Πιθανοθεωρητικές Μέθοδοι στην Ανάλυση Λογικών Κυκλωμάτων

Μεταπτυχιακή Εργασία

Δημήτρης Καλοφικάκης
Επιβλέπων: Μιχάλης Κολουντζάκης
μέλη της Επιτροπής:
Ελένη Τζανάκη, Νίκος Φραντζικινάκης

12 Σεπτεμβρίου 2020

Περίληψη

Το κείμενο που ακολουθεί αποτελεί διπλωματική εργασία που εκπονήθηκε στο πλαίσιο του μεταπτυχιακού προγράμματος «Μαθηματικά και Εφαρμογές τους» του Τμήματος Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης. Με άξονα ένα βασικό πρόβλημα όπως περιγράφεται στο βιβλίο «Gems of Theoretical Computer Science»[1] του Uwe Schöning, αναδεικνύεται ο ρόλος της Πιθανοθεωρητικής Μεθόδου στην Ανάλυση Λογικών Κυκλωμάτων.

Αρκετά από τα μαθηματικά προβλήματα που τίθενται, ενέχουν σημαντική εγγενή δυσκολία και συχνά μοναδική διέξοδος μοιάζει η επιστράτευση της Θεωρίας Πιθανοτήτων. Το πρόβλημα που εξετάζεται στην εργασία αυτή είναι το κατά πόσο λογικά κυκλώματα μικρής πολυπλοκότητας –συγκεκριμένα της κλάσης AC^0– μπορούν να εκφράσουν λογικές συναρτήσεις ισοτιμίας. Αποδεικνύεται ότι κάτι τέτοιο είναι αδύνατο.

Αναλύονται δύο αποδείξεις με διαφορετικές οπτικές, με καίρια εμπλοκή της Πιθανοθεωρητικής Μεθόδου και στις δύο. Στην πρώτη απόδειξη η προσέγγιση είναι αναλυτική και σημείο κλειδί της επιχειρηματολογίας είναι η τεχνική του τυχαίου περιορισμού. Η δεύτερη απόδειξη έχει αλγεβρική λογική και αποτελείται από δύο βήματα: στο πρώτο, με πιθανοθεωρητική τεχνική, γίνεται μια στενή συσχέτιση των κυκλωμάτων με τον χώρο πολυωνύμων μικρής πολυπλοκότητας· στο δεύτερο βήμα προκύπτει το συμπέρασμα με σύγκριση των διαστάσεων των γραμμικών χώρων που αναδεικνύονται στο πρώτο.

Από την πρώτη απόδειξη, προκύπτει ότι λογικά κυκλώματα πολυωνυμικού μεγέθους πρέπει να έχουν βάθος τουλάχιστον λογαριθμικό για να μπορούν να υπολογίσουν συναρτήσεις ισοτιμίας, ενώ από τη δεύτερη απόδειξη το φράγμα αυτό βελτιώνεται σε

$$\Omega\left(\frac{\log n}{\log\log n}\right)$$

Ευχαριστίες

Ευχαριστώ τον επιβλέποντα, καθηγητή Μιχάλη Κολουντζάκη, για την άψογη συνεργασία και την υπομονή του.

Αφιέρωση

Η εργασία αυτή αφιερώνεται στους μικρούς ήρωες της επιστημονικής περιοχής που αναφέρεται η εργασία: Merrick Furst, James Saxe, Michael Sipser, Miklós Ajtai, Alexander Razborov, Roman Smolensky.

Αφιερώνεται ιδιαίτερα στην Bella Abramovna Subbotovskaya που ουσιαστικά με τους τυχαίους περιορισμός έδωσε το έναυσμα για την πορεία προς το Switching Lemma, αλλά και στον ασκητή της επιστήμης, Erdős Pál που κυριολεκτικά καθόρισε την Πιθανοθεωρητική Μέθοδο. Και οι δύο, με διαφορετικό τρόπο, θυσίασαν τη ζωή τους, ασυμβίβαστα, στον βωμό της επιστήμης.

Αφιερώνεται, τέλος, σε όλη την ακολουθία των ανθρώπων, σε όλη την έκταση του χρόνου, που άοκνα μόχθησαν και μοχθούν πάνω στην επιστήμη, οικοδομώντας συλλογικά το περιεχόμενο, μικρό μέρος του οποίου παρουσιάστηκε σε αυτή την εργασία.

Περιεχόμενα

1 Εισαγωγή

Η Θεωρία Πιθανοτήτων, πέρα από την προφανή σημασία της ως αυτόνομο αντικείμενο, από το δεύτερο μισό του 20ού αιώνα έχει διεισδύσει σε πεδία μαθηματικών με φαινόμενα που δεν περιέχουν καμιά τυχαιότητα. Η διείσδυση αυτή δεν είναι μόνο εργαλειακού χαρακτήρα, αλλά και διαφορετικής οπτικής και διαίσθησης, δίνοντας έτσι σοβαρή ώθηση –ή ακόμα και διέξοδο– σε ορισμένου τύπου δύσκολα προβλήματα. Τα προβλήματα αυτά συνήθως έχουν ισχυρή συνδυαστική και αλγοριθμική διάσταση, ενώ συχνά, όταν επιδιώκεται η απόδειξη ύπαρξης ενός αντικειμένου, εμπεριέχουν σημαντική δυσκολία κατασκευής παραδείγματος. Αυτά τα χαρακτηριστικά εμφανίζονται σε πολλά μαθηματικά προβλήματα που τίθενται από την Επιστήμη Υπολογιστών, δημιουργώντας έτσι ένα πεδίο κατ' εξοχήν κατάλληλο για εφαρμογή πιθανοθεωρητικών μεθόδων.

Το συγκείμενο της παρούσας εργασίας είναι η Θεωρία Πολυπλοκότητας και ειδικότερα η Πολυπλοκότητα Λογικών Κυκλωμάτων, τα οποία οποία αποτελούν έναν αφαιρετικό τρόπο αναπαράστασης Λογικών Συναρτήσεων:

$$\{\textit{αληθές}, \textit{ψευδές}\}^n \to \{\textit{αληθές}, \textit{ψευδές}\}\,, n \in \mathbb{N}$$

Η μελέτη επικεντρώνεται στις Λογικές Συναρτήσεις γιατί μπορούν να εκφράσουν οποιονδήποτε υπολογισμό· υπολογισμός μπορεί να θεωρηθεί η μετατροπή μιας πληροφορίας από μια μορφή σε μια άλλη. Κάθε πληροφορία μπορεί σχετικά εύκολα να απεικονιστεί ως μια πλειάδα δυαδικών ψηφίων («bit string»). Συνεπώς αν η αρχική πληροφορία έχει μήκος n και η μετατροπή της μήκος m, τότε ο υπολογισμός μπορεί να εκφραστεί από μια συνάρτηση $\{0,1\}^n \to \{0,1\}^m$. Χωρίς βλάβη της γενικότητας, υποθέτουμε $m = 1$.

Γενικότερα η Θεωρία Πολυπλοκότητας [2] έχει σκοπό την ταξινόμηση υπολογιστικών προβλημάτων, κατατάσσοντάς τα σε κλάσεις, ιεραρχικά, σύμφωνα με την εγγενή δυσκολία τους· δηλαδή σύμφωνα με την ελάχιστη απαίτησή τους σε υπολογιστικούς πόρους συναρτήσει του μεγέθους των αρχικών δεδομένων (είσοδος). Υπό αυτό το πρίσμα μιλάμε για αποδοτικότητα ή μη, μιας λύσης ενός προβλήματος. Ως υπολογιστικό πρόβλημα εννοούμε ένα πρόβλημα το οποίο μπορεί να λυθεί με αλγοριθμικό τρόπο και υποθέτουμε ότι ο αλγόριθμος εκτελείται από μια αφηρημένη μηχανή, που την ονομάζουμε μοντέλο υπολογισμού. Η Μηχανή Turing [3] είναι το πιο βασικό παράδειγμα και μέχρι στιγμής δεν έχει κατασκευαστεί άλλο μοντέλο το οποίο να υπολογίζει κάτι που να μην μπορεί να το υπολογίσει μια Μηχανή Turing, τουλάχιστον το ίδιο αποδοτικά. Άλλα μοντέλα υπολογισμού [4] είναι οι Μηχανές Πεπερασμένων Καταστάσεων (FSM), οι Μηχανές Αυθαίρετης Πρόσβασης (RAM), τα Λογικά Κυκλώματα, κ.α.

Ο λόγος ύπαρξης διαφορετικών μοντέλων είναι ότι μας δίνουν διαφορετικές οπτικές και μαθηματικά εργαλεία, από τα οποία ευνοείται η μελέτη διαφορετικών κλάσεων πολυπλοκότητας. Επίσης, η φύση του μοντέλου καθορίζει τους υπολογιστικούς πόρους βάσει των οποίων εκτιμούμε την ελάχιστη απαίτηση των προβλημάτων. Για παράδειγμα, στις Μηχανές Turing οι πόροι είναι ο χρόνος (πλήθος βημάτων εκτέ-

λεσης) και ο χώρος (μνήμη), ενώ στα Λογικά Κυκλώματα είναι το βάθος (μέγιστο μονοπάτι) και το μέγεθος (πλήθος πυλών).

Ένα από τα βασικότερα ζητήματα της Θεωρίας Πολυπλοκότητας είναι η σχέση των κλάσεων NP και P [5]. Η πρώτη κλάση περιλαμβάνει τα προβλήματα για τα οποία μια δοσμένη λύση μπορεί να επαληθευτεί αποδοτικά, δηλαδή σε πολυωνυμικής τάξης χρόνο. Η δεύτερη κλάση περιλαμβάνει τα προβλήματα που μπορούν να λυθούν αποδοτικά. Το ερώτημα αν οι P και NP ταυτίζονται, είναι από τα σημαντικότερα και πιο καταζητούμενα ανοιχτά ερωτήματα των σύγχρονων μαθηματικών [6].

Προς αυτή την κατεύθυνση, η μελέτη κάτω φραγμάτων στα Λογικά Κυκλώματα θεωρείται σημαντική [7] γιατί μοιάζει να είναι ένα ενδεδειγμένο μονοπάτι για την απόδειξη ότι $P \neq NP$. Αυτό γιατί κατ' αρχάς, τα κυκλώματα έχουν απλούστερο ορισμό από ότι οι Μηχανές Turing και είναι πιο δόκιμα για συνδυαστική ανάλυση. Επίσης, η πολυπλοκότητά τους είναι στενά συνδεδεμένη με την πολυπλοκότητα των Μηχανών Turing [8]: αν μία λογική συνάρτηση n μεταβλητών έχει χρονική πολυπλοκότητα $\mathcal{O}(T(n))$ τότε το αντίστοιχο κύκλωμα που την υπολογίζει έχει πολυπλοκότητα –δηλαδή μέγεθος– $\mathcal{O}\left(T(n)\log T(n)\right)$ [9]. Αυτό σημαίνει ότι ένα κάτω φράγμα στην πολυπλοκότητα κυκλωμάτων που υπολογίζουν μια συνάρτηση, συνεπάγεται άμεσα ένα κάτω φράγμα στη χρονική πολυπλοκότητα αυτής της συνάρτησης. Οπότε η εξεύρεση μιας συνάρτησης $f \in NP$ η οποία εκφράζεται από ένα κύκλωμα με κάτω φράγμα πολυπλοκότητας μεγαλύτερο της πολυωνυμικής τάξης, θα σήμαινε ότι $P \neq NP$.

Το πρόβλημα που επεξεργαζόμαστε σε αυτή την εργασία αφορά στη σχέση ανάμεσα σε λογικές συναρτήσεις και σε κυκλώματα μικρής πολυπλοκότητας. Ειδικότερα, εξετάζεται η σχέση των συναρτήσεων ισοτιμίας με την κλάση AC^0. Η κλάση AC^k ορίζεται ως το σύνολο των λογικών συναρτήσεων n μεταβλητών, οι οποίες μπορούν να εκφραστούν από κυκλώματα πολυωνυμικού μεγέθους και βάθους $\mathcal{O}\left(\log^k n\right)$. Το ερώτημα που τίθεται είναι κατά πόσο κυκλώματα σταθερού βάθους, δηλαδή για $k = 0$, μπορούν να υπολογίσουν συναρτήσεις ισοτιμίας. Το ερώτημα αυτό είναι σημαντικό γιατί οι συναρτήσεις ισοτιμίας ουσιαστικά αποτελούν τα βασικά δομικά στοιχεία των λογικών συναρτήσεων· μάλιστα, συνιστούν ορθοκανονική βάση του 2^n-διάστατου γραμμικού χώρου των λογικών συναρτήσεων n μεταβλητών.

Η απάντηση στο παραπάνω ερώτημα, όπως θα δούμε, είναι αρνητική και αποδεικνύεται με την ανάδειξη κάτω φραγμάτων στο βάθος των κυκλωμάτων. Παρουσιάζονται δύο αποδείξεις [10], με την Πιθανοθεωρητική Μέθοδο να έχει καίριο ρόλο και στις δύο, δίνοντας τη δυνατότητα σύνθεσης επιχειρημάτων ύπαρξης και εφικτότητας («impossibility»). Στην πρώτη απόδειξη (Κεφ. 2), όπου προκύπτει ένα κάτω φράγμα $\Omega\left(\log n\right)$, η οπτική είναι αναλυτική· δηλαδή αξιοποιούνται λειτουργικές ιδιότητες των εμπλεκόμενων μαθηματικών αντικειμένων. Στη δεύτερη απόδειξη (Κεφ. 3), όπου το κάτω φράγμα βελτιώνεται σε $\Omega\left(\frac{\log n}{\log\log n}\right)$, η οπτική είναι αλγεβρική και αξιοποιούνται δομικές ιδιότητες μέσω αναγωγής στον χώρο των πολυωνύμων μικρού βαθμού.

Η ανάλυση των αποδείξεων έγινε με επίκεντρο την εφαρμογή της Πιθανοθεωρητικής Μεθόδου και με στόχο την ανάδειξη τόσο της τεχνικής όσο και της διαισθητικής

προσέγγισης που υπεισέρχεται στην επιχειρηματολογία. Επίσης, αν και το γενικότερο πλαίσιο εμπίπτει στην τομή των Μαθηματικών και της Επιστήμης Υπολογιστών, έγινε προσπάθεια ώστε το εκφραστικό ύφος της εργασίας να τείνει προς την πλευρά των Μαθηματικών. Εξαίρεση αποτελεί η ορολογία των κυκλωμάτων, όπου για λόγους απλότητας των διατυπώσεων μιλάμε για «είσοδο», «έξοδο» και «πύλες».

Επίσης, τα επιδιωκόμενα αποτελέσματα είναι κατά κάποιο τρόπο ποιοτικά. Μας ενδιαφέρει η ασυμπτωτική συμπεριφορά και όχι τόσο οι παραμετρικές λεπτομέρειες. Για τον λόγο αυτό χρησιμοποιείται ο ασυμπτωτικός συμβολισμός, που ουσιαστικά εκφράζει την τάξη μεγέθους μιας συνάρτησης.

Ορισμός 1.1 (Συμβολισμός «Big-Oh»).
Έστω $f, g : \mathbb{N} \to \mathbb{N}$. *Τότε, γράφουμε* $f = \mathcal{O}(g)$ *αν υπάρχει σταθερά* c *έτσι ώστε,* $f(n) \leq cg(n)$ *για κάθε αρκούντως μεγάλο* n. *Επίσης, γράφουμε* $f = \Omega(g)$ *όταν* $g = \mathcal{O}(f)$.

Μερικές προφανείς ιδιότητες:

- $f(n) + g(n) = \mathcal{O}(f(n) + g(n))$
- $f(n) \cdot g(n) = \mathcal{O}(f(n) \cdot g(n))$
- $\mathcal{O}(cf(n)) = \mathcal{O}(f(n)), c$ σταθερά.
- Στην πρόσθεση, οι μικρότερες τάξεις απορροφούνται από τις μεγαλύτερες, π.χ. $\mathcal{O}(n^3) + \mathcal{O}(\log n) = \mathcal{O}(n^3)$ ή $\mathcal{O}(2^n) + \mathcal{O}(n^k) = \mathcal{O}(2^n)$.

Η συγγραφή της εργασίας αυτής έγινε έχοντας κατά νου αναγνώστες που δεν έχουν απαραίτητα προηγούμενες γνώσεις στη Θεωρία Πολυπλοκότητας. Η ποιοτική περιγραφή του πλαισίου της εργασίας σε αυτό το κεφάλαιο θα πρέπει να είναι αρκετή για μπορεί κάποιος να έχει αίσθηση για το πού τοποθετείται το εξεταζόμενο πρόβλημα και ποια η σημασία του. Επίσης, η εφαρμογή της Πιθανοθεωρητικής Μεθόδου στα Κεφάλαια 2 και 3 δεν απαιτεί προχωρημένες γνώσεις στη Θεωρία Πιθανοτήτων. Χρειάζεται κάποιο επίπεδο μαθηματικής ωριμότητας, αλλά τεχνικά αρκεί η εξοικείωση με τα βασικά της Διακριτής Πιθανότητας, καθώς και με τα βασικά της Γραμμικής Άλγεβρας.

Για τις Λογικές Συναρτήσεις και τα Λογικά Κυκλώματα, γίνεται μια σύντομη αναφορά στην παράγραφο 1.1, ενώ στην παράγραφο 1.2 δίνεται μια σύντομη περιγραφή της Πιθανοθεωρητικής Μεθόδου γενικά.

1.1 Λογικές Συναρτήσεις και Κυκλώματα

Λογική Συνάρτηση ονομάζουμε μια συνάρτηση της μορφής

$$\{\textit{αληθές}, \textit{ψευδές}\}^n \to \{\textit{αληθές}, \textit{ψευδές}\}, n \in \mathbb{N}$$

Η αναπαράσταση μιας Λογικής Συνάρτησης μπορεί να γίνεται με διαφορετικούς τρόπους αναλόγως το μαθηματικό περιβάλλον του εξεταζόμενου προβλήματος. Οι

αναπαραστάσεις που –άμεσα ή έμμεσα– χρησιμοποιούνται σε αυτή την εργασία είναι,

- $\mathbb{R}^n \supset \{0,1\}^n \to \{0,1\} \subset \mathbb{R}$, όπου το 0 αντιστοιχεί στο *ψευδές* και το 1 στο *αληθές*.
- $\mathbb{F}_2^n \to \mathbb{F}_2$, όπου το 0 αντιστοιχεί στο *ψευδές* και το 1 στο *αληθές*.
- $\mathbb{R}^n \supset \{\pm 1\}^n \to \{\pm 1\} \subset \mathbb{R}$, όπου το -1 συμβολίζει το *αληθές* και το $+1$ το *ψευδές*.

Σε κάθε περίπτωση μπορούμε να μιλάμε για Λογικές Συναρτήσεις όταν μπορούμε να συνθέτουμε τις πράξεις της λογικής σύζευξης και διάζευξης, ώστε να ισχύουν οι γνωστοί κανόνες de Morgan,

$$\begin{aligned} \neg(P \wedge Q) &= (\neg P) \vee (\neg Q) \\ \neg(P \vee Q) &= (\neg P) \wedge (\neg Q) \\ P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R) \end{aligned}$$

Για παράδειγμα, η λογική σύζευξη μπορεί να εκφραστεί από τη συνάρτηση

$$AND_2 : \{\pm 1\}^2 \to \{\pm 1\}, AND_2(x_1, x_2) = \frac{1}{2} + \frac{1}{2}x_1 + \frac{1}{2}x_2 - \frac{1}{2}x_1 x_2$$

Όπως φαίνεται, η AND_2 είναι ένα πολυγραμμικό πολυώνυμο. Αυτό ισχύει γενικότερα για κάθε λογική συνάρτηση. Μάλιστα, επειδή η συνάρτηση ισοτιμίας έχει τη μορφή, $\pi_n(x_1, \ldots, x_n) = \prod_{i=1}^n x_i$, είναι σαφές ότι κάθε λογική συνάρτηση είναι γραμμικός συνδυασμός συναρτήσεων ισοτιμίας. Εύκολα μπορεί να δει κάποιος ότι το σύνολο των λογικών συναρτήσεων n μεταβλητών είναι γραμμικός χώρος που η βάση του είναι οι συναρτήσεις ισοτιμίας.

Αν, τώρα, f είναι μία λογική συνάρτηση μίας μεταβλητής, τότε αυτή μπορεί να αναλυθεί ως εξής:

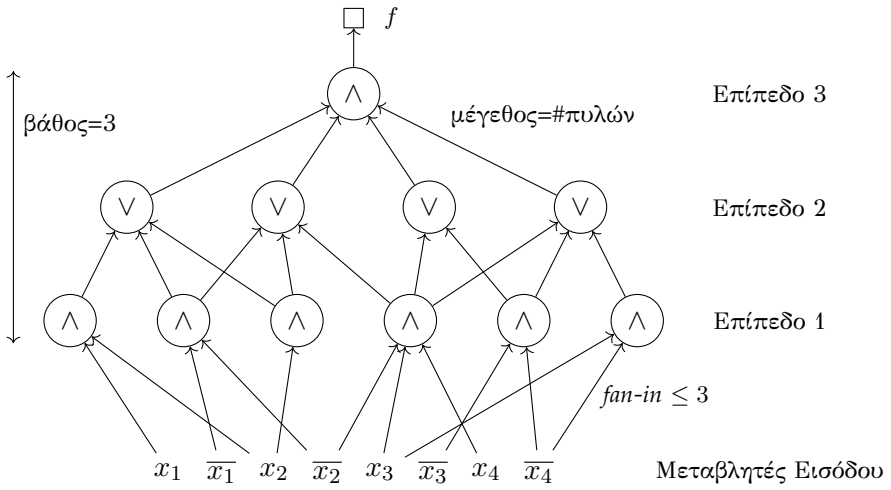
$$f(x) = f(1) \cdot x + f(0) \cdot \overline{x}$$

Η ισότητα αυτή αποτελεί το Θεώρημα Επέκτασης του Boole [11], ενώ αναφέρεται και ως το θεμελιώδες θεώρημα της Άλγεβρας Boole [12]· επεκτείνεται επαγωγικά και σε λογικές συναρτήσεις πολλών μεταβλητών:

Θεώρημα 1.2 (Θεώρημα Επέκτασης του Boole).
Έστω f λογική συνάρτηση. Τότε,

$$f(x_1, \ldots, x_n) = \sum_{i_1=0}^{1} \sum_{i_2=0}^{1} \cdots \sum_{i_k=0}^{1} x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k} f\left(1^{i_1}, 1^{i_2}, \ldots, 1^{i_k}, x_{k+1}, \cdots, x_n\right)$$

όπου, $x^i := \begin{cases} x, \text{ όταν } i = 0 \\ \overline{x}, \text{ όταν } i = 1 \end{cases}$



Ένα λογικό κύκλωμα που υπολογίζει μια συνάρτηση f, αναπαρίσταται ως ένα κατευθυνόμενο δέντρο με ρίζα, με όλες τις ακμές του να κατευθύνονται από τα φύλλα προς τη ρίζα. Τα φύλλα του δέντρου συμβολίζουν τις μεταβλητές εισόδου. Τις κορυφές του δέντρου τις ονομάζουμε **πύλες**. Υποθέτουμε ότι το δέντρο είναι ισορροπημένο και ένα σύνολο των πυλών που βρίσκεται σε ίση απόσταση από τη ρίζα, το ονομάζουμε **επίπεδο**. **Μέγεθος** του κυκλώματος ονομάζουμε το πλήθος των πυλών του και **βάθος**, το μέγιστο μήκος μονοπατιού από τη ρίζα έως τα φύλλα. Τέλος, οι πύλες στο Επίπεδο 1 ενδέχεται να έχουν άνω φράγμα στο πλήθος μεταβλητών εισόδου που επιδέχονται· αυτό το ονομάζουμε **φράγμα εισόδου** ή «**fan-in**».

Σχήμα 1.1: Ένα τυπικό λογικό κύκλωμα με πύλες *AND*, *OR* και η ορολογία του.

Το θεώρημα αυτό, στη βιβλιογραφία της σχεδίασης υπολογιστών κυκλωμάτων, αναφέρεται συχνά ως Θεώρημα Επέκτασης του Shannon, καθώς λανθασμένα αποδίδεται σε αυτόν. Αυτό οφείλεται στο ότι ο Shannon περιγράφει αυτή την επέκταση σε δημοσίευσή του [13], όπου γίνεται ουσιαστικά η πρώτη προσπάθεια μέτρησης υπολογιστικής δυσκολίας σε κυκλώματα. Βασικός σκοπός της μελέτης υπολογιστικής πολυπλοκότητας κυκλωμάτων ήταν αρχικά η ελαχιστοποίηση των υλικών στοιχείων υλοποίησης. Η γενικότερη Θεωρία Πολυπλοκότητας Αλγορίθμων ξεκινάει αργότερα, από τους Hartmanis και Stearns το 1965 [14].

Στην εργασία αυτή, παραμένοντας στο περιβάλλον της Θεωρίας Πολυπλοκότητας, ένα κύκλωμα θεωρούμε ότι είναι μια αφαιρετική αναπαράσταση μιας Λογικής Συνάρτησης. Ουσιαστικά, ένα κύκλωμα που υπολογίζει μια συνάρτηση f, είναι το δίκτυο των συνθέσεων στοιχειωδών λογικών συναρτήσεων στις οποίες μπορεί να αναλυθεί η f. Το δίκτυο αυτό το αναπαριστούμε ως ένα ακυκλικό κατευθυνόμενο γράφο του οποίου οι εσωτερικές κορυφές είναι οι στοιχειώδεις συναρτήσεις και τα φύλλα είναι οι μεταβλητές της συνάρτησης (βλ. Σχήμα 1.1).

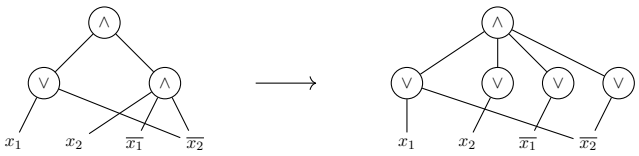
Ως προς την ορολογία, θα λέμε ότι μια συνάρτηση υπολογίζεται ή εκφράζεται από ένα κύκλωμα. Τις εσωτερικές κορυφές του γράφου που αναπαριστά το κύκλωμα τις αποκαλούμε πύλες. Τα φύλλα, που τα ονομάζουμε είσοδο του κυκλώματος, συμβολίζουν τις μεταβλητές της συνάρτησης.

Οι στοιχειώδεις συναρτήσεις που θα χρησιμοποιήσουμε είναι η λογική σύζευξη και η λογική διάζευξη:

$$AND, OR : \{0,1\}^n \to \{0,1\},$$
$$AND\,(x_1, \ldots, x_n) = 1 \Leftrightarrow \forall i \in \{1, \ldots, n\} : x_i = 1$$
$$OR\,(x_1, \ldots, x_n) = 1 \Leftrightarrow \exists i \in \{1, \ldots, n\} : x_i = 1$$

Επίσης, η είσοδος του κυκλώματος θα αποτελείται από τις μεταβλητές της συνάρτησης και τις αρνήσεις τους. Ως μεγέθη πολυπλοκότητας ενός κυκλώματος θεωρούμε το βάθος, δηλαδή το μήκος του μέγιστου μονοπατιού από τη ρίζα έως τα φύλλα, και το μέγεθος, δηλαδή το πλήθος των πυλών. Ο γενικότερος στόχος είναι η αναπαράσταση λογικών συναρτήσεων με τα μικρότερα δυνατά μεγέθη.

Αν ένα κύκλωμα βάθους t, είναι ισορροπημένο (δηλαδή όλες οι είσοδοι έχουν την ίδια απόσταση από την έξοδο), τότε στο κύκλωμα μπορούμε να μιλήσουμε για επίπεδα. Το επίπεδο 0 αποτελείται από τις μεταβλητές εισόδου, των οποίων η απόσταση από την έξοδο είναι t, το επίπεδο 1 αποτελείται από τις πύλες που η απόστασή τους από την έξοδο είναι $t-1$, κ.ο.κ. Επίσης, το μέγιστο πλήθος των μεταβλητών που επιδέχονται οι πύλες του επιπέδου θα το ονομάζουμε φράγμα εισόδου (fan-in). Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι τα κυκλώματα που εξετάζουμε είναι ισορροπημένα και ότι κάθε επίπεδο αποτελείται από πύλες του ίδιου τύπου, καθώς και ότι διαδοχικά επίπεδα έχουν διαφορετικού τύπου πύλες. Αυτό ισχύει γιατί αν μία πύλη είναι ίδιου τύπου με μια γειτονική της, μπορεί να απορροφηθεί και να προστεθούν καταχρηστικά κατάλληλες πύλες, π.χ.:



Λόγω αυτού του χαρακτηριστικού, η κλάση συναρτήσεων που θα μας απασχολήσει και αναφέραμε νωρίτερα, συμβολίζεται AC^0, από το «Alternating Class».

Περισσότερα σχετικά με τις Λογικές Συναρτήσεις και Κυκλώματα μπορεί κάποιος να δει στα βιβλία [15] και [16].

1.2 Πιθανοθεωρητική Μέθοδος

Στην παράγραφο αυτή γίνεται μια σχεδόν επιγραμματική επισκόπηση των πολύ βασικών τεχνικών της Πιθανοθεωρητικής Μεθόδου [17]. Αρχικά, μια προσπάθεια ποιοτικής περιγραφής με δυο φράσεις:

– *Πώς ακριβώς είναι, κανείς δεν ξέρει· όμως υπάρχει.*

– *Έστω ότι σε ένα κουτί υπάρχουν βόλοι. Αν γνωρίζουμε ότι η πιθανότητα, μετά από τυχαία επιλογή, να πάρουμε ένα μπλε βόλο είναι θετική, τότε ξέρουμε ότι σίγουρα υπάρχει τουλάχιστον ένας μπλε βόλος στο κουτί.*

Αυτές οι δύο φράσεις [18] –η πρώτη σχεδόν αφορισμός, η δεύτερη σχεδόν ταυτολογία– συναποτελούν το σκοπό και την κεντρική ιδέα της Πιθανοθεωρητικής Μεθόδου. Το φαινόμενο της ύπαρξης ή μη, βόλων στο κουτί δεν περιέχει καμιά τυχαιότητα· όμως, η τεκμηρίωση του συμπεράσματος βασίζεται στη Θεωρία Πιθανοτήτων. Δεν μας νοιάζει ποιος ακριβώς βόλος είναι μπλε και ποια η περιγραφή του, θέλουμε να ξέρουμε μόνο ότι σίγουρα υπάρχει, ή όχι.

Σε ένα άλλο παράδειγμα, θεωρούμε ένα πρωτάθλημα κάποιου αθλήματος με m ομάδες, όπου όλοι παίζουν με όλους, ακριβώς μία φορά [19]. Οι διοργανωτές θέλουν να δώσουν έπαθλα σε n συμμετέχοντες –τους νικητές– και θα ήθελαν να αποκλειστεί η περίπτωση κάποια ομάδα να έχει νικήσει όλους τους νικητές και να μην πάρει βραβείο. Είναι δυνατό κάτι τέτοιο; Όσο κι αν αυτό μοιάζει διαισθητικά παράδοξο, για σχετικά μικρό πλήθος νικητών είναι αδύνατο να εξασφαλιστεί η ακεραιότητά τους. Το πρόβλημα αυτό, αντιμετωπίστηκε από τον Ούγγρο μαθηματικό Erdős Pál [20], ο οποίος θεωρείται ο πατριάρχης της Πιθανοθεωρητικής Μεθόδου: απέδειξε [21] ότι αν $n \in \mathbb{N}$, τότε για όλα τα αρκούντως μεγαλύτερα m και για κάθε υποσύνολο n ομάδων, αν τα αποτελέσματα όλων των ανά δύο αναμετρήσεων επιλεγούν τυχαία (ανεξάρτητα και ομοιόμορφα), τότε με μεγάλη πιθανότητα υπάρχει μια ομάδα έξω από το σύνολο των νικητών, που έχει νικήσει και τις n ομάδες.

Συνοπτικά, η βασική διαδικασία της Πιθανοθεωρητικής Μεθόδου είναι απλή και στοιχειώδης:

Βασική Πιθανοθεωρητική Μέθοδος	
1.	Ορισμός τυχαίου πειράματος.
2.	Καθορισμός μέτρων πιθανοτήτων.
3.	Εκτίμηση πιθανοτήτων ενδεχομένων.
$\Rightarrow$	Αν ένα αντικείμενο έχει θετική πιθανότητα, τότε υπάρχει.

Η διαδικασία αυτή, ενώ φαίνεται τετριμμένη, υποκρύπτει άφθονη δυσκολία και ευρηματικότητα. Η σχεδόν μεταφυσική φύση της Θεωρίας Πιθανοτήτων μοιάζει να διεμβολίζει δύσκολα προβλήματα με τη χρήση ενός ευρέος φάσματος από τεχνικές και έννοιες.

Μια από τις πιο συνηθισμένες τεχνικές, αξιοποιεί τη γραμμικότητα της Μέσης Τιμής [22]. Αν $X_1, \ldots, X_n$ τυχαίες μεταβλητές και $X = c_1X_1 + \cdots + c_nX_n$, τότε

$$\mathbb{E}[X] = c_1\,\mathbb{E}[X_1] + \cdots + c_n\,\mathbb{E}[X_n]$$

Η αιτία που καθιστά αυτή την ιδιότητα, ισχυρό εργαλείο, πηγάζει από το γεγονός ότι δεν υπάρχει καμιά προϋπόθεση ανεξαρτησίας ανάμεσα στις X_i. Το κλειδί σε αυτή την τεχνική, είναι να βρεθεί η κατάλληλη ανάλυση της X σε άθροισμα απλούστερων τυχαίων μεταβλητών. Η ανάλυση αυτή μας οδηγεί συνήθως στο συμπέρασμα ότι υπάρχει ένα σημείο του πιθανοθεωρητικού χώρου στο οποίο $X \geq \mathbb{E}[X]$ και ένα άλλο όπου $X \leq \mathbb{E}[X]$.

Χαρακτηριστικό είναι το παράδειγμά της επόμενης πρότασης, η οποία θεωρείται το πρώτο αποτέλεσμα με χρήση της Πιθανοθεωρητικής Μεθόδου. Ένα τουρνουά μπορούμε να το θεωρήσουμε ως έναν κατευθυνόμενο γράφο όπου ανάμεσα σε δύο κορυφές υπάρχει ακριβώς μία ακμή. Επίσης, μονοπάτι Hamilton ονομάζεται ένα μονοπάτι στο οποίο κάθε κορυφή εμφανίζεται ακριβώς μία φορά.

Πρόταση 1.3. *[23] Υπάρχει τουρνουά T με n παίκτες, το οποίο έχει τουλάχιστον $n!2^{-(n-1)}$ μονοπάτια Hamilton.*

Απόδειξη. Έστω ένα τουρνουά στο οποίο οι κατευθύνσεις των ακμών έχουν επιλεγεί τυχαία (ομοιόμορφα και ανεξάρτητα μεταξύ τους) και X το πλήθος των μονοπατιών Hamilton. Αναλύουμε την X σε δείκτριες τυχαίες μεταβλητές: για κάθε μετάθεση, σ, των κορυφών έστω $X_\sigma = 1$ όταν η σ δίνει ένα μονοπάτι Hamilton στο T, δηλαδή όταν $(\sigma(i), \sigma(i+1)) \in T, \forall i$. Τότε, $X = \sum X_\sigma$, όπου το πλήθος των όρων του αθροίσματος είναι $n!$, επομένως

$$\mathbb{E}[X] = \sum \mathbb{E}[X_\sigma] = n! \left(\frac{1}{2}\right)^{n-1}$$

Από αυτό είναι σαφές το συμπέρασμα ότι υπάρχει μη τυχαία επιλογή κατευθυνσιοδότησης του αρχικού μη κατευθυνόμενου γράφου, έτσι ώστε το τουρνουά που προκύπτει να έχει τουλάχιστον $\mathbb{E}[X]$ μονοπάτια Hamilton. □

Συχνά ως προέκταση της γραμμικότητας της μέσης τιμής εμφανίζεται η τεχνική των τροποποιήσεων (alterations) [24], κατά την οποία το πιθανοθεωρητικό μοντέλο που κατασκευάζεται, δεν δίνει άμεσα τη ζητούμενη απάντηση, αλλά μόνο μετά από κατάλληλη τροποποίηση του μαθηματικού αντικειμένου. Στην πράξη, συνήθως δημιουργείται ένα υπερσύνολο του αντικειμένου που μας ενδιαφέρει και στη συνέχεια αφαιρούνται στοιχεία που δεν ικανοποιούν την επιθυμητή ιδιότητα.

Ένα χαρακτηριστικό παράδειγμα σχετίζεται με τον αριθμό Ramsey, $R(k,l)$, που είναι ο ελάχιστος θετικός ακέραιος n, τέτοιος ώστε για κάθε 2-χρωματισμό (με μπλε, κόκκινο) των ακμών ενός πλήρους γράφου K_n, υπάρχει είτε ένας κόκκινος μονοχρωματικός πλήρης υπογράφος K_k είτε ένας αντίστοιχος μπλε K_l. Η πρόταση λέει ότι $R(k,k) > s = n - \binom{n}{k}2^{1-\binom{k}{2}}$, δηλαδή ένας πλήρης γράφος με λιγότερες από s κορυφές δεν περιέχει κανένα μονοχρωματικό υπογράφο k κορυφών.

Αυτό αποδεικνύεται θεωρώντας αρχικά έναν τυχαίο 2-χρωματισμό ενός πλήρους γράφου n κορυφών. Κατόπιν υπολογίζεται η μέση τιμή, $\mu = \binom{n}{k}2^{1-\binom{k}{2}}$, του πλήθους M των μονοχρωματικών υπογράφων k κορυφών και επιλέγεται ένας –μη τυχαίος– χρωματισμός τέτοιος ώστε $M < \mu$. Στη συνέχεια, εφαρμόζεται η τροποποίηση, αφαιρώντας μία κορυφή από κάθε μονοχρωματικό υποσύνολο, δημιουργώντας έτσι έναν

πλήρη γράφο με $n - \mu$ κορυφές και κανένα μονοχρωματικό υπογράφο k κορυφών· άρα $R(k, k) > s$.

Όπως με τη μέση τιμή, στην πιθανοθεωρητική μεθοδολογία χρησιμοποιείται και η διασπορά σε συνδυασμό με την ανισότητα Chebyshev, σύμφωνα με την οποία αν X είναι μια διακριτή τυχαία μεταβλητή με πεπερασμένη μέση τιμή, μ, και μη μηδενική διασπορά, σ^2, τότε,

$$\forall \lambda > 0, \mathbb{P}\left[|X - \mu| > \lambda\sigma\right] \leq \frac{1}{\lambda^2}$$

Στη διαδικασία που ακολουθείται σε αυτή την τεχνική, ορίζεται μια τυχαία μεταβλητή, X, για την ποσότητα που μας ενδιαφέρει. Στη συνέχεια αναλύεται ως άθροισμα απλούστερων –συνήθως δείκτριων– μεταβλητών,

$$X = X_1 + \cdots + X_n$$

υπολογίζεται η διασπορά της,

$$\mathrm{Var}\left[X\right] = \sum_{i=1}^{n} \mathrm{Var}\left[X_i\right] + \sum_{i \neq j} \mathrm{Cov}\left(X_i, X_j\right)$$

και με τη χρήση της ανισότητας Chebyshev καταλήγουμε σε συμπεράσματα.

Κλείνοντας την πολύ σύντομη περιήγηση στις τεχνικές της Πιθανοθεωρητικής Μεθόδου, αναφέρουμε το Lovász Τοπικό Λήμμα [25], το οποίο εφαρμόζεται στην περίπτωση όπου έχουμε ένα σύνολο από μη επιθυμητά ενδεχόμενα για τα οποία θα θέλαμε να εκτιμήσουμε την πιθανότητα να μη συμβαίνει κανένα. Αν αυτά είναι ανεξάρτητα μεταξύ τους, με την πιθανότητα του καθενός να είναι μικρότερη του 1, τότε η πιθανότητα να μη συμβαίνει κανένα είναι θετική (αν και ίσως μικρή). Το Τοπικό Λήμμα μας βοηθάει να καταλήξουμε στο ίδιο συμπέρασμα αρκεί τα ανεξάρτητα μεταξύ τους ενδεχόμενα να είναι πολύ περισσότερα από τα εξαρτημένα, και η πιθανότητα του καθενός να είναι σχετικά μικρή.

2 Κάτω Φράγματα για Συναρτήσεις Ισοτιμίας

Σε αυτό το κεφάλαιο, εξετάζουμε κατά πόσο οι συναρτήσεις ισοτιμίας μπορούν να εκφραστούν ως κυκλώματα σταθερού βάθους και μεγέθους πολυωνυμικού ως προς το πλήθος των μεταβλητών εισόδου.

Το ερώτημα αυτό απαντήθηκε από τους Merrick Furst, James Saxe, Michael Sipser το 1984 [26], και παράλληλα και ανεξάρτητα από τον Miklós Ajtai [27]. Και στις δύο εργασίες χρησιμοποιήθηκε η τεχνική του τυχαίου περιορισμού [28, 29], η οποία επινοήθηκε το 1961 από την Ρωσίδα Bella Abramovna Subbotovskaya [30, 31], εφαρμόζοντάς την σε φόρμουλες DNF[1].

Η απάντηση στο ερώτημα που τίθεται είναι αρνητική: οι συναρτήσεις ισοτιμίας δεν μπορούν να εκφραστούν από κυκλώματα σταθερού βάθους. Ξεκινώντας από την επόμενη πρόταση θα το αποδείξουμε αρχικά για την περίπτωση κυκλωμάτων βάθους 2. Η απόδειξη [32] δημοσιεύθηκε το 1961 από τον Oleg Borisovich Lupanov (1932 – 2006), του οποίου μαθήτρια ήταν η Subbotovskaya.

Πρόταση 2.1. *Έστω η συνάρτηση ισοτιμίας*

$$\pi_n : \{0,1\}^n \to \{0,1\}, \pi_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \mod 2$$

Η π_n δεν μπορεί να εκφραστεί από κύκλωμα OR-AND πολυωνυμικού μεγέθους και βάθους 2.

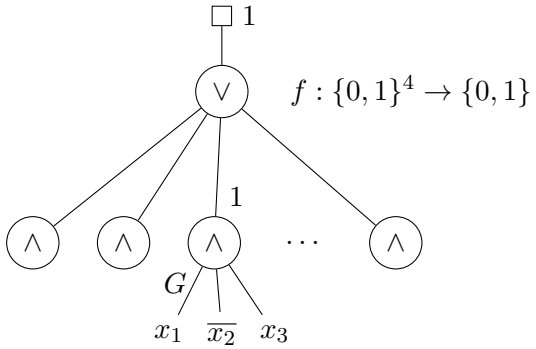
Απόδειξη.
Αρχικά, αποδεικνύουμε ότι κάθε πύλη AND στο επίπεδο 1 του κυκλώματος, αναγκαστικά έχει ακριβώς n εισόδους.

Αν δεν ισχύει αυτό, τότε υπάρχει μια πύλη AND στο πρώτο επίπεδο, ας την πούμε G, με πλήθος εισόδων είτε το πολύ $n-1$ είτε τουλάχιστον $n+1$. Για την πρώτη περίπτωση –βλ. Σχήμα 2.1–, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι στις εισόδους της δεν περιλαμβάνονται οι $x_n, \overline{x_n}$. Τότε, αν $y_1, \ldots, y_{n-1}$ είναι οι είσοδοι της G, με $y_i \in \{x_i, \overline{x_i}\}, i = 1 \ldots n-1$, τότε η τιμή της είναι 1, ακριβώς όταν $y_i = 1$ για κάθε $i \in \{1, \ldots, n-1\}$. Δηλαδή, τότε και μόνο τότε, όταν $x_i = 1$, ακριβώς για εκείνα τα i για τα οποία $y_i = x_i$. Για τα υπόλοιπα i θα έχουμε αναγκαστικά $x_i = 0$ και άρα $y_i = \overline{x_i} = 1$.

Σε αυτή την περίπτωση, για οποιαδήποτε τιμή ανατεθεί στη μεταβλητή x_n, το αποτέλεσμα της πύλης OR στο δεύτερο επίπεδο θα είναι πάντα 1. Οπότε, το συνολικό κύκλωμα δεν μπορεί να εκφράζει συνάρτηση ισοτιμίας n μεταβλητών. Άτοπο, άρα κάθε πύλη AND στο πρώτο επίπεδο του κυκλώματος έχει τουλάχιστον n εισόδους.

Επίσης, καμία πύλη δεν μπορεί να έχει περισσότερες από n εισόδους γιατί αλλιώς, αν υπήρχε κάποια, αναγκαστικά θα περιέχονταν στις εισόδους της κάποια

[1] DNF σημαίνει Disjunctive Normal Form, δηλαδή ένα λογικό γινόμενο αθροισμάτων.



$f(1, 0, 1, \cdot) \equiv 1 \Rightarrow f \not\equiv \pi_4$.

(α΄) Στο επίπεδο 1 δεν μπορεί να υπάρχει πύλη με πλήθος εισόδων μικρότερο του n.

x_1	x_2	x_3	x_4	π_4
0	0	0	0	0
0	0	1	0	1
⋮	⋮	⋮	⋮	⋮
1	**0**	**1**	**0**	**0**
⋮	⋮	⋮	⋮	⋮
1	**0**	**1**	**1**	**1**
⋮	⋮	⋮	⋮	⋮
1	1	1	1	0

(β΄) Ο πίνακας αλήθειας της π_n για $n = 4$, ο οποίος έχει 2^n γραμμές.

Σχήμα 2.1: Στο παράδειγμα του σχήματος, η πύλη *AND* με εισόδους $x_1, \overline{x_2}, x_3$ σταθεροποιείται στο 1 όταν $(x_1, x_2, x_3) = (1, 0, 1)$. Τότε για κάθε τιμή του x_4 όλο το κύκλωμα σταθεροποιείται στο 1· άρα δεν μπορεί να εκφράζει συνάρτηση ισοτιμίας. Επίσης, κάθε πύλη *AND* αντιστοιχεί σε ακριβώς μία γραμμή του πίνακα αλήθειας της π_4 με τιμή εξόδου 1. Άρα το πλήθος των πυλών στο επίπεδο 1 είναι 2^{n-1}.

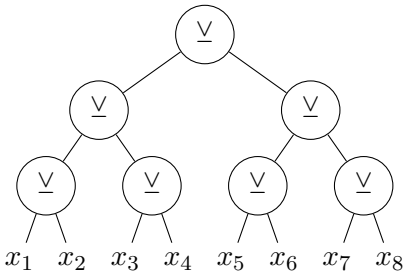
μεταβλητή μαζί με την άρνησή της και τότε η πύλη θα είχε σταθερή τιμή 0 και δεν θα έπαιζε κανένα ρόλο στο κύκλωμα.

Για να μπορεί το κύκλωμα να εκφράζει τη συνάρτηση ισοτιμίας π_n, θα πρέπει η τιμή της εξόδου του να είναι 1 ακριβώς στις περιπτώσεις που ο πίνακας αλήθειας της π_n δίνει τιμή 1. Αυτό συμβαίνει όταν μία από τις πύλες του πρώτου επιπέδου έχει τιμή 1. Αφού λοιπόν κάθε πύλη AND έχει ακριβώς n εισόδους, $y_1, \ldots, y_n$ με $y_i \in \{x_i, \overline{x_i}\}$, παίρνει τιμή 1 ακριβώς σε ένα συνδυασμό τιμών των $x_1, \ldots, x_n$. Ο συνδυασμός είναι αυτός για τον οποίο, $y_1 = \cdots = y_n = 1$. Αυτό σημαίνει ότι η κάθε πύλη αντιστοιχεί ακριβώς σε μία γραμμή του πίνακα αλήθειας της συνάρτησης ισοτιμίας με τιμή 1. Το πλήθος των γραμμών αυτών είναι $2^n/2 = 2^{n-1}$ και άρα, πρέπει να υπάρχουν ακριβώς 2^{n-1} πύλες AND.

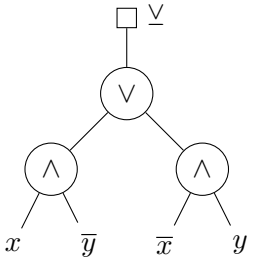
Άρα το μέγεθος του κυκλώματος δεν μπορεί να είναι πολυωνυμικό ως προς n.
□ (Πρόταση 2.1)

Με ανάλογο τρόπο παίρνουμε το ίδιο αποτέλεσμα για αντίστοιχα λογικά κυκλώματα *AND-OR*· δηλαδή με πύλες *OR* στο πρώτο επίπεδο και μία *AND* στο δεύτερο.

Όπως αναφέρθηκε παραπάνω, στην παράγραφο αυτή θα δείξουμε ότι λογικά



(α′) Συνάρτηση ισοτιμίας π_8 εκφρασμένη ως κύκλωμα πυλών *XOR*.



(β′) Η πύλη *XOR* συναρτήσει πυλών *AND* και *OR*.

Σχήμα 2.2: Η συνάρτηση ισοτιμίας π_n μπορεί να εκφραστεί από κύκλωμα βάθους $\mathcal{O}(\log n)$.

κυκλώματα σταθερού βάθους δεν μπορούν να υπολογίσουν συναρτήσεις ισοτιμίας. Όμως, αξίζει να σημειώσουμε, ποια λογικά κυκλώματα μπορούν να τις εκφράσουν. Η επόμενη πρόταση μας δείχνει ότι το κάτω φράγμα που αναζητούμε είναι το πολύ λογαριθμικό.

Πρόταση 2.2.
Μια συνάρτηση ισοτιμίας n μεταβλητών, μπορεί να υπολογιστεί από κύκλωμα βάθους $\mathcal{O}(\log n)$.

Απόδειξη.

Μία συνάρτηση ισοτιμίας μπορεί να εκφραστεί από ένα δυαδικό δένδρο με πύλες XOR, όπου στο επίπεδο 1, κάθε πύλη έχει δύο εισόδους και κάθε μεταβλητή εμφανίζεται σε ακριβώς μία πύλη –βλ. Σχήμα 2.2. Το βάθος του δέντρου είναι $\mathcal{O}(\log n)$.

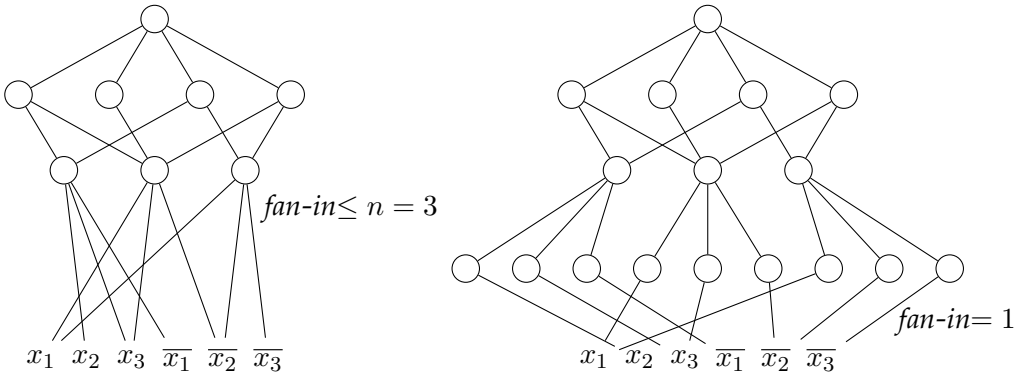
Επίσης, κάθε πύλη XOR μπορεί να εκφραστεί ως ένα *OR-AND* κύκλωμα δύο επιπέδων, αφού $XOR(x_1, x_2) = x_1\overline{x_2} + \overline{x_1}x_2 = OR(AND(x_1, \overline{x_2}), AND(\overline{x_1}, x_2))$. Οπότε το βάθος του δέντρου διπλασιάζεται. Επομένως, μια συνάρτηση ισοτιμίας n μεταβλητών μπορεί να υπολογιστεί από ένα κύκλωμα βάθους $\mathcal{O}(\log n)$.

□ (Πρόταση 2.2)

Για τη συνέχεια, υπενθυμίζουμε ότι AC^k είναι το σύνολο των συναρτήσεων που μπορούν να εκφραστούν ως κυκλώματα χωρίς άνω φράγμα εισόδου με μέγεθος πολυωνυμικό ως προς το πλήθος n των εισόδων και βάθος $\mathcal{O}(\log^k n)$, όπου k μη αρνητικός ακέραιος. Από την πρόταση 2.2 προκύπτει άμεσα ότι $\pi_n \in AC^1$ για κάθε $n \in \mathbb{N}$.

Το επόμενο θεώρημα, που θα καλύψει το υπόλοιπο κεφάλαιο, αποδεικνύει ότι $\pi_n \notin AC^0$. Αρχικά ορίζουμε την έννοια του τυχαίου περιορισμού.

Ορισμός 2.3 (Τυχαίος Περιορισμός). *Ως τυχαίο περιορισμό μιας λογικής συνάρτησης f, θεωρούμε μια άλλη λογική συνάρτηση g, η οποία προκύπτει όταν σταθε-*



Η καταχρηστική προσθήκη ενός επιπλέον επιπέδου λογικών πυλών μίας εισόδου, καθιστά το φράγμα εισόδου στο πρώτο επίπεδο του κυκλώματος σταθερό, 1. Αυτό δεν μεταβάλλει την τάξη μεγέθους των δομικών στοιχείων του κυκλώματος. Αν το αρχικό κύκλωμα έχει πολυωνυμικό μέγεθος και σταθερό βάθος, το ίδιο ισχύει και για το νέο λογικό κύκλωμα. Επομένως, η αδυναμία τέτοιων κυκλωμάτων να εκφράσουν συναρτήσεις ισοτιμίας (Θεώρημα 2.4), είναι αρκετό να αποδειχθεί για σταθερό φράγμα εισόδου στο πρώτο επίπεδο.

Σχήμα 2.3: $\pi_n \notin AC^0, \forall n \in \mathbb{N}$ (Θεώρημα 2.4). Αρκεί να αποδειχθεί για κυκλώματα σταθερού φράγματος εισόδου στο πρώτο επίπεδο.

ροποιήσουμε τυχαία κάποιες από τις μεταβλητές εισόδου σε συγκεκριμένες τιμές, 0 *ή* 1.

Θεώρημα 2.4 (Furst, Saxe, Sipser [26]).
Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, *συνάρτηση ισοτιμίας.*
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Απόδειξη.

Αρχικά παρατηρούμε ότι αρκεί να δείξουμε το θεώρημα για την περίπτωση όπου οι πύλες του πρώτου επιπέδου έχουν φράγμα εισόδου σταθερό, ανεξάρτητο του n. Αν ισχύει αυτό, τότε το θεώρημα, στη γενική περίπτωση, προκύπτει άμεσα: έστω $\pi_n \in A^0$. Τότε, υπάρχει πολυωνυμικού μεγέθους κύκλωμα, σταθερού βάθους t, που υπολογίζει κάποια συνάρτηση ισοτιμίας. Καταχρηστικά, μπορούμε να προσθέσουμε, κάτω από το πρώτο επίπεδο, άλλο ένα επίπεδο τοποθετώντας μία πύλη μίας εισόδου για κάθε μεταβλητή εισόδου κάθε πύλης του πρώτου επιπέδου –βλ. παράδειγμα στο Σχήμα 2.3.

Οι πύλες του πρώτου επιπέδου, οι οποίες έχουν απεριόριστο άνω φράγμα εισόδου, μπορούν να έχουν το πολύ n εισόδους, διαφορετικά στις εισόδους τους θα περιλαμβάνονται συμπληρωματικές μεταβλητές και οι πύλες θα εκφυλίζονται. Επομένως, με την εισαγωγή του νέου επιπέδου, προστίθενται το πολύ n πύλες για κάθε πύλη του πρώτου επιπέδου.

Αν λοιπόν, $p(n)$ είναι το πολυώνυμο που φράσσει το μέγεθος του αρχικού κυκλώματος, το μέγεθος του νέου κυκλώματος είναι το πολύ $\mathcal{O}(np(n))$. Επομένως, έχουμε ένα νέο κύκλωμα το οποίο μπορεί να εκφράσει συνάρτηση ισοτιμίας, έχει πολυωνυμικό μέγεθος, βάθος $t+1$, και φράγμα εισόδου στο πρώτο επίπεδο, σταθερό 1. Άτοπο· άρα $\pi_n \notin AC^0$ για κάθε n.

Αρκεί, λοιπόν, να δείξουμε τον ακόλουθο ισχυρισμό.

Ισχυρισμός 1. *Για οποιαδήποτε $t, c \in \mathbb{N}$ και για οποιοδήποτε πολυώνυμο p, καμία συνάρτηση ισοτιμίας n μεταβλητών δεν μπορεί να υπολογιστεί από κύκλωμα με φράγμα εισόδου c, βάθος t και μέγεθος $p(n)$.*

***Απόδειξη** (Ισχυρισμού 1).*
Η απόδειξη του ισχυρισμού είναι επαγωγική ως προς το βάθος του κυκλώματος. Η βάση της επαγωγής, για $t = 2$, έχει ήδη αποδειχθεί στην Πρόταση 2.1: κυκλώματα βάθους 2 με πολυωνυμικό μέγεθος δεν μπορούν να εκφράσουν συναρτήσεις ισοτιμίας.

Έστω τώρα, ότι για κυκλώματα βάθους μεγαλύτερο από 2, ο ισχυρισμός δεν ισχύει. Δηλαδή, υποθέτουμε ότι υπάρχει κάποιο $t > 2$, για το οποίο η συνάρτηση ισοτιμίας μπορεί να υπολογιστεί από κύκλωμα πολυωνυμικού μεγέθους, βάθους t και σταθερού φράγματος εισόδου.

Μπορούμε επίσης να υποθέσουμε ότι το t είναι ο ελάχιστος αριθμός με αυτή την ιδιότητα. Θα δείξουμε ότι υπάρχει πολυωνυμικού μεγέθους κύκλωμα, βάθους $t-1$, με σταθερό φράγμα εισόδου το οποίο υπολογίζει συνάρτηση ισοτιμίας. Από αυτό θα προκύψει αντίφαση προς την υπόθεση ότι το t είναι το ελάχιστο με αυτό την ιδιότητα.

Έστω $k \in \mathbb{N}, k > \deg p(n)$, όπου $p(n)$ είναι το πολυώνυμο που φράσσει το μέγεθος του κυκλώματος, και c μια σταθερά που φράσσει το πλήθος των εισόδων που επιδέχεται κάθε πύλη στο επίπεδο 1.

Θεωρούμε την ακολουθία $\{S_n\}_{n\in\mathbb{N}}$, κυκλωμάτων βάθους t τα οποία εκφράζουν συναρτήσεις ισοτιμίας n μεταβλητών. Η ιδέα είναι να τροποποιηθούν τα στοιχεία αυτής της ακολουθίας έτσι ώστε να προκύψει μια νέα ακολουθία κυκλωμάτων, $\{S'_n\}_{n\in\mathbb{N}}$, η οποία για μεγάλα n να αναδεικνύει την ύπαρξη κυκλώματος βάθους $t-1$ και πολυωνυμικού μεγέθους, το οποίο να υπολογίζει συνάρτηση ισοτιμίας.

Ο τρόπος που κατασκευάζονται τα κυκλώματα S'_n είναι ο εξής: από κάθε στοιχείο της πρώτης ακολουθίας με πλήθος μεταβλητών μεγαλύτερο από n, έστω $4n^2$, σταθεροποιούμε κατάλληλα επιλεγμένες μεταβλητές πλήθους $4n^2 - n$, σε τιμές 0 ή 1. Έτσι το νέο κύκλωμα που προκύπτει, εκφράζει μια λογική συνάρτηση n μεταβλητών, η οποία μάλιστα, είναι συνάρτηση ισοτιμίας, ή το συμπλήρωμά της.

Αυτό ισχύει γιατί αν $\pi_n(x_1, \ldots, x_n)$ είναι συνάρτηση ισοτιμίας, τότε αν σταθεροποιηθεί η πρώτη μεταβλητή, έχουμε

$$\pi_n(0, x_2, \ldots, x_n) = \pi_{n-1}(x_2, \ldots, x_n)$$
$$\pi_n(1, x_2, \ldots, x_n) = \overline{\pi_{n-1}}(x_2, \ldots, x_n)$$

Αντίστοιχα, το ίδιο συμβαίνει αν σταθεροποιηθεί οποιαδήποτε άλλη μεταβλητή. Γενικότερα, αν σταθεροποιηθούν m μεταβλητές και άρτιο πλήθος από αυτές πάρουν την τιμή 1, τότε η νέα συνάρτηση είναι συνάρτηση ισοτιμίας $n-m$ μεταβλητών. Αλλιώς είναι το συμπλήρωμά της.

Στην περίπτωση που το κύκλωμα S'_n εκφράζει συμπλήρωμα συνάρτησης ισοτιμίας, θα πρέπει να εξεταστεί αν μπορεί να προκύψει κύκλωμα με ανάλογα δομικά χαρακτηριστικά το οποίο να υπολογίζει συνάρτηση ισοτιμίας. Αυτό γίνεται φανερό από την ακόλουθη παρατήρηση

Παρατήρηση 1: Το κύκλωμα που υπολογίζει την $\overline{\pi_n}$ έχει ακριβώς τις ίδιες δομικές ιδιότητες με αυτό που υπολογίζει την π_n· δηλαδή το ίδιο μέγεθος, βάθος και φράγμα εισόδου. Αυτό συμβαίνει γιατί

$$\overline{\pi_n}\left(x_1,\ldots,x_n\right)=\left(1+\sum_{i=1}^{n}x_i\right)=\left(1+x_k+\sum_{\substack{i=1\\i\neq k}}^{n}x_i\right)=$$

$$\left(\overline{x_k}+\sum_{\substack{i=1\\i\neq k}}^{n}x_i\right)=\pi_n\left(x_1,\ldots,\overline{x_k},\ldots,x_n\right)$$

όπου τις παραπάνω εκφράσεις τις λογικές μεταβλητές τις έχουμε θεωρήσει ως στοιχεία του σώματος $(\mathbb{F}_2,+,\cdot)$.

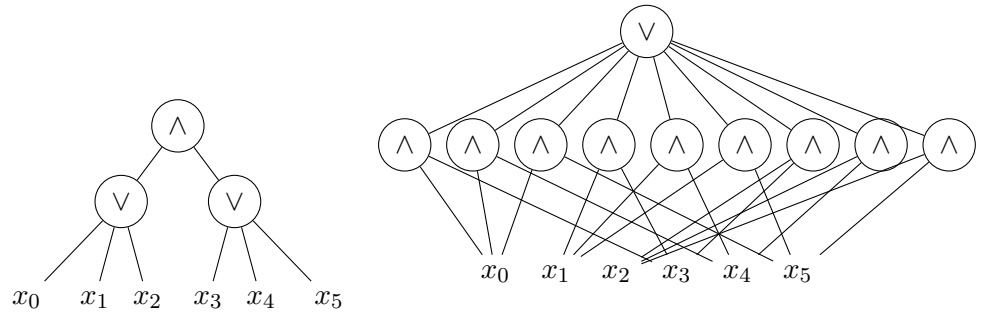
Από τις σχέσεις αυτές συμπεραίνουμε ότι ένα κύκλωμα που εκφράζει μια συνάρτηση ισοτιμίας, υπολογίζει το συμπλήρωμά της αν απλώς αντιστρέψουμε μία λογική μεταβλητή, κάτι που δεν μεταβάλει τη δομή και τα μεγέθη του κυκλώματος.

□ (Παρατήρηση 1)

Μπορούμε λοιπόν να θεωρήσουμε ότι σταθεροποιώντας κατάλληλες μεταβλητές ενός κυκλώματος S_{4n^2}, παίρνουμε ένα κύκλωμα S'_n το οποίο υπολογίζει μια συνάρτηση ισοτιμίας n μεταβλητών.

Το βασικό ερώτημα εδώ είναι με ποιον τρόπο επιλέγουμε τη σταθεροποίηση των μεταβλητών στα κυκλώματα της πρώτης ακολουθίας. Έχοντας ως στόχο να δείξουμε την *ύπαρξη* κυκλώματος S'_n που να μας οδηγήσει σε άτοπο, η ιδέα είναι να εφαρμόσουμε την πιθανοθεωρητική μέθοδο, στον τρόπο κατασκευής των περιορισμένων κυκλωμάτων και να δείξουμε ότι για μεγάλα n, με θετική πιθανότητα υπάρχει S'_n πολυωνυμικού μεγέθους και βάθους $t-1$, το οποίο να υπολογίζει συνάρτηση ισοτιμίας. Το βάθος $t-1$ θα προκύψει αντιστρέφοντας, μέσω των κανόνων de Morgan, τα επίπεδα 1 και 2, έτσι ώστε τα επίπεδα 2 και 3 να έχουν τον ίδιο τύπο πυλών και να μπορούν να συγχωνευθούν, μειώνοντας έτσι το βάθος του κυκλώματος κατά ένα.

Ουσιαστικά, η ιδέα είναι να εφαρμοστεί η Πιθανοθεωρητική Μέθοδος των Τροποποιήσεων (alterations) [24] που αναφέραμε στην Εισαγωγή (Παρ. 1.2). Τροποποιούμε τυχαία ένα αντικείμενο μεγαλύτερης κλίμακας, έτσι ώστε με θετική πιθανότητα να υπάρχει αντικείμενο μικρότερης κλίμακας που να έχει την ιδιότητα που στοχεύουμε, δηλαδή να υπολογίζει συνάρτηση ισοτιμίας.



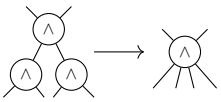
$(x_0 + x_1 + x_2) \cdot (x_3 + x_4 + x_5)$

$x_0x_3 + x_0x_4 + x_0x_5 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5$

Στο παράδειγμα του σχήματος στο αριστερό κύκλωμα το φράγμα εισόδου στο πρώτο επίπεδο είναι $c = 3$ και στο δεύτερο $d = 2$. Εναλλάσσοντας τα δύο επίπεδα με την εφαρμογή των κανόνων «De Morgan» το πλήθος των πυλών γίνεται c^d. Αυτό σημαίνει ότι αν το φράγμα εισόδου στο δεύτερο επίπεδο εξαρτάται από το n, το συνολικό μέγεθος του κυκλώματος μπορεί να αυξηθεί εκθετικά.

Σχήμα 2.4: Η αντιμετάθεση δύο διαδοχικών επιπέδων μπορεί να οδηγήσει σε εκθετική αύξηση του μεγέθους του λογικού κυκλώματος –βλ. Παρατήρηση 2.

Να σημειώσουμε εδώ το προφανές, ότι η συγχώνευση δύο διαδοχικών επιπέδων με ίδιου τύπου πύλες, δεν αυξάνει το μέγεθος του κυκλώματος, αλλά το μειώνει· π.χ.:



Όμως, το πρόβλημα που προκύπτει είναι ότι αυτή η αντιστροφή ενδέχεται να οδηγήσει σε εκθετική αύξηση του μεγέθους του κυκλώματος, όπως φαίνεται από την ακόλουθη παρατήρηση.

Παρατήρηση 2: Η αντιστροφή δύο επιπέδων ενδέχεται να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

Έστω ένα *AND-OR* κύκλωμα δύο επιπέδων –βλ. Σχήμα 2.4– όπου όλες οι πύλες *OR* του πρώτου επιπέδου έχουν άνω φράγμα εισόδου c και η πύλη *AND* του δεύτερου επιπέδου έχει άνω φράγμα εισόδου d. Αν τροποποιήσουμε το κύκλωμα με τη χρήση των κανόνων «De Morgan», έτσι ώστε το πρώτο επίπεδο να αποτελείται από πύλες *AND* και το δεύτερο από μία πύλη *OR*, τότε το νέο κύκλωμα, στη γενική περίπτωση, μπορεί να έχει c^d πύλες *AND*.

Κατά συνέπεια, το μέγεθός του γίνεται εκθετικό αν το d εξαρτάται τουλάχιστον γραμμικά από το n. Αυτό ισχύει, γιατί αν συμβολίσουμε με άθροισμα τη λογική διάζευξη και με πολλαπλασιασμό τη λογική σύζευξη τότε το αρχικό κύκλωμα εκφράζει μια λογική συνάρτηση στη μορφή ενός γινομένου d παραγόντων, όπου κάθε

παράγοντας είναι άθροισμα c όρων,

$$\overbrace{\left(\sum\dots\right)\times\underbrace{\left(\sum\dots\right)}_{c\text{ όροι}}\times\dots\times\left(\sum\dots\right)}^{d\text{ παράγοντες}}$$

Η μετατροπή, με τους κανόνες «de Morgan», αυτής της έκφρασης σε άθροισμα γινομένων παράγει ένα νέο άθροισμα c^d όρων και κάθε όρος αντιστοιχεί σε μία πύλη AND, d εισόδων.

□ (Παρατήρηση 2)

Έχοντας, λοιπόν, κατά νου την παραπάνω παρατήρηση, ο τρόπος εφαρμογής του τυχαίου περιορισμού πρέπει να είναι τέτοιος ώστε να αποφευχθεί μια ενδεχόμενη εκθετική αύξηση στο μέγεθος του κυκλώματος. Για να γίνει αυτό, αρκεί η κατασκευή του S'_n να είναι τέτοια ώστε το πλήθος εισόδων των πυλών στο δεύτερο επίπεδο να μην εξαρτάται από το πλήθος των μεταβλητών εισόδου.

Ένα άλλο βασικό ζητούμενο είναι, με την εφαρμογή του περιορισμού στο αρχικό κύκλωμα, να μη μειωθούν τόσο πολύ οι μεταβλητές εισόδου ώστε το συνολικό πλήθος των πυλών να γίνει εκθετικό. Για να εξασφαλιστεί αυτό θα πρέπει το πλήθος των μεταβλητών που δεν σταθεροποιούνται να είναι το πολύ πολυωνυμικά μικρότερο σε σχέση με το αρχικό. Έτσι διατηρείται η πολυωνυμική τάξη μεγέθους του πλήθους πυλών του κυκλώματος ως προς τις μεταβλητές εισόδου.

Με βάση τα παραπάνω, για κάθε μεταβλητή x_i, ανεξάρτητα από τις υπόλοιπες, ορίζουμε τον τυχαίο περιορισμό με το παρακάτω τυχαίο πείραμα:

- Με πιθανότητα $\frac{1}{\sqrt{n}}$ η x_i παραμένει μεταβλητή.
- Με πιθανότητα $\frac{1-1/\sqrt{n}}{2}$ η x_i σταθεροποιείται στο 0.
- Με πιθανότητα $\frac{1-1/\sqrt{n}}{2}$ η x_i σταθεροποιείται στο 1.

Θα δούμε παρακάτω, στην Πρόταση 2.5 ότι η πιθανότητα $1/\sqrt{n}$ μας εξασφαλίζει τελικά (δηλ. για μεγάλα n) την επιθυμητή μείωση των μη σταθεροποιημένων μεταβλητών. Επίσης, ορίζοντας ισοπίθανα τα ενδεχόμενα σταθεροποίησης μιας μεταβλητής σε 0 και 1, μπορούμε να έχουμε συμμετρία στον χειρισμό των πυλών AND και OR.

Ας συμβολίσουμε με r ένα τυχαίο περιορισμό και με x_i^r το αποτέλεσμα της δράσης του στη μεταβλητή x_i, οπότε $x_i^r \in \{0, 1, x_i\}$. Έστω επίσης, S^r το κύκλωμα που προκύπτει από την εφαρμογή του περιορισμού στο κύκλωμα S. Αν X[2] είναι η

[2]Ουσιαστικά η X ακολουθεί τη διωνυμική κατανομή με πιθανότητα επιτυχίας $p = 1/\sqrt{n}$.

τυχαία μεταβλητή που εκφράζει το πλήθος των μεταβλητών στο κύκλωμα S^r, τότε

$$\mathbb{E}[X] = n \cdot \frac{1}{\sqrt{n}} = \sqrt{n}$$
$$\mathrm{Var}[X] = n \cdot \frac{1}{\sqrt{n}} \cdot \left(1 - \frac{1}{\sqrt{n}}\right) = \sqrt{n} - 1$$

Πριν προχωρήσουμε, θα πρέπει να βεβαιωθούμε επίσης ότι η νέα ακολουθία, των περιορισμένων κυκλωμάτων, είναι πλήρης, χωρίς κενά· δηλαδή ορίζεται για κάθε $n \in \mathbb{N}$. Ακριβέστερα, θέλουμε με την εφαρμογή της παραπάνω τυχαίας διαδικασίας, για κάθε $n \in \mathbb{N}$ να υπάρχει περιορισμένο κύκλωμα S'_n· να μπορούμε δηλαδή να γεμίσουμε τα τυχόν κενά της τυχαία παραγόμενης ακολουθίας περιορισμένων κυκλωμάτων –υπενθυμίζουμε ότι θέλουμε να δείξουμε ότι $\pi_n \notin AC^0$, **για κάθε** $n \in \mathbb{N}$.

Έστω, λοιπόν, το κύκλωμα S_{4n^2} για κάποιο σταθεροποιημένο n. Με θετική πιθανότητα, το $S^r_{4n^2}$ έχει τουλάχιστον n (μη σταθεροποιημένες) μεταβλητές εισόδου. Άρα, υπάρχει περιορισμένο κύκλωμα με m μεταβλητές εισόδου, όπου $n \leq m \leq 4n^2$. Το μέγεθος του κυκλώματος S_{4n^2} έχουμε υποθέσει ότι είναι πολυωνυμικό ως προς το πλήθος των μεταβλητών εισόδου, δηλαδή είναι $\mathcal{O}\left(\left(4n^2\right)^k\right) = \mathcal{O}\left(n^{2k}\right)$. Αυτό εξακολουθεί να ισχύει στο περιορισμένο κύκλωμα, αφού το m είναι το πολύ πολυωνυμικά μικρότερο του $4n^2$. Αν, τώρα, κάθε μία από τις έξτρα $m - n$ μεταβλητές, τις σταθεροποιήσουμε ~~στην τιμή 0~~, τότε έχουμε ένα περιορισμένο κύκλωμα με τα επιθυμητά χαρακτηριστικά: n εισόδους και πολυωνυμικό μέγεθος· οπότε και η παραγόμενη ακολουθία είναι πλήρης, χωρίς κενά.

Όπως αναφέρθηκε παραπάνω, η μείωση του πλήθους των μεταβλητών πρέπει να είναι το πολύ πολυωνυμική. Με τις επιλεγμένες πιθανότητες, όπως φαίνεται στην ακόλουθη πρόταση, αυτό ισχύει.

Πρόταση 2.5.
Μετά την εφαρμογή του περιορισμού στο κύκλωμα S_n, με μεγάλη πιθανότητα το πλήθος, X, των μεταβλητών εισόδου στο περιορισμένο κύκλωμα, S^r_n, είναι τουλάχιστον $\sqrt{n}/2$,

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

Απόδειξη *(Πρότασης 2.5).*
Από την ανισότητα Chebyshev έχουμε

$$\mathbb{P}\left[\left|X - \mathbb{E}[X]\right| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{\mathrm{Var}[X]}{\left(\sqrt{n}/2\right)^2} \leq \frac{4}{\sqrt{n}}$$

Επίσης

$$\mathbb{P}\left[\left|X - \mathbb{E}[X]\right| \leq \frac{\sqrt{n}}{2}\right] = \mathbb{P}\left[X \geq \frac{3\sqrt{n}}{2} \text{ ή } X \leq \frac{\sqrt{n}}{2}\right]$$

Επομένως,

$$\mathbb{P}\left[X \leq \frac{\sqrt{n}}{2}\right] \leq \mathbb{P}\left[\left|X - \mathbb{E}[X]\right| \leq \frac{\sqrt{n}}{2}\right] \leq \frac{4}{\sqrt{n}} = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

□ (Πρόταση 2.5)

Με την πρόταση αυτή, ουσιαστικά έχουμε στήσει το βασικό πλαίσιο της απόδειξης. Υπενθυμίζουμε ότι, με στόχο να καταλήξουμε σε άτοπο, έχουμε υποθέσει ότι $t > 2$ είναι το ελάχιστο σταθερό βάθος που απαιτείται για ένα πολυωνυμικού μεγέθους κύκλωμα για να εκφράσει συνάρτηση ισοτιμίας. Με βάση αυτό, θέλουμε να δείξουμε ότι υπάρχει τέτοιο κύκλωμα βάθους $t-1$, το οποίο θα μας δώσει το επιθυμητό άτοπο.

Όπως αναφέρθηκε παραπάνω –Παρατήρηση 2, Σχήμα 2.4–, η εξάρτηση του πλήθους εισόδων στο επίπεδο 2 από το πλήθος των μεταβλητών εισόδων παίζει καθοριστικό ρόλο στο αποτέλεσμα που επιδιώκουμε, καθώς η αντιμετάθεση δύο διαδοχικών επιπέδων μπορεί να αυξήσει εκθετικά το μέγεθος του κυκλώματος.

Το ζήτημα αυτό το προσεγγίζουμε σταθεροποιώντας ένα υποκύκλωμα δύο επιπέδων με ρίζα μια πύλη *AND*. Χωρίς βλάβη της γενικότητας και λόγω του ισοπίθανου των ενδεχομένων σταθεροποίησης των μεταβλητών εισόδου σε 1 ή 0, μπορούμε να υποθέσουμε ότι το επίπεδο 1 αποτελείται από πύλες *OR* και, επομένως, το επίπεδο 2 από πύλες *AND*. Σε διαφορετική περίπτωση, λόγω συμμετρίας των πιθανοτήτων, ισχύει το ίδιο επιχείρημα αλληλοαντικαθιστώντας πύλες AND με πύλες OR, μηδενικά με άσσους, και μεταβλητές x_i με $\overline{x_i}$.

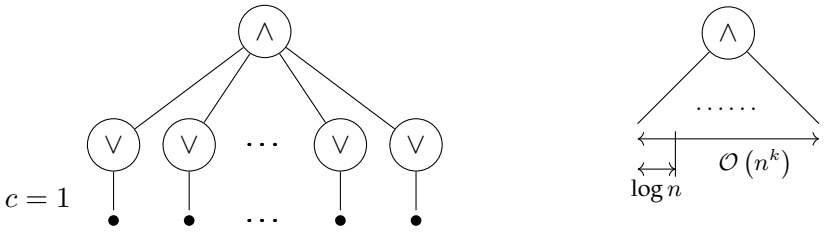
Θα δείξουμε, λοιπόν, ότι ο τυχαίος περιορισμός παράγει μια μη επιθυμητή ιδιότητα –στην περίπτωσή μας «εξάρτηση από πολλές μεταβλητές»– στην πύλη *AND* με πιθανότητα το πολύ $\mathcal{O}\left(\frac{1}{n^k}\right)$. Αφού όλες οι πύλες του κυκλώματος είναι της τάξεως $\mathcal{O}\left(n^{k-1}\right)$, συμπεραίνουμε ότι η πιθανότητα να συμβεί η μη επιθυμητή ιδιότητα σε *κάποια* πύλη *AND* του επιπέδου 2, είναι το πολύ $\mathcal{O}\left(\frac{1}{n^k} \cdot n^{k-1}\right) = \mathcal{O}\left(\frac{1}{n}\right)$ (υπενθυμίζουμε ότι k είναι ακέραιος αυστηρά μεγαλύτερος από τον βαθμό του πολυωνύμου που φράσσει το μέγεθος του κυκλώματος). Δηλαδή, με μεγάλη πιθανότητα, μετά την εφαρμογή του τυχαίου περιορισμού, καμία πύλη *AND* στο επίπεδο 2 δεν έχει την ανεπιθύμητη ιδιότητα.

Αποδεικνύουμε, λοιπόν, τον ακόλουθο ισχυρισμό:

Ισχυρισμός 2. *Για κάθε AND-OR κύκλωμα δύο επιπέδων με φράγμα εισόδου (fan-in) το πολύ c, υπάρχει σταθερά $e = e_c$ –εξαρτώμενη από το c–, τέτοια ώστε η πιθανότητα η τιμή της πύλης AND, μετά την εφαρμογή του περιορισμού, να εξαρτάται από περισσότερες από e_c μεταβλητές, είναι το πολύ $\mathcal{O}\left(1/n^k\right)$.*

***Απόδειξη** (Ισχυρισμού 2).*
Σε αυτή την πρόταση, έχουμε ένα απλό κύκλωμα δύο επιπέδων με φράγμα εισόδου, c, στο πρώτο επίπεδο. Αυτή η παράμετρος, που είναι ένας θετικός ακέραιος, καθορίζει και κλιμακώνει το πρόβλημα. Επομένως είναι λογικό η απόδειξη του ισχυρισμού να κινείται στο πλαίσιο της μαθηματικής επαγωγής ως προς c.

Για $c = 1$, οι πύλες *OR* του πρώτου επιπέδου εκφυλίζονται, οπότε το κύκλωμα αποτελείται από μία πύλη *AND*. Με σκοπό να εκμεταλλευτούμε διαφορετικές πιθανοθεωρητικές ιδιότητες σε διαφορετικές τάξεις μεγέθους του προβλήματος, η ιδέα



(α΄) **(β΄)**

Όταν το φράγμα εισόδου στο πρώτο επίπεδο του *AND-OR* κυκλώματος είναι $c = 1$ (σχήμα αριστερά), τότε οι πύλες *OR* εκφυλίζονται οπότε έχουμε ένα κύκλωμα μίας πύλης. Το πρόβλημα χωρίζεται φυσιολογικά σε δύο περιπτώσεις (σχήμα δεξιά): μικρής ($\leq \log n$) και μεγάλης ($\geq \log n$) κλίμακας ~~φράγμα εισόδου~~ πλήθους μεταβλητών εισόδου. Με τον τυχαίο περιορισμό, στην πρώτη περίπτωση είναι πολύ πιθανό να σταθεροποιηθούν όλες –πλην σταθερού πλήθους– είσοδοι, ενώ στη δεύτερη είναι πολύ πιθανό να υπάρχει μία είσοδος που σταθεροποιείται στο 0. Σε κάθε περίπτωση είναι πολύ πιθανό η πύλη *AND* να εξαρτάται σταθερό, το πολύ, πλήθος μεταβλητών εισόδου.

Σχήμα 2.5: Η βάση της επαγωγής για την απόδειξη ότι (βλ. Ισχυρισμός 2) σε ένα κύκλωμα *AND-OR*, με μεγάλη πιθανότητα η πύλη *AND* εξαρτάται από, το πολύ, σταθερό πλήθος μεταβλητών εισόδου.

είναι να διαχωρίσουμε δύο περιπτώσεις: μικρό και μεγάλο φράγμα εισόδου.

Να σημειώσουμε εδώ ότι η έννοια μικρό και μεγάλο φράγμα εισόδου έχει να κάνει με την τάξη μεγέθους ως προς n. Έτσι, εφόσον έχουμε το πολύ πολυωνυμικό μέγεθος το μικρό φράγμα εισόδου φυσιολογικά προσδιορίζεται ως λογαριθμικό μέγεθος. Όπως θα φανεί στη συνέχεια, το σημείο αυτό μοιάζει σαν να είναι σημείο καμπής στην κλίμακα του προβλήματος και εξετάζοντάς το εποπτικά, θα δούμε ότι ο συγκεκριμένος διαχωρισμός είναι μάλλον δομικά αναπόφευκτος.

Στην πρώτη, λοιπόν περίπτωση, υποθέτουμε ότι το φράγμα εισόδου της πύλης *AND* είναι τουλάχιστον $4k \log_2 n$. Τότε, μπορούμε πρόχειρα να εκτιμήσουμε ότι είναι πολύ πιθανό να υπάρχει μία είσοδος, η οποία με τον τυχαίο περιορισμό, σταθεροποιείται στην τιμή 0· οπότε, η πύλη *AND* είναι ανεξάρτητη από οποιαδήποτε μεταβλητή. Συγκεκριμένα, η πιθανότητα η πύλη *AND* να μη σταθεροποιείται στο 0 είναι $\mathcal{O}\left(1/n^k\right)$.

Αυτό ισχύει γιατί η πιθανότητα αυτή φράσσεται άνω, από την πιθανότητα καμία είσοδος να μην έχει σταθεροποιηθεί στο 0. Δηλαδή, αν $E \subset \{x_i, \overline{x_i} | i = 1, \ldots, n\}$ είναι το σύνολο των εισόδων της πύλης *AND*,

$$\begin{aligned} \mathbb{P}\left[e \neq 0, \forall e \in E\right] &\leq \left(1 - \mathbb{P}\left[e = 0\right]\right)^{|E|} \\ &\leq \left(\frac{\sqrt{n}+1}{2\sqrt{n}}\right)^{4k \log_2 n} \end{aligned}$$

Η συνάρτηση $\frac{x+1}{2x}$ είναι φθίνουσα, επομένως για κάθε $n \geq 4$ έχουμε

$$\left(\frac{\sqrt{n}+1}{2\sqrt{n}}\right) \leq \frac{3}{4}$$

Επομένως,

$$\mathbb{P}\left[e \neq 0, \forall e \in E\right] \leq \left(\frac{3}{4}\right)^{4k\log_2 n} = n^{4k\log_2(3/4)}$$

$$\Rightarrow \mathbb{P}\left[e \neq 0, \forall e \in E\right] = \mathcal{O}\left(\frac{1}{n^k}\right)$$

Παρατηρήστε ότι η ανισότητα αυτή ισχύει γιατί $|E| \geq 4k\log_2 n$.

Στη δεύτερη –συμπληρωματική– περίπτωση, υποθέτουμε ότι το φράγμα εισόδου της πύλης *AND* είναι το πολύ $4k\log_2 n$. Τότε, είναι πολύ πιθανό, ο τυχαίος περιορισμός να σταθεροποιεί τις περισσότερες, εκτός από σταθερού πλήθους τελικά, μεταβλητές. Αυτό έχει νόημα –δηλ. είναι εφικτό–, γιατί αν X είναι η τυχαία μεταβλητή που περιγράφει το πλήθος των μεταβλητών που δεν σταθεροποιήθηκαν, τότε

$$\mathbb{E}\left[X\right] = \left(4k\log_2 n\right)\frac{1}{\sqrt{n}} \to 0, \text{ καθώς } n \to +\infty$$

Και εδώ, παρατηρήστε, ότι αν η τάξη μεγέθους του φράγματος εισόδου ήταν μεγαλύτερη από $log_2 n$, η μέση τιμή της X δεν θα έτεινε προς το μηδέν.

Αν $N \geq 4k\log_2 n$ είναι το πλήθος των εισόδων στην πύλη *AND*, έχουμε μια διωνυμική κατανομή N τυχαίων πειραμάτων. Επομένως, αν α είναι σταθερός αριθμός, τότε

$$\begin{aligned}
\mathbb{P}\left[X \geq \alpha\right] &= \sum_{i=\alpha}^{N}\binom{N}{i}\left(\frac{1}{\sqrt{n}}\right)^i\left(1-\frac{1}{\sqrt{n}}\right)^{N-i} \\
&\leq \sum_{i=\alpha}^{N}\binom{N}{i}\left(\frac{1}{\sqrt{n}}\right)^i \leq \left(\frac{1}{\sqrt{n}}\right)^\alpha \sum_{i=\alpha}^{N}\binom{N}{i} \\
&\leq \left(\frac{1}{\sqrt{n}}\right)^\alpha 2^N \leq \left(\frac{1}{\sqrt{n}}\right)^\alpha 2^{4k\log_2 n} \\
&= n^{4k-\frac{\alpha}{2}}
\end{aligned}$$

Ο στόχος είναι η πιθανότητα του μη επιθυμητού ενδεχομένου –δηλαδή το να σταθεροποιούνται μεταβλητές, περισσότερες από α–, να είναι τάξης μεγέθους το πολύ $\mathcal{O}\left(\frac{1}{n^k}\right)$. Ένα τέτοιο α, που ικανοποιεί αυτή την απαίτηση είναι, $\alpha = e_1 = 10k$. Οπότε,

$$\mathbb{P}\left[X \geq 10k = e_1\right] = \mathcal{O}\left(\frac{1}{n^k}\right)$$

Άρα, σε κάθε περίπτωση, όταν το φράγμα εισόδου στο επίπεδο 1 είναι $c = 1$, με μεγάλη πιθανότητα η τιμή της πύλης *AND* εξαρτάται από το πολύ σταθερού πλήθους μεταβλητές.

Συνεχίζοντας, τώρα, προς το επαγωγικό βήμα, υποθέτουμε ότι υπάρχει σταθερά e_{c-1} η οποία ικανοποιεί το ζητούμενο και βάσει αυτού θα δείξουμε ότι υπάρχει σταθερά e_c που επίσης ικανοποιεί το ζητούμενο.

Όμοια με πριν, διαχωρίζουμε δύο περιπτώσεις με μεγάλο και μικρό φράγμα εισόδου στην πύλη *AND*. Στην πρώτη περίπτωση –όπου δεν χρησιμοποιείται η επαγωγή–, υποθέτουμε ότι πριν τον τυχαίο περιορισμό, η πύλη *AND* συνδέεται με το επίπεδο 1, με $N \geq d \log_2 n$ πύλες *OR*, οι οποίες ανά δύο έχουν ξένα σύνολα μεταβλητών εισόδου, όπου $d = k2^c$.

Θα δείξουμε ότι μετά την εφαρμογή του τυχαίου περιορισμού, είναι πολύ πιθανό όλες οι μεταβλητές κάποιας από τις πύλες *OR* του πρώτου επιπέδου, να είναι σταθεροποιημένες στο 0. Αυτό συνεπάγεται ότι και η πύλη *AND* του δεύτερου επιπέδου είναι κι αυτή σταθεροποιημένη στο 0, οπότε δεν εξαρτάται από καμιά μεταβλητή. Ειδικότερα θα δείξουμε ότι η πιθανότητα η πύλη *AND* να μη σταθεροποιηθεί στο μηδέν, είναι $\mathcal{O}\left(\frac{1}{n^k}\right)$. Αυτό αποδεικνύεται ως εξής:

Αν θεωρήσουμε μία συγκεκριμένη πύλη *OR*, έχουμε,

$$\begin{gathered}\mathbb{P}\left[\text{πύλη } OR \equiv 1\right] = \\ 1 - \mathbb{P}\left[\text{πύλη } OR \equiv 0\right] = \\ 1 - \left(\frac{1 - 1/\sqrt{n}}{2}\right)^c \leq 1 - \frac{1}{2^c}\end{gathered}$$

Άρα,

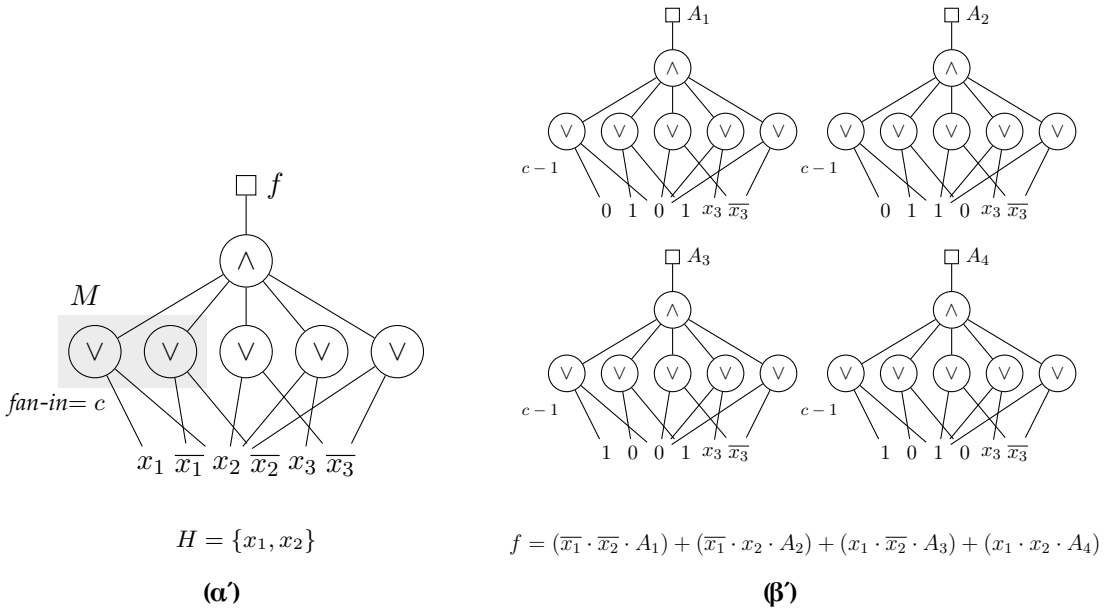
$$\begin{gathered}\mathbb{P}\left[\text{πύλη } AND \not\equiv 0\right] \leq \\ \mathbb{P}\left[\text{για κάθε πύλη } OR \text{ του } 1^{\text{ου}} \text{ επιπέδου: } OR \equiv 1\right] \leq \\ \left(\mathbb{P}\left[\text{μία πύλη } OR \equiv 1\right]\right)^N \leq \left(\mathbb{P}\left[\text{μία πύλη } OR \equiv 1\right]\right)^{d \log_2 n} \leq \\ \left(1 - \frac{1}{2^c}\right)^{d \log_2 n} = n^{k2^c \log_2\left(1-2^{-c}\right)} \leq n^{k2^c\left(-2^{-c}\right)} = \frac{1}{n^k}\end{gathered}$$

Επομένως, με μεγάλη πιθανότητα η πύλη *AND* δεν εξαρτάται από καμιά μεταβλητή.

Στη δεύτερη περίπτωση λειτουργεί το επαγωγικό βήμα. Η ιδέα είναι να αναλυθεί το κύκλωμα σε υποκυκλώματα με φράγμα εισόδου $c-1$ για τα οποία μπορούμε να χρησιμοποιήσουμε την επαγωγική υπόθεση. Όπως θα δούμε παρακάτω, το στοίχημα είναι το πλήθος αυτών των υποκυκλωμάτων να μην είναι υπερβολικά μεγάλο, έτσι ώστε να ισχύει το άνω φράγμα που επιδιώκουμε.

Επιλέγουμε λοιπόν από το πρώτο επίπεδο, πύλες *OR* οι οποίες έχουν σύνολα εισόδων ανά δύο ξένα μεταξύ τους και θεωρούμε M ένα μεγιστικό σύνολο από τέτοιες πύλες. Θέλουμε να εμπλέξουμε όσο γίνεