορισμούς που ικανοποιούνται με αυτήν την αληθοτιμή της μεταβλητής. Όταν διαγράφουμε έναν κόμβο, αφαιρούμε αυτόν μαζί με τις προκείμενες ακμές σε αυτόν.

Γενικά, ο αλγόριθμος SID δίνει καλύτερα αποτελέσματα, ενώ περαιτέρω αριθμητικά πειράματα υποδεικνύουν ότι για μεγαλύτερες τιμές του N είναι αποδοτικός

Κεφάλαιο 2

Η Εκτίμηση του Κατωφλιού Ικανοποίησης για το Τυχαίο Πρόβλημα K-SAT

2.1 Η Συνάρτηση Πολυπλοκότητας του Αλγο- ρίθμου Survey Propagation

Ανακεφαλαιώνοντας την προηγούμενη παράγραφο και υιοθετώντας τον συμβολισμό του [12], οι εξισώσεις Survey Propagation (1.22) είναι οι εξής:

$$\begin{aligned}\pi_{i \rightarrow a}^u &= \prod_{b \in V_a^u(i)} (1 - \eta_{b \rightarrow i}) \\ \pi_{i \rightarrow a}^s &= \prod_{b \in V_a^s(i)} (1 - \eta_{b \rightarrow i}) \\ \eta_{a \rightarrow i} &= \prod_{j \in V(a) \setminus i} \frac{\pi_{j \rightarrow a}^u (1 - \pi_{j \rightarrow a}^s)}{\pi_{j \rightarrow a}^u + \pi_{j \rightarrow a}^s - \pi_{j \rightarrow a}^u \pi_{j \rightarrow a}^s}\end{aligned}\tag{2.1}$$

και η συνάρτηση πολυπλοκότητας (1.23) ισούται με:

$$\Sigma = \frac{1}{N} \left[\sum_{a \in A} \Sigma_a^c - \sum_{j \in V} \Sigma_j^v - \sum_{(aj) \in E} \Sigma_{aj}^{cv} \right]\tag{2.2}$$

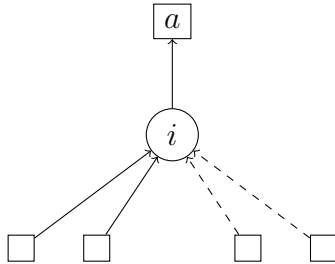
όπου

$$\begin{aligned}\Sigma_a^c &= \log \left(\prod_{i \in V(a)} (\pi_{j \rightarrow a}^u + \pi_{j \rightarrow a}^s - \pi_{j \rightarrow a}^u \pi_{j \rightarrow a}^s) - \prod_{i \in V(a)} \pi_{j \rightarrow a}^u (1 - \pi_{j \rightarrow a}^s) \right) \\ \Sigma_j^u &= \Sigma_{aj}^{cu} = \log \left(\prod_{b \in V_+(j)} (1 - \eta_{b \rightarrow j}) + \prod_{b \in V_-(j)} (1 - \eta_{b \rightarrow j}) - \prod_{b \in V(j)} (1 - \eta_{b \rightarrow j}) \right)\end{aligned}\quad (2.3)$$

όπου τα $\Sigma_j^u, \Sigma_{aj}^{cu}$ διαφέρουν στο ότι στο τελευταίο δεσμεύουμε στην ύπαρξη της ακμής aj .

Αριθμητικά πειράματα δείχνουν ότι η συνάρτηση αυτή είναι φθίνουσα συνάρτηση του a , το οποίο οδήγησε στην εικασία ότι το ζητούμενο κατώφλι είναι η τιμή του a που μηδενίζει αυτήν την συνάρτηση. Θυμίζουμε ότι $\Sigma = \frac{1}{N} \log N_c$ όπου N_c το πλήθος συστάδων λύσεων.

Θα απλουστεύσουμε το πρόβλημα μας θεωρώντας $\pi_{i \rightarrow a}^u, \pi_{i \rightarrow a}^s \sim \pi$ και $\eta_{a \rightarrow i} \sim \eta$, δηλαδή ότι τα μηνύματα του μοντέλου αποτελούν μετρήσεις των τυχαίων μεταβλητών π και η , των οποίων την κατανομή θα προσεγγίσουμε στη συνέχεια.



Βλέπουμε ότι τα $\pi_{i \rightarrow a}^{u/s}$ είναι γινόμενα $k_{\pm}^i = |V_a^{u/s}(i)|$ παραγόντων $(1 - \eta)$, δεδομένου ότι υπάρχει η ακμή $a - i$. Για μεγάλα N , ο βαθμός μιας μεταβλητής ακολουθεί κατανομή Poisson με μέσο $K\alpha$. Επίσης, το πλήθος των πλήρων και διακεκομμένων ακμών που συνορεύουν σε μια μεταβλητή είναι ανεξάρτητες και όμοια κατανεμημένες τυχαίες μεταβλητές που ακολουθούν την κατανομή Poisson με μέσο $\frac{K\alpha}{2}$. Επειδή η ύπαρξη της ακμής $a - i$ δεν εξαρτάται από την ύπαρξη των άλλων ακμών,

την ίδια κατανομή ακολουθούν επίσης τα k_{\pm}^i τα οποία είναι και αυτά ανεξάρτητα μεταξύ τους.

Για λόγους ευκολίας, ορίζουμε $\varphi = -\log(1 - \eta)$ και $x = -\log \pi$ και ορίζουμε $S(\varphi)$ και $B(x)$ αντίστοιχα τις συναρτήσεις πυκνότητας πιθανότητας τους. Αυτές είναι θετικές συναρτήσεις ορισμένες στο $[0, \infty)$, πεπλεγμένες και με μάζα στο 0. Οι εξισώσεις Survey Propagation (2.1) για αυτές είναι:

$$\begin{aligned}
x_{i \rightarrow a}^u &= \sum_{b \in V_a^u(i)} \phi_{b \rightarrow i} \\
x_{i \rightarrow a}^s &= \sum_{b \in V_a^s(i)} \phi_{b \rightarrow i} \\
\phi_{a \rightarrow j} &= -\log \left(1 - \prod_{i \in V(a) \setminus j} \frac{e^{x_{i \rightarrow a}^u} - 1}{e^{x_{i \rightarrow a}^u} + e^{x_{i \rightarrow a}^s} - 1} \right)
\end{aligned} \tag{2.4}$$

Δεσμεύοντας ως προς τις διάφορες τιμές του k , υπολογίζουμε την $B(x)$:

$$B(x) = \sum_{k=0}^{\infty} f_{\frac{K\alpha}{2}}(k) S^{\oplus k}(x) \tag{2.5}$$

όπου $f_{\frac{K\alpha}{2}}(k) = \frac{(\frac{K\alpha}{2})^k}{k!} e^{-\frac{K\alpha}{2}}$ η συνάρτηση μάζας πιθανότητας της κατανομής Poisson με μέσο $\frac{K\alpha}{2}$. Η συνάρτηση πυκνότητας της φ θα είναι ίση με:

$$S(\phi) = \int \prod_{i=1}^{k-1} [B(x_i) dx_i B(y_i) dy_i] \delta \left(\phi + \log \left(1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1} \right) \right) \tag{2.6}$$

Το οποίο αντιστοιχεί στο να αθροίσουμε τις πυκνότητες των $x_i, y_i \sim B$ για όλους τους συνδυασμούς τους που επαληθεύουν την εξίσωση Survey Propagation για το φ .

Για τον υπολογισμό της συνάρτησης πολυπλοκότητας, ορίζουμε:

$$\begin{aligned}
I_s &= \int \prod_{i=1}^s dx_i dy_i B(x_i) B(y_i) \log \left[\prod_{i=1}^s (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^s (e^{x_i} - 1) \right] \\
&= \mathbb{E} \left[\log \left[\prod_{i=1}^s (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^s (e^{x_i} - 1) \right] \right] \\
\Sigma_0 &= \int dx dy B(x) B(y) \log (e^x + e^y - 1) = \mathbb{E} [\log (e^x + e^y - 1)]
\end{aligned} \tag{2.7}$$

θα παρουσιάσουμε τώρα το αποτέλεσμα αυτής της ενότητας το οποίο θα το αποδείξουμε στη συνέχεια μέσω μιας σειράς ισχυρισμών.

Πρόταση 1. Η αναμενόμενη τιμή της συνάρτησης πολυπλοκότητας δίνεται από τον τύπο:

$$\mathbb{E}[\Sigma] = \Sigma_0 + a [kI_{k-1} - (k-1)I_k] \quad (2.8)$$

Ισχυρισμός 12. Για την πολυπλοκότητα περιορισμών ισχύει:

$$\mathbb{E}[\Sigma_a^c] = -2k\mathbb{E}[x] + I_k \quad (2.9)$$

Απόδειξη. Με $x_i, y_i \sim B(x)$ έχουμε:

$$\begin{aligned} \mathbb{E}[\Sigma_a^c] &= \mathbb{E} \left[\log \left[\prod_{i=1}^k (e^{-x_i} + e^{-y_i} - e^{-x_i - y_i}) - \prod_{i=1}^k (e^{-x_i} - e^{-x_i - y_i}) \right] \right] \\ &= \mathbb{E} \left[\log \left[\left(\prod_{i=1}^k e^{-(x_i + y_i)} \right) \left(\prod_{i=1}^k (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^k (e^{x_i} - 1) \right) \right] \right] \\ &= -k\mathbb{E}[x_i + y_i] + \mathbb{E} \left[\log \left[\prod_{i=1}^k (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^k (e^{x_i} - 1) \right] \right] \\ &= -2k\mathbb{E}[x] + I_k \end{aligned}$$

□

Ισχυρισμός 13. Για την πολυπλοκότητα μεταβλητών ισχύει:

$$\mathbb{E}[\Sigma_j^v] = -2\mathbb{E}[x] + \Sigma_0 \quad (2.10)$$

Απόδειξη. Με $x, y \sim B(x)$ έχουμε:

$$\begin{aligned} \mathbb{E}[\Sigma_j^v] &= \mathbb{E} [\log (e^{-x} + e^{-y} - e^{-(x+y)})] \\ &= \mathbb{E} [\log e^{-(x+y)} + \log (e^x + e^y - 1)] \\ &= -2\mathbb{E}[x] + \Sigma_0 \end{aligned}$$

□

Ισχυρισμός 14. Για την πολυπλοκότητα ακμών ισχύει:

$$\mathbb{E}[\Sigma_{a,j}^{cv}] = -2\mathbb{E}[x] - (k-1)\Sigma_0 + I_k \quad (2.11)$$

Απόδειξη. Θυμίζουμε ότι έχουμε δεσμεύσει στην ύπαρξη της ακμής $a-j$ και άρα με $x_k, y_k \sim B(x)$ και υποθέτοντας χωρίς βλάβη ότι η ακμή είναι πλήρης, είναι :

$$\begin{aligned} \Sigma_{a,j}^{cv} &= \log ((1 - \eta_{a \rightarrow j})e^{-x_k} + e^{-y_k} - (1 - \eta_{a \rightarrow j})e^{-(x_k + y_k)}) \\ &= \log (e^{-(x_k + y_k)}) + \log ((1 - \eta_{a \rightarrow j})e^{y_k} + e^{x_k} - (1 - \eta_{a \rightarrow j})) \end{aligned}$$

Επομένως

$$\begin{aligned}
\mathbb{E}[\Sigma_{aj}^{cv}] &= -2\mathbb{E}[x] + \mathbb{E}[(1 - \eta)e^{y_k} + e^{x_k} - (1 - \eta)] \\
&= -2\mathbb{E}[x] + \mathbb{E}\left[\left(1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1}\right) e^{y_k} + e^{x_k} - \left(1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1}\right)\right] \\
&= -2\mathbb{E}[x] + \mathbb{E}\left[\log\left(\frac{1}{\prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1)}\right)\right] \\
&\quad + \mathbb{E}\left[\log\left(\left(\prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^{k-1} (e^{x_i} - 1)\right) (e^{y_k} - 1) + \prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1)e^{x_k}\right)\right] \\
&= -2\mathbb{E}[x] - (k-1)\Sigma_0 \\
&\quad + \mathbb{E}\left[\log\left((e^{x_k} + e^{y_k} - 1) \prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1) - (e^{x_k} - 1) \prod_{i=1}^{k-1} (e^{x_i} - 1)\right)\right] \\
&= -2\mathbb{E}[x] - (k-1)\Sigma_0 + I_k
\end{aligned}$$

Ισχυρισμός 15. Για την αναμενόμενη τιμή της x ισχύει:

$$\mathbb{E}[x] = \frac{K\alpha}{2} [(k-1)\Sigma_0 - I_{k-1}] \quad (2.12)$$

Απόδειξη. Σύμφωνα με τις εξισώσεις Survey Propagation είναι:

$$\pi = \prod_{i=1}^{k \sim P_0(\frac{K\alpha}{2})} (1 - \eta_i) \implies x = \sum_{i=1}^{k \sim P_0(\frac{K\alpha}{2})} \phi_i \implies \mathbb{E}[x] = \frac{K\alpha}{2} \mathbb{E}[\phi] \quad (2.13)$$

Επίσης:

$$\begin{aligned}
I_{k-1} &= \int \prod_{i=1}^s dx_i dy_i B(x_i) B(y_i) \log \left[\prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1) - \prod_{i=1}^{k-1} (e^{x_i} - 1) \right] \\
&= \int \prod_{i=1}^s dx_i dy_i B(x_i) B(y_i) \left(\log \left[\prod_{i=1}^{k-1} (e^{x_i} + e^{y_i} - 1) \right] + \log \left[1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1} \right] \right) \\
&= (k-1)\Sigma_0 - \mathbb{E}[\phi]
\end{aligned} \quad (2.14)$$

Το ζητούμενο προκύπτει με αντικατάσταση του $\mathbb{E}[\phi]$ από την (2.13) στην (2.14). \square

Απόδειξη της Πρότασης 1 Απο τον τύπο της συνάρτησης πολυπλοκότητας (2.2) είναι:

$$\begin{aligned}
N\mathbb{E}[\Sigma] &= M\mathbb{E}[\Sigma_a^c] + N\mathbb{E}[\Sigma_i^v] - kM\mathbb{E}[\Sigma_{aj}^{cv}] \\
&= \alpha N(-2k\mathbb{E}[x] + I_k) - N(-2\mathbb{E}[x] + \Sigma_0) - k\alpha N(-2\mathbb{E}[x] - (k-1)\Sigma_0 + I_k) \\
&= -2N\mathbb{E}[x] + (\alpha N - k\alpha N)I_k + (N + k(k-1)\alpha N)\Sigma_0 \\
&= -k\alpha N((k-1)\Sigma_0 - I_{k-1}) + (\alpha N - k\alpha N)I_k + (N + k(k-1)\alpha N)\Sigma_0 \\
&= k\alpha N I_{k-1} + (\alpha N - k\alpha N)I_k + N\Sigma_0
\end{aligned}$$

Άρα

$$\mathbb{E}[\Sigma] = k\alpha I_{k-1} + (\alpha - k\alpha)I_k + \Sigma_0$$

Το οποίο ισοδυναμεί με το ζητούμενο (2.8). □

2.2 Αριθμητική Εκτίμηση του Κατωφλιού Ικανοποίησης για μικρά K

Πριν προχωρήσουμε στην ανάλυση της συνάρτησης πολυπλοκότητας για μεγάλα k , θα επιχειρήσουμε να εκτιμήσουμε το κατώφλι ικανοποίησης για μικρές τιμές αυτού μέσω του αλγορίθμου Population Dynamics. Σκοπός του αλγορίθμου αυτού είναι η κατασκευή δειγμάτων από τις πεπλεγμένες κατανομές των x και ϕ , τα οποία θα τα χρησιμοποιήσουμε στη συνέχεια για να εκτιμήσουμε την τιμή της συνάρτησης πολυπλοκότητας για διάφορες τιμές του α . Πριν προχωρήσουμε παρακάτω, παρατηρούμε ότι οι κατανομές των x και ϕ έχουν μάζα στο 0, την οποία θα αφαιρέσουμε για να δουλέψουμε με συνεχείς κατανομές. Θεωρούμε:

$$\begin{aligned} S(\phi) &= t\delta(\phi) + (1-t)S_r(\phi) \\ B(x) &= \tau\delta(x) + (1-\tau)A(x) \end{aligned} \quad (2.15)$$

Όπου θυμίζουμε ότι:

$$\begin{aligned} B(x) &= \sum_{k=0}^{\infty} f_{\frac{K\alpha}{2}}(k) S^{\oplus k}(x) \\ S(\phi) &= \int \prod_{i=1}^k [B(x_i) dx_i B(y_i) dy_i] \delta \left(\phi + \log \left(1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{y_i} + e^{y_i} - 1} \right) \right) \end{aligned}$$

Οι εξισώσεις αυτές δίνουν:

$$\begin{aligned} \tau &= \sum_{k=0}^{\infty} \frac{\left(\frac{K\alpha}{2}\right)^k}{k!} e^{-\frac{K\alpha}{2}} = e^{-\frac{K\alpha}{2}(1-t)} \\ t &= 1 - (1-\tau)^{K-1} \end{aligned} \quad (2.16)$$

Όπου η δεύτερη προκύπτει από το γεγονός ότι στον τύπο του $S(\phi)$ το όρισμα της δ συνάρτησης μηδενίζεται αν και μόνο αν ένα από τα $x_i = 0$.

Από τα αριθμητικά πειράματα με τον αλγόριθμο Survey Propagation στο προηγούμενο κεφάλαιο, περιμένουμε ότι για μικρές τιμές του α θα είναι $t = 1$ μοναδική λύση, το οποίο αντιστοιχεί στο να είναι όλα τα Warnings μηδενικά. Η λύση αυτή είναι τετριμμένη για κάθε τιμή του α , μόλις αυτό όμως περάσει μια ορισμένη τιμή, που εξαρτάται από το K , περιμένουμε μη τετριμμένη λύση κοντά στο 0. Αυτό αντιστοιχεί στην ύπαρξη μη μηδενικών warnings καθώς δημιουργούνται οι συστάδες λύσεων. Θέλουμε η πιθανότητα αυτή να είναι μικρή, καθώς μη μηδενικό warning κατά μήκος δύο ετερόσημων ακμών τις ίδιες μεταβλητής συνεπάγεται την μη ικανοποιησιμότητα του στιγμιότυπου. Λύνοντας ως προς t έχουμε την σχέση:

$$t = 1 - (1 - e^{-\frac{K\alpha}{2}(1-t)})^{K-1} \quad (2.17)$$

Το ανάπτυγμα της οποίας δίνει $t \sim (K-1)e^{-\frac{1}{2}\alpha K}$. Περιμένουμε λοιπόν αυτήν την συμπεριφορά των ευσταθών λύσεων του συστήματος, η οποία επιβεβαιώνεται πειραματικά. Θα υπολογίσουμε τώρα τις συναρτήσεις $S_r(\phi), B(x), A(x)$, θέτοντας $\gamma = \frac{K\alpha}{2}(1-t) \implies \tau = e^{-\gamma}$

Ο τύπος του $S_r(\phi)$ διαφέρει από αυτόν του $S(\phi)$ στο ότι πλέον $x_i \sim A(x)$, λόγω των ποσοτήτων $e^{x_i} - 1$ στον λογάριθμο οι οποίες τον μηδενίζουν για $x_i = 0$ για κάποιο i .

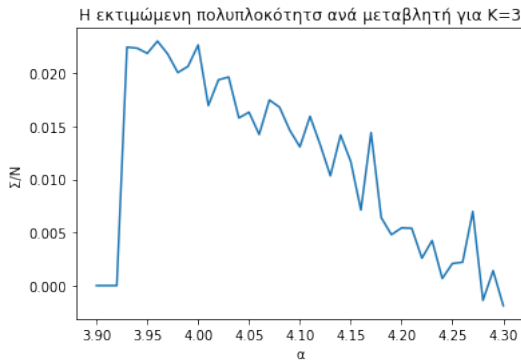
$$S_r(\phi) = \int \prod_{i=1}^k [A(x_i)dx_i B(y_i)dy_i] \delta \left(\phi + \log \left(1 - \prod_{i=1}^{k-1} \frac{e^{x_i} - 1}{e^{y_i} + e^{y_i} - 1} \right) \right) \quad (2.18)$$

Στον τύπο του $B(x)$, παρατηρείστε ότι τα μηδενικά ϕ_j δεν επηρεάζουν το αποτέλεσμα, καθώς δεν επηρεάζουν τον όρο $\delta(x - \sum_j \phi_j)$. Επομένως, αρκεί να λάβουμε υπόψη μόνο τα μη μηδενικά ϕ_j . Τώρα, επειδή κάθε ϕ_j είναι μηδενικό με πιθανότητα t , το πλήθος των μη μηδενικών ϕ_j ακολουθεί κατανομή Ποισσον με μέσο $\frac{K\alpha}{2}(1-t) = \gamma$. Άρα έχουμε:

$$B(y) = e^{-\gamma} \sum_{k=0}^{\infty} \frac{\gamma^k}{k!} \int \prod_{i=1}^k [d\phi_j S_r(\phi_j)] \delta \left(y - \sum_j \phi_j \right) \quad (2.19)$$

Για τον υπολογισμό του $A(x)$, αρκεί απλά στον παραπάνω τύπο να δεσμεύσουμε στο ότι $k \geq 1$. Επειδή $1 - P(k=0) = 1 - e^{-\gamma}$, έχουμε:

$$A(x) = \frac{1}{e^{\gamma} - 1} \sum_{k=1}^{\infty} \frac{\gamma^k}{k!} \int \prod_{i=1}^k [d\phi_j S_r(\phi_j)] \delta \left(x - \sum_j \phi_j \right) \quad (2.20)$$



Σχήμα 2.1: Για $K = 3$ η εκτίμηση του Αλγορίθμου Population Dynamics είναι $\alpha_s \approx 4.27$, $\alpha_d \approx 3.93$

Θα προσεγγίσουμε τώρα τις κατανομές αυτές με τον αλγόριθμο Population Dynamics, ο οποίος αρχικοποιεί την κατανομή $S_r(\phi)$ και προσεγγίζει μέσω αυτής τις κατανομές των $A(x), B(x)$ σύμφωνα με τους παραπάνω τύπους (2.18), (2.19) και (2.20). Με αυτές εκτιμά εκ νέου την κατανομή $S_r(\phi)$ και επαναλαμβάνει την διαδικασία μέχρι συγκλίσεως. Δίνουμε περιγραφή του αλγορίθμου.

Ο Αλγόριθμος Population Dynamics:

1. Υπολόγισε τα t και $\gamma = \frac{K\alpha}{2}(1 - t)$.
2. Αρχικοποίησε τα iid $\varphi_j \sim \exp(2^{1-K})$.
3. Για $j = 1$ ως $K - 1$:
 - Πάρε $k \geq 1$ απο κατανομή $\propto \gamma^k/k!$.
 - Διάλεξε τυχαία k δείκτες i_1, \dots, i_k από το $\{1, \dots, N\}$.
 - Υπολόγισε το $x_j = \varphi_{i_1} + \dots + \varphi_{i_k} \sim A(x)$.
4. Για $j = 1$ ως $K - 1$:
 - Πάρε $k \geq 0$ απο κατανομή $Po(\gamma)$.
 - Αν $k = 0$ τότε θέσε $y_j = 0$.
 - Αν $k \geq 0$, διάλεξε τυχαία k δείκτες. i_1, \dots, i_k από το $\{1, \dots, N\}$ και υπολόγισε το $y_j = \varphi_{i_1} + \dots + \varphi_{i_k} \sim B(y)$.
5. Υπολόγισε το $z = \prod_{j=1}^{K-1} \left(1 + \frac{e^{y_j}}{e^{x_j} - 1}\right)$.
6. Αντικατέστησε τυχαίο ϕ_l από τον πληθυσμό με το $\varphi_0 = \log 1 + 1/(z - 1) \sim S(\varphi)$.

Στο [12] υπολογίστηκαν μέσω του αλγορίθμου αυτού εκτιμήσεις για περισσότερες τιμές του K και με μεγαλύτερη ακρίβεια. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα.

K	α_d	α_s
3	3.927	4.267
4	8.297	9.931
5	16.12	21.117
6	30.50	43.37
7	57.22	87.79

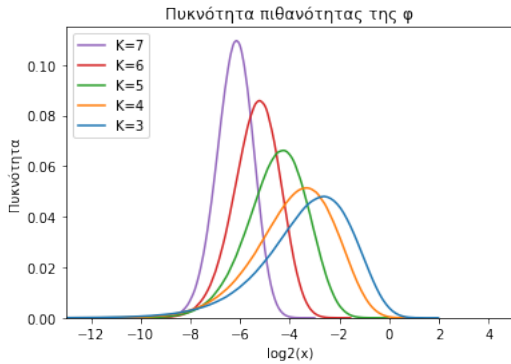
2.3 Η Εικασία του Κατωφλιού Ικανοποίησης

Στην ενότητα αυτή θα παρουσιάσουμε την εκτίμηση μας για το κατώφλι ικανοποίησης για μεγάλα K , το οποίο όπως εξηγήσαμε προηγουμένως θα είναι το σημείο μηδενισμού της συνάρτησης πολυπλοκότητας. Θα παρουσιάσουμε αρχικά το αποτέλεσμα και έπειτα θα το δείξουμε.

Εικασία 1. Το κατώφλι ικανοποίησης για το τυχαίο πρόβλημα $K - SAT$ επαληθεύει:

$$\alpha_s = 2^K \log 2 - \frac{\log 2 + 1}{2} + \mathcal{O}(2^{-K}) \quad (2.21)$$

Καθώς το K γίνεται πολύ μεγάλο, οι εξισώσεις (2.18), (2.19) και (2.20) των $S_r(\phi)$, $A(x)$ και $B(x)$ αντίστοιχα απλοποιούνται. Θα θέσουμε $\varepsilon = 2^{-K}$ και $\hat{\alpha} = 2^{-K}\alpha$, και θα υπολογίσουμε τα αναπτύγματα των $S_r(\phi)$, $A(x)$, $B(x)$ σε δυνάμεις του ε , όπου γενικά θα επιτρέψουμε και δυνάμεις των $K, \log K$ οι οποίες θα αγνοούνται στον \mathcal{O} -συμβολισμό. Επειδή $t \sim (K-1)e^{-\frac{K\alpha}{2}}$ είναι μικρότερο από κάθε δύναμη του ε , μπορούμε για τον υπολογισμό των αναπτυγμάτων να υποθέσουμε $t = 0$, και άρα $A(x) = B(x)$.



Σχήμα 2.2: Προσέγγιση της κατανομής του φ από τον αλγόριθμο Population Dynamics

Από το διπλανό διάγραμμα φαίνεται ότι για μικρές τιμές του K , η φ συγκεντρώνεται ολοένα και περισσότερο σε σημείο ολοένα και πλησιέστερα στο 2^{1-K} και μικρότερο αυτού. Θα υποθέσουμε λοιπόν το ακόλουθο για τις ροπές τις φ :

$$M_n := \mathbb{E}[\varphi^n] = \mathcal{O}(\varepsilon^n), \quad n \geq 1 \quad (2.22)$$

Επειδή η x είναι άθροισμα $Po(\gamma)$ το πλήθος ανεξάρτητων τυχαίων μεταβλητών συγκατανεμημένων της φ , ο νόμος της συνολικής συσσώρευσης [17] δίνει τον ακόλουθο τύπο για τα αθροιστικά \hat{b}_n της x :

$$\hat{b}_n = \gamma M_n, \quad n \geq 1 \quad (2.23)$$

και άρα λόγω της (2.22) είναι:

$$\hat{b}_n = \mathcal{O}(\varepsilon^{n-1}) \quad (2.24)$$

όπου τα αθροιστικά \hat{b}_n ορίζονται μέσω της ισότητας:

$$\exp \left[\sum_{n=1}^{\infty} \frac{\lambda^n}{n!} \hat{b}_n \right] = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} \mathbb{E}[y^n] \quad (2.25)$$

Το ακόλουθο λήμμα θα μας επιτρέψει να προσδιορίσουμε τις κεντρικές ροπές b_n του x έχοντας τα αθροιστικά του.

Λήμμα 3. Η κεντρικές ροπές b_n και τα αθροιστικά \hat{b}_n συνδέονται μέσω της σχέσης:

$$b_n = \sum_{k=1}^n B_{n,k}(0, \hat{b}_2, \dots, \hat{b}_{n-k+1}) \quad (2.26)$$

όπου $B_{n,k}$ το μερικό πολυώνυμο Bell.

Απόδειξη αυτού μπορεί να βρεθεί στο [18]. Αυτό που αρκεί να παρατηρήσουμε είναι ότι αυτές συμπεριφέρονται ασυμπτωτικά ως:

$$b_n = \mathcal{O}(\epsilon^{\lceil \frac{n}{2} \rceil}), \quad n \geq 2 \quad (2.27)$$

όπου η κύρια συνεισφορά προέρχεται πχ από τον όρο $\hat{b}_2^{\frac{n}{2}}$ για n άρτιο.

Ορίζουμε τώρα μεταβλητή ζ με κατανομή:

$$D(\zeta) = \int dx dy B(x)B(y) \delta\left(\zeta - \frac{e^x - 1}{e^x + e^y - 1}\right) \quad (2.28)$$

μέσω της οποίας μπορούμε να γράψουμε :

$$S_r(\phi) = \int \prod_{i=1}^{K-1} [d\zeta_i D(\zeta_i)] \delta\left(\phi + \log\left[1 - \prod_{i=1}^{K-1} \zeta_i\right]\right) \quad (2.29)$$

Θα υπολογίσουμε τώρα τις ροπές της D μέσω αναπτύγματος Taylor γύρω από το $(x, y) = (\mathbb{E}[x], \mathbb{E}[x])$. Συγκεκριμένα, θα είναι:

$$\mathbb{E}[\zeta^l] = \sum_{p,q=0}^{\infty} D_{p,q}^{(l)} b_p b_q \quad (2.30)$$

όπου $D_{p,q}^{(l)}$ είναι ο αντίστοιχος συντελεστής του πολυωνύμου Taylor που ικανοποιεί:

$$D_{p,q}^{(l)} = \frac{1}{p!q!} \frac{\partial^{p+q}}{\partial x^p \partial y^q} \left(\frac{e^x - 1}{e^x + e^y - 1} \right)^l \Big|_{x=y=\mathbb{E}[x]} \quad (2.31)$$

Επειδή τώρα $b_0 = 1, b_1 = 0, b_n = \mathcal{O}(\epsilon^{\lceil \frac{n}{2} \rceil}), \quad n \geq 2$ μπορούμε, επιτρέποντας σφάλμα $\mathcal{O}(\epsilon^2)$ να αγνοήσουμε όλους τους όρους εκτός των $D_{0,0}^{(l)}, D_{2,0}^{(l)}, D_{0,2}^{(l)}$. Ο πρώτος από αυτούς επαληθεύει:

$$D_{0,0}^{(l)} = \left(\frac{e^{\gamma M_1} - 1}{2e^{\gamma M_1} - 1} \right)^l = \left(\frac{1 - \delta}{2 - \delta} \right)^l = 2^{-l} \left(1 - \frac{l}{2} \delta \right) + \mathcal{O}(\epsilon^2) = 2^{-l} \left(1 - \frac{l}{2} \epsilon \right) + \mathcal{O}(\epsilon^2) \quad (2.32)$$

όπου θέσαμε $\delta = e^{-\gamma M_1}$. Επειδή από τα γνωστά φράγματα είναι $\hat{\alpha} = \log 2 + \mathcal{O}(\epsilon)$, παίρνουμε $\delta = \epsilon + \mathcal{O}(\epsilon^2)$. Με παρόμοιο τρόπο υπολογίζουμε:

$$D_{2,0}^{(l)} + D_{0,2}^{(l)} = 2^{-l} \frac{l(l-1)}{4} + \mathcal{O}(\epsilon) \quad (2.33)$$

Από τον τύπο του Taylor για το $-\log(1-x)$ γύρω από το 0 λαμβάνει κανείς:

$$\begin{aligned} M_1 &= \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}[\zeta^l]^{K-1} \\ &= \sum_{l=1}^{\infty} \frac{(2\epsilon)^l}{l} \left(1 - \frac{l}{2} \epsilon + \frac{l(l-1)}{4} b_2 + \mathcal{O}(\epsilon^2) \right)^{K-1} \\ &= 2\epsilon \left(1 - \frac{K-1}{2} \epsilon \right) + 2\epsilon^2 + \mathcal{O}(\epsilon^3) \end{aligned} \quad (2.34)$$

Όπου για την παραπάνω ακρίβεια μπορέσαμε να αγνοήσουμε τους όρους $l \geq 2$ στο άθροισμα, Ενώ για τον όρο $l = 1$ πήραμε ανάπτυγμα και για $l = 2$ μόνο τον σταθερό όρο στην παρένθεση. Παρατηρείστε ότι δικαιολογείται η υπόθεση στην εισαγωγική ενότητα για το μέγεθος του x , καθώς είναι $x = \omega_K(1)$. Με παρόμοιο τρόπο έχουμε $\varphi^2 = x^2 + \mathcal{O}(x^3)$ (όπου x από το προηγούμενο ανάπτυγμα) και άρα:

$$\begin{aligned} M_2 &= \mathbb{E}[\zeta^2]^{K-1} + \mathcal{O}(\epsilon^3) \\ &= 4\epsilon^2 + \mathcal{O}(\epsilon^3) \end{aligned} \quad (2.35)$$

Έχοντας τα M_1, M_2 μπορούμε τώρα να προσεγγίσουμε την μέση τιμή και διασπορά της x ως:

$$\begin{aligned} \mathbb{E}[x] &= \frac{K\hat{\alpha}}{2\epsilon} M_1 = \log 2 + \hat{\alpha}K - \hat{\alpha} \frac{K^2}{2} \epsilon + 2\hat{\alpha}K\epsilon - \frac{\epsilon}{2} + \mathcal{O}(\epsilon^2) \\ b_2 = \hat{b}_2 &= \frac{K\hat{\alpha}}{2\epsilon} M_2 = 2\hat{\alpha}K\epsilon + \mathcal{O}(\epsilon^2) \end{aligned} \quad (2.36)$$

Είμαστε τώρα σε θέση να υπολογίσουμε τα Σ_0, I_{K-1}, I_K των (2.7) και (2.14), επίσης μέσω αναπτυγμάτων Taylor γύρω από το $(\mathbb{E}[x], \mathbb{E}[x])$.

Ξεκινάμε με το Σ_0 . Άμεσα βλέπουμε ότι για $x, y \sim B$ είναι:

$$\Sigma_0 = \mathbb{E}[\log(e^x + e^y - 1)] \approx \log 2 + \mathbb{E}[x] = \log 2 + \hat{\alpha}K - \hat{\alpha}\frac{K^2}{2}\epsilon + 2\hat{\alpha}K\epsilon - \frac{\epsilon}{2} + \mathcal{O}(\epsilon^2) \quad (2.37)$$

Όπου η προσέγγιση δικαιολογείται από το ότι $x, y = \omega_K(1)$ με ψηλή πιθανότητα.

Έχουμε ήδη δει στην (2.14) ότι:

$$\begin{aligned} I_{K-1} &= (K-1)\Sigma_0 - \mathbb{E}[\phi] = (K-1)\Sigma_0 - M_1 \\ &= (K-1)\Sigma_0 - (2\epsilon - (K-1)\epsilon^2 + 2\epsilon^2 + \mathcal{O}(\epsilon^3)) \end{aligned} \quad (2.38)$$

Επίσης, ο όρος I_K επαληθεύει:

$$I_K = K\Sigma_0 + \mathbb{E} \left[\log \left(1 - \prod_{i=1}^K \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1} \right) \right] \quad (2.39)$$

όπου ο τελευταίος όρος υπολογίζεται παρόμοια όπως και το M_1 στην (2.34) μέσω αναπτύγματος Taylor.

$$\begin{aligned} \mathbb{E} \left[\log \left(1 - \prod_{i=1}^K \frac{e^{x_i} - 1}{e^{x_i} + e^{y_i} - 1} \right) \right] &= \sum_{l=1}^{\infty} \frac{1}{l} \mathbb{E}[\zeta^l]^K \\ &= \sum_{l=1}^{\infty} \frac{\epsilon^l}{l} \left(1 - \frac{l}{2}\epsilon + \frac{l(l-1)}{4}b_2 + \mathcal{O}(\epsilon^2) \right)^K \\ &= \epsilon \left(1 - \frac{K}{2}\epsilon \right) + \frac{\epsilon^2}{2} + \mathcal{O}(\epsilon^3) \end{aligned} \quad (2.40)$$

Συνδυάζοντας τα (2.38) και (2.40) λαμβάνει κανείς:

$$KI_{K-1} - (K-1)I_K = -(K+1)\epsilon - 2K\epsilon^2 + \frac{K^2}{2}\epsilon^2 - \frac{1}{2}\epsilon^2 + \mathcal{O}(\epsilon^3) \quad (2.41)$$

άρα μπορούμε τώρα με τις (2.37) και (2.41) να εκφράσουμε την αναμενόμενη συνάρτηση πολυπλοκότητας (2.8) σε δυνάμεις του ϵ . Συγκεκριμένα, θα είναι:

$$\mathbb{E}[\Sigma] = \log 2 - \frac{\epsilon}{2} - \hat{\alpha}\frac{1+\epsilon}{2} + \mathcal{O}(\epsilon^2) \quad (2.42)$$

Η οποία μηδενίζεται για:

$$\hat{\alpha} = \hat{\alpha}_s = \log 2 - \frac{\log 2 + 1}{2} \epsilon + \mathcal{O}(\epsilon^2) \quad (2.43)$$

Το οποίο δίνει την εικασία.

2.4 Η Απόδειξη της Εικασίας

Όπως αναφέραμε στην εισαγωγή, οι Franco και Paull [2] έδειξαν ότι το αναμενόμενο πλήθος από Satisfying Assignments ισούται με $2^N(1 - 2^{-K})^{\alpha N}$ το οποίο είναι τάξης $o(1)$ για $\alpha > 2^k \log 2$. Οι Dubois και Boufkhad [6] βελτίωσαν το άνω φράγμα μέσω εφαρμογής της μεθόδου πρώτης ροπής στα Satisfying Assignments στα οποία δεν υπάρχει δυνατότητα αλλαγής μιας μεταβλητής από "Αληθής" σε "Ψευδής". Οι λύσεις αυτές είναι υπό μια έννοια τοπικά μέγιστες και περιορίζεται το φαινόμενο να έχουμε πάρα πολλές λύσεις με πολύ μικρή πιθανότητα. Έτσι έδειξαν ότι $\alpha_s \leq 2^K \log 2 - \frac{1+\log 2}{2} - o(1)$.

Για την απόδειξη της εικασίας που παρουσιάσαμε στο προηγούμενο κεφάλαιο μένει να δειχτεί ότι το παραπάνω αποτελεί επίσης κάτω φράγμα του κατωφλιού. Αυτό έχει αποδειχτεί αρχικά από τους Coja Oghlan και Panagiotou στο [13]. Θα παρουσιάσουμε εδώ συνοπτικά τον τρόπο με τον οποίο απέδειξαν το κάτω φράγμα, ο οποίος φαίνεται να βασίζεται σε ιδέες των παραπάνω αλγορίθμων. Θα υιοθετήσουμε τον συμβολισμό των συγγραφέων και θα ονομάσουμε $\Phi = \Phi_1 \wedge \dots \wedge \Phi_M$ την σύζευξη των περιορισμών που αποτελούν το στιγμιότυπο του προβλήματος K-SAT. Σε κάθε μεταβλητή x_i αντιστοιχούμε δύο γράμματα $x_i, \neg x_i$. Το σύνολο όλων των γραμμάτων, δηλαδή των μεταβλητών και των αρνήσεων τους το ονομάζουμε L . Τέλος, κάθε γράμμα $l \in L$ εμφανίζεται σε d_l περιορισμούς, ορίζοντας ακριβώς τόσους κλώνους του l . Το σύνολο των κλώνων όλων των γραμμάτων το ονομάζουμε \mathcal{L} , ενώ τους απαριθμούμε για κάθε γράμμα και έτσι θεωρούμε $\text{pch}(l, j) \in \mathcal{L}$ τον j -οστό κλώνο του γράμματος $l, j \in [d_l]$. Ως προς το μοντέλα γραφημάτων ενός στιγμιότυπου του SAT, έχουμε τις εξείς αντιστοιχίες:

- Τα Φ_i αντιστοιχούν στις κορυφές περιορισμών F του G .
- Τα x_i αντιστοιχούν στις κορυφές μεταβλητών A του G .
- Το \mathcal{L} αντιστοιχεί στο σύνολο ακμών E του G . εάν για κάθε μεταβλητή απαριθμήσουμε τις πλήρεις και διακεκομμένες συνορεύουσες ακμές ξεχωριστά.
- Το σύνολο των κλώνων του γράμματος x_i αντιστοιχεί στις συνορεύουσες πλήρεις ακμές στην κορυφή i .
- Το σύνολο των κλώνων του γράμματος $\neg x_i$ αντιστοιχεί στις συνορεύουσες διακεκομμένες ακμές στην κορυφή i .

Θα ορίσουμε τώρα δύο απεικονίσεις οι οποίες αντιστοιχούν στον αλγόριθμο Warning Propagation, η μία από το σύνολο των γραμμάτων στο $\{0, 1, *\}$ και η άλλη από το σύνολο των κλώνων στα χρώματα $\{r, b, g, y\}$.

Ορισμός 2. Μια απεικόνιση $\zeta : V \rightarrow \{0, 1, *\}$ ονομάζεται κάλυμμα του Φ εάν η επέκταση της στο σύνολο των γραμμάτων, με $\zeta(\neg x_i) = \neg\zeta(x_i)$, όπου $\neg 0 = 1$, $\neg 1 = 0$, $\neg * = *$, ικανοποιεί:

1. Κάθε περιορισμός περιέχει είτε ένα γράμμα που απεικονίζεται μέσω της ζ στο 1, είτε δύο γράμματα που να απεικονίζονται στο $*$.
2. Κάθε γράμμα l για το οποίο $\zeta(l) = 1$ περιέχεται σε έναν περιορισμό τα υπόλοιπα γράμματα του οποίου απεικονίζονται στο 0.

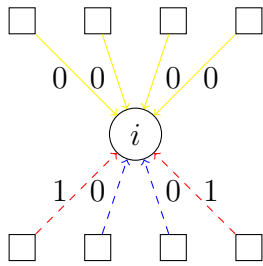
Σε αντιστοιχία με τον αλγόριθμο Warning Propagation, το 1. λέει ότι για κάθε περιορισμό, είτε θα αναγκάζονται όλες οι μεταβλητές εκτός από μία να τον ικανοποιήσουν, οπότε η τελευταία θα λάβει μη μηδενικό μήνυμα, είτε υπάρχουν περισσότερες από μια που είναι διαθέσιμες να τον ικανοποιήσουν. Το 2. λέει ότι για να πάρει μια μεταβλητή τιμή διάφορη του $*$, θα πρέπει κάποιος περιορισμός να στέλνει αντίστοιχο μη μηδενικό μήνυμα σε αυτήν.

Θα ορίσουμε τώρα τους χρωματισμούς των γραμμάτων, οι οποίοι ουσιαστικά αποτελούν επέκταση των καλυμμάτων στους κλώνους κάθε γράμματος. Στόχος τους είναι να χαρακτηρίσουν κριτικούς περιορισμούς, αυτοί δηλαδή που θα αναγκάσουν μια μεταβλητή να πάρει μια συγκεκριμένη αληθτιμμή.

Ορισμός 3. Μία απεικόνιση $\xi : \mathcal{L} \rightarrow \{r, b, g, y\}$ ονομάζεται χρωματισμός εάν ικανοποιεί τις παρακάτω συνθήκες:

1. Για κάθε γράμμα $l \in L$ ισχύει ακριβώς ένα από τα παρακάτω:
 - Κάθε κλώνος του l και του $\neg l$ είναι πράσινος (g).
 - Κάθε κλώνος του l χρωματίζεται είτε κόκκινος (r) είτε μπλε (b), και κάθε κλώνος του $\neg l$ κίτρινος (y).
 - Κάθε κλώνος του $\neg l$ χρωματίζεται είτε κόκκινος (r) είτε μπλε (b), και κάθε κλώνος του l κίτρινος (y).
2. Δεν υπάρχει γράμμα $l \in L$ για το οποίο όλοι οι κλώνοι είναι μπλε (b).

Η ερμηνεία της απεικόνισης αυτής στο μοντέλο γραφήματος μοιάζει με την προηγούμενη, με την διαφορά ότι μελετάμε τώρα της συνορεύουσες ακμές κάθε μεταβλητής ξεχωριστά.



Σχήμα 2.3: Τα μηνύματα $w_{a \rightarrow i}$ και το αντίστοιχο μοντέλο χρωμάτων. Θα είναι $\zeta(x_i) = 0$, $\zeta(\neg x_i) = 1$

Αν μια μεταβλητή δέχεται μη μηδενικό μήνυμα από συνορεύουσα διακεκομμένη ακμή, τότε αυτή χρωματίζεται κόκκινη, και οι συνορεύουσες διακεκομμένες ακμές που στέλνουν στην μεταβλητή μηδενικό μήνυμα χρωματίζονται μπλε. Οι πλήρεις ακμές χρωματίζονται χίτρινες.

Παρατηρείστε ότι περιοριζόμαστε σε ικανοποιήσιμα στιγμιότυπα, άρα τα μηνύματα στις συνορεύουσες πλήρεις ακμές είναι μηδενικά. Όμοια εργαζόμαστε αν τα μη μηδενικά μηνύματα προέρχονται από πλήρεις ακμές. Αν καμία συνορεύουσα ακμή δεν στέλνει μη μηδενικό μήνυμα, χρωματίζονται όλες πράσινες.

Θα ορίσουμε τώρα πότε ένας χρωματισμός είναι έγκυρος.

Ορισμός 4. Ένας χρωματισμός είναι έγκυρος εάν ικανοποιούνται οι δύο παρακάτω συνθήκες:

- Εάν ένας περιορισμός περιέχει κόκκινο (r) κλώνο, τότε οι υπόλοιποι κλώνοι του είναι χίτρινοι (y).
- Κάθε περιορισμός που δεν περιέχει κόκκινο κλώνο (r) περιέχει τουλάχιστον δύο κλώνους που είναι μπλε (b) οι πράσινοι (g).

Η δεύτερη συνθήκη αντιστοιχεί στην αποστολή μη μηδενικού μηνύματος κατά μήκος μια ακμής από περιορισμό σε μεταβλητή, αν όλες οι υπόλοιπες συνορεύουσες μεταβλητές αναγκάζονται να μην τον ικανοποιήσουν.

Ο παραπάνω ορισμός εξασφαλίζει την ύπαρξη μιας 1 – 1 αντιστοιχίας μεταξύ καλυμμάτων και χρωματισμών. Κάνοντας την αλλαγή $\{r, b\} \rightarrow 1, y \rightarrow 0, g \rightarrow *$ λαμβάνει κανείς ξανά το κάλυμμα που έδωσε τον έγκυρο χρωματισμό.

Ένα πρόβλημα που πρέπει να αντιμετωπιστεί είναι η ύπαρξη συσχετίσεων. Συγκεκριμένα, υπάρχει μια γενική τάση όλων των Satisfying Assignments προς την ανάθεση που προκύπτει αν θέσουμε κάθε μεταβλητή αληθής ή ψευδής ανάλογα με την αληθοτιμή που προτιμούν οι περισσότεροι γειτονικοί περιορισμοί, καθώς έτσι αυξάνεται το αναμενόμενο πλήθος των ικανοποιημένων περιορισμών. Θα ορίσουμε ένα κατάλληλο υποσύνολο του συνόλου των χρωματισμών ώστε δύο τυχαία επιλεγμένοι χρωματισμοί αυτού του υποσυνόλου φαίνονται ασυσχέτιστοι. Θα ορίσουμε τώρα τις αναθέσεις τύπων, τις οποίες μπορούμε να σκεφτούμε ως προτιμήσεις των ακμών να λάβουν κάθε χρώμα.

Ορισμός 5. Μια ανάθεση τύπων του Φ είναι μία απεικόνιση $\theta : \mathcal{L} \rightarrow P(\{r, b, g, y\})$ που αντιστοιχεί σε κάθε κλώνο j ενός γράμματος l μια κατανομή πάνω στα χρώματα του παραπάνω μοντέλου, ενώ ικανοποιεί τις συνθήκες:

- Για κάθε γράμμα $l \in L$ και κάθε δύο κλώνους του j, j' (ισοδύναμα για κάθε μεταβλητή και κάθε δύο ομόσημες συνορεύουσες ακμές του) ισχύει $\theta_{i,j}^z = \theta_{i,j'}^z \quad \forall z \in \{0, 1, *\}$.
- Για κάθε γράμμα l και για κάθε κλώνο j του l και j' του $\neg l$ (ισοδύναμα για κάθε μεταβλητή και κάθε δύο ετερόσημες συνορεύουσες ακμές της) ισχύει $\theta_{i,j}^* = \theta_{-l,j'}^*$ και $\theta_{i,j}^1 = \theta_{-l,j'}^0$.

Παρατηρείστε ότι η πρώτη συνθήκη επιτρέπει διαφοροποιήσεις μεταξύ των κλώνων του ίδιου γράμματος μόνο στον μοιρασμό της μάζας στο 1 στα χρώματα $\{r, b\}$. Ίδανικά, θα θέταμε τις παραπάνω πιθανότητες απλά ίσες με τις συχνότητες εμφάνισης κάθε χρώματος στους διαφορετικούς έγκυρους χρωματισμούς του G . Ωστόσο, η απεικόνιση αυτή δεν είναι ιδιαίτερα εύχρηστη, καθώς υπολογισμοί με αυτήν είναι δύσκολοι. Αντί αυτού, θα εκμεταλλευτούμε τις εκτιμήσεις του αλγορίθμου Survey Propagation. Συγκεκριμένα, για μεταβλητές των οποίων τα αντίστοιχα γράμματα τους ικανοποιούν:

$$\max \left(\left| d_{x_i} - \frac{K\alpha}{2} \right|, \left| d_{\neg x_i} - \frac{K\alpha}{2} \right| \right) \leq K^3 2^{\frac{K}{2}}$$

δηλαδή για μεταβλητές των οποίων το πλήθος γειτονικών πλήρων και διακεκομμένων ακμών δεν απέχει υπερβολικά από την αναμενόμενη τιμή τους, ο Αλγόριθμος Survey Propagation προβλέπει την εξής κατανομή πάνω στα $\{0, 1, *\}$:

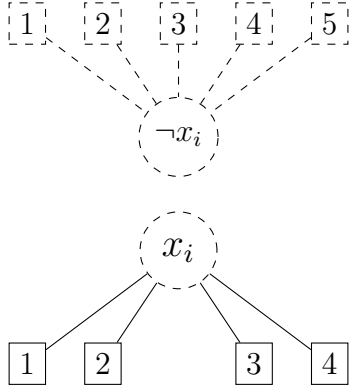
$$\mathbb{P}[\zeta(x_i) = z | d_{x_i}, d_{\neg x_i}] = \begin{cases} \frac{1}{2} + \frac{d_{x_i} - d_{\neg x_i}}{2^{K-1}} - 2^{-K-2}, & z = 1 \\ \frac{1}{2} - \frac{d_{x_i} - d_{\neg x_i}}{2^{K-1}} - 2^{-K-2}, & z = 0 \\ 2^{-K-1}, & z = * \end{cases} \quad (2.44)$$

Όπου αγνοήσαμε όρους τάξης $o(2^{-K})$. Τις εκτιμήσεις αυτές μπορεί να λάβει κανείς μέσω των μεταβλητών η που ορίσαμε σε προηγούμενη παράγραφο καθώς και την ασυμπτωτική συμπεριφορά τους, η οποία δίνει $\eta \sim 2^{-K}$. Όπως δείχνουν οι συγγραφείς, μπορούμε χωρίς βλάβη να αφαιρέσουμε μεταβλητές των οποίων το πλήθος πλήρων ή διακεκομμένων ακμών δεν ικανοποιεί την παραπάνω υπόθεση, καθώς και περιορισμούς που περιέχουν περισσότερες από δύο τέτοιες μεταβλητές. Το γράφημα που προκύπτει περιέχει σχεδόν όλες τις μεταβλητές και κάθε Satisfying Assignment αυτού επεκτείνεται σε Satisfying Assignment του αρχικού γραφήματος. Το γράφημα G' που

προκύπτει αντιστοιχεί σε στιγμιότυπο Φ' με n μεταβλητές και m περιορισμούς μήκους $\kappa \in \{K, K-1, K-2\}$ και επαληθεύει:

$$\liminf_{n \rightarrow \infty} \mathbb{P}[\Phi \text{ is Satisfiable}] \geq \liminf_{n \rightarrow \infty} \mathbb{P}[\Phi' \text{ is Satisfiable}] \quad (2.45)$$

Είμαστε τώρα σε θέση να ορίσουμε την προτίμηση που θέλουμε να έχουν οι ακμές-κλώνοι στο κατάλληλο υποσύνολο έγκυρων χρωματισμών. Είδαμε ότι για κάθε μεταβλητή η εκτίμηση του αλγορίθμου Survey Propagation (2.44) εξαρτάται μόνο από το πλήθος γειτονικών πλήρων και διακεκομμένων ακμών. Θα επεκτείνουμε τώρα την παραπάνω κατανομή σε κατανομή πάνω στα χρώματα κάθε ακμής. Επειδή αυτά εξαρτώνται και από τις υπόλοιπες ακμές του γειτονικού περιορισμού κάθε ακμής, θα ορίσουμε τύπους γραμμάτων και περιορισμών.



Σχήμα 2.4: Ο τύπος του γράμματος x_i . Σε κάθε ακμή αντιστοιχούμε κατανομή στα χρώματα

Ο τύπος κάθε γράμματος ορίζεται να είναι ένα διάνυσμα τεσσάρων θέσεων $\theta_i = (d_i, d_{-i}, (\theta_{i,j})_{j \in d_i}, (\theta_{-i,j'})_{j' \in d_{-i}})$ το οποίο μας δίνει πληροφορία για το πλήθος κλώνων αυτού, το πλήθος κλώνων της άρνησής του, και τις κατανομές-προτιμήσεις αυτών στα χρώματα. Ορίζουμε επίσης τύπους περιορισμών, οι οποίοι συνδυάζουν απλά τους τύπους των γραμμάτων σε κάθε συνιστώσα τους. Ένας περιορισμός για παράδειγμα, που περιέχει τους κλώνους $(l_1, j_1), (l_2, j_2), (l_3, j_3)$ σε διάζευξη θα έχει τύπο $\lambda = (\theta_{l_1, j_1}, \theta_{l_2, j_2}, \theta_{l_3, j_3}) := (\lambda_1, \lambda_2, \lambda_3)$. Με αυτόν τον τρόπο μπορούμε τώρα σε επίπεδο περιορισμών να ορίσουμε τη κατάλληλη κατανομή πάνω στα χρώματα για κάθε ακμή. Αφετηρία αποτελούν οι εκτιμήσεις $\lambda_j^1, \lambda_j^0, \lambda_j^*$ που προβλέπει ο αλγόριθμος Survey Propagation (2.44) και που αναφέραμε παραπάνω.

Αν $\lambda = (\lambda_1, \dots, \lambda_\kappa)$ ένας τύπος περιορισμών, ορίζουμε τις εξής κατανομές των χρωμάτων $(\Lambda_1, \dots, \Lambda_\kappa)$ με $\Lambda_j \in \mathcal{P}(\{r, g, b, y\}) \quad \forall j \in [\kappa]$:

$$\begin{aligned} \Lambda_j^r &= (\lambda_j^1 + \lambda_j^*) \prod_{j' \neq j} \lambda_{j'}^0 \\ \Lambda_j^b &= \lambda_j^1 - \Lambda_j^r \\ \Lambda_j^y &= \lambda_j^0 \\ \Lambda_j^g &= \lambda_j^* (1 - \prod_{j' \neq j} \lambda_{j'}^0) \end{aligned}$$

Αυτή η κατανομή πάνω σε κάθε ακμή ορίζει την κατάλληλη ανάθεση τύπων, την ο-

ποία θα ονομάσουμε θ -τύπο. Τους τύπους γραμμάτων και περιορισμών που ορίζονται μέσω αυτής της ανάθεσης ονομάζουμε θ -τύπους γραμμάτων και θ -τύπους περιορισμών αντίστοιχα. Για κάθε θ -τύπο γράμματος, η κατανομή των κλώνων του στα χρώματα εξαρτάται μόνο από τους βαθμούς του γράμματος και της άρνησης του, καθώς και τους βαθμούς των γραμμάτων που βρίσκονται σε κοινό περιορισμό με αυτά. Ως αποτέλεσμα, όπως δείχνουν οι συγγραφείς, έχουμε μη φραγμένο πλήθος γραμμάτων και περιορισμών που ακολουθούν έναν θ -τύπο γράμματος και περιορισμού αντίστοιχα. Αν T είναι το σύνολο των θ -τύπων γραμμάτων και T^* το σύνολο των θ -τύπων περιορισμών, τότε ορίζουμε θ -χρωματισμούς τους χρωματισμούς που σέβονται την παραπάνω προτίμηση των ακμών, δηλαδή:

Ορισμός 6. Ένας χρωματισμός ξ ονομάζεται

θ – χρωματισμός του Φ εάν ικανοποιεί τις παρακάτω συνθήκες:

- Για κάθε $t \in T$, για κάθε κλώνο h του t και για κάθε χρώμα $z \in \{r, b, g, y\}$ έχουμε $|\{l \in L_t : \xi(l, h) = z\}| \propto \theta_{t,h}^z$,
Όπου σταθερά κανονικοποίησης είναι το πλήθος γραμμάτων που ακολουθούν αυτόν τον θ -τύπο.
- Για κάθε $\lambda \in T_\theta^*$, για κάθε συνιστώσα j του λ και για κάθε χρώμα $z \in \{r, y\}$ έχουμε $|\{i \in M_\lambda : \xi(\lambda_j) = z\}| \propto \lambda_j^z$,
Όπου η σταθερά κανονικοποίησης είναι το πλήθος περιορισμών που ακολουθούν αυτόν τον θ -τύπο.

Αν για παράδειγμα η πρώτη ακμή ενός θ -τύπου γράμματος έχει πιθανότητα-προτίμηση 0.3 κίτρινου χρώματος, τότε το 1 λέει ότι σε κάθε θ -χρωματισμό θέλουμε σε κλάσμα 0.3 των γραμμάτων αυτού του θ -τύπου να είναι κίτρινη η πρώτη τους ακμή. Αν η δεύτερη ακμή σε έναν περιορισμό έχει πιθανότητα-προτίμηση 0.1 κόκκινου χρώματος, το 2 λέει ότι σε κλάσμα 0.1 των περιορισμών αυτού του θ -τύπου θα είναι η δεύτερη ακμή κόκκινη.

Αν \mathcal{T} είναι η ελάχιστη σ-άλγεβρα ως προς την οποία όλοι οι θ -τύποι γραμμάτων και περιορισμών είναι μετρήσιμοι, τότε δεδομένης της \mathcal{T} ένα τυχαίο στιγμιότυπο μπορεί παραχθεί ως εξής:

1. Διάλεξε τυχαία ένα διάνυσμα $(\lambda_1, \dots, \lambda_m)$ από θ -τύπους περιορισμών με την πιθανότητα επιλογής κάθε θ -τύπου ανάλογη του πλήθους περιορισμών που το ακολουθούν, και ανεξάρτητα από τις υπόλοιπες επιλογές.
2. Διάλεξε τυχαία και ομοιόμορφα έναν αντίστοιχο περιορισμό για κάθε θ -τύπο περιορισμών και επέλεξε τυχαία αντιστοιχία κλώνων στις συνιστώσες αυτών, υπό την συνθήκη ότι αυτοί έχουν όλοι τον ίδιο θ -τύπο με την συνιστώσα στην οποία αντιστοιχούνται.

Από την παραπάνω κατασκευή έχουμε:

$$\mathbb{P}[\Phi' \text{ is Satisfiable}] = \mathbb{E}[\mathbb{P}[\Phi' \text{ is Satisfiable}|\mathcal{T}]] \quad (2.46)$$

Πριν προχωρήσουμε στην μέθοδο των ροπών, θα πρέπει ακόμα να προσέξουμε δύο λεπτομέρειες. Θέλουμε να βρούμε Satisfying Assignments, όχι απλά καλύμματα. Θα ονομάζουμε ένα κάλυμμα επεκτάσιμο αν υπάρχει τρόπος να τεθούν αληθοτιμές στις μεταβλητές που απεικονίζονται στο * ώστε να πάρουμε Satisfying Assignment. Επίσης, μια τεχνική λεπτομέρεια που χρειάζεται στον υπολογισμό της δεύτερης ροπής είναι η έννοια του διαχωρίσιμου καλύμματος. Με Z' το πλήθος έγκυρων θ -χρωματισμών του Φ , θα ονομάζουμε ένα κάλυμμα διαχωρίσιμο εάν δεν υπάρχουν περισσότερα από $\mathbb{E}[Z'|\mathcal{T}]$ έγκυροι θ -χρωματισμοί ζ του Φ ώστε

$$\frac{1}{2n} \left| \left\{ l \in L' : \hat{\xi}(l) \neq \hat{\zeta}(l) \right\} \right| \notin \left[\frac{1}{2} - 2^{-0.49K}, \frac{1}{2} - 2^{-0.49K} \right]$$

Το οποίο αντιστοιχεί στην διαχωρισιμότητα των συστάδων που προβλέπει η μέθοδος 1RSB Cavity

Ορισμός 7. Ένας θ -χρωματισμός ξ είναι καλός αν είναι έγκυρος, επεκτάσιμος και διαχωρίσιμος

Ορίζουμε Z το πλήθος των καλών θ -χρωματισμών. Οι μέθοδοι των ροπών τότε δίνουν

Πρόταση 2. Υπάρχει $\varepsilon_K = \Theta(2^{-\frac{K}{2}})$ ώστε για $\alpha = 2^K \log 2 - \frac{1-\log 2}{2} - \varepsilon_K$ να είναι $\mathbb{E}[Z|\mathcal{T}] = e^{\Omega(n)}$ με ψηλή πιθανότητα

Πρόταση 3. Αν $\varepsilon_K = O(2^{-\frac{K}{2}})$ είναι τέτοιο ώστε για $\alpha = 2^K \log 2 - \frac{1-\log 2}{2} - \varepsilon_K$ να είναι $\mathbb{E}[Z|\mathcal{T}] = e^{\Omega(n)}$ με ψηλή πιθανότητα, τότε $\mathbb{E}[Z^2|\mathcal{T}] \leq O(\mathbb{E}[Z|\mathcal{T}]^2)$ με ψηλή πιθανότητα

Η πρόταση 3 μαζί με την πρόταση 4 και την μέθοδο δεύτερης ροπής (2) δίνει το κάτω φράγμα του κατωφλιού το οποίο συμφωνεί με το άνω φράγμα, και οπότε αποδεικνύεται η εικασία. Για λεπτομερείς αποδείξεις των παραπάνω προτάσεων παραπέμπουμε στο [13].

Βιβλιογραφία

- [1] J. Ding, A. Sly, and N. Sun, “Proof of the satisfiability conjecture for large k ,” *Annals of Mathematics*, vol. 196, 07 2022.
- [2] J. Franco and M. Paull, “Probabilistic analysis of the davis putnam procedure for solving the satisfiability problem,” *Discrete Applied Mathematics*, vol. 5, no. 1, pp. 77–87, 1983.
- [3] M. te Chao and J. Franco, “Probabilistic analysis of a generalization of the unit clause literal selection heuristic for the k -satisfiability problem,” *INFORMATION SCIENCE*, vol. 51, pp. 289–314, 1990.
- [4] A. Goerdt, “A threshold for unsatisfiability,” *Journal of Computer and System Sciences*, vol. 53, no. 3, pp. 469–486, 1996.
- [5] S. Kirkpatrick and B. Selman, “Critical behavior in the satisfiability of random boolean expressions,” *Science*, vol. 264, no. 5163, pp. 1297–1301, 1994.
- [6] O. Dubois and Y. Boufkhad, “A general upper bound for the satisfiability threshold of random r -sat formulae,” *Journal of Algorithms*, vol. 24, no. 2, pp. 395–420, 1997.
- [7] E. Friedgut and J. Bourgain, “Sharp thresholds of graph properties, and the k -sat problem,” *Journal of the American Mathematical Society*, vol. 12, no. 4, pp. 1017–1054, 1999.
- [8] D. Achlioptas and C. Moore, “Random k -sat: Two moments suffice to cross a sharp threshold,” *SIAM Journal on Computing*, vol. 36, no. 3, pp. 740–762, 2006.
- [9] D. Achlioptas and Y. Peres, “The threshold for random k -sat is $2k \ln(2) - o(k)$,” vol. 17, pp. 223–231, 01 2003.
- [10] D. Achlioptas and F. Ricci-Tersenghi, “On the solution-space geometry of random constraint satisfaction problems,” in *Proceedings of the Thirty-Eighth Annual*

ACM Symposium on Theory of Computing, STOC '06, (New York, NY, USA), p. 130–139, Association for Computing Machinery, 2006.

- [11] M. Mezard and R. Zecchina, “Random k-satisfiability problem: From an analytic solution to an efficient algorithm,” *Physical review. E, Statistical, nonlinear, and soft matter physics*, vol. 66, p. 056126, 12 2002.
- [12] S. Mertens, M. Mezard, and R. Zecchina, “Threshold values of random k-sat from the cavity method,” *Random Structures and Algorithms*, vol. 28, 05 2006.
- [13] A. Coja-Oghlan and K. Panagiotou, “The asymptotic k-sat threshold,” *Advances in Mathematics*, vol. 288, pp. 985–1068, 01 2016.
- [14] M. Mézard and A. Montanari, *Information, Physics, and Computation*. Oxford University Press, 01 2009.
- [15] A. Braunstein and R. Zecchina, “Survey propagation as local equilibrium equations,” *J Stat Mech Theory*, vol. 2004, 12 2003.
- [16] A. Braunstein, M. Mézard, and R. Zecchina, “Survey propagation: An algorithm for satisfiability,” *Random Structures & Algorithms*, vol. 27, no. 2, pp. 201–226, 2005.
- [17] D. Brillinger, “The calculation of cumulants via conditioning,” *Annals of the Institute of Statistical Mathematics*, vol. 21, pp. 215–218, 12 1969.
- [18] P. J. Smith, “A recursive formulation of the old problem of obtaining moments from cumulants and vice versa,” *The American Statistician*, vol. 49, no. 2, pp. 217–218, 1995.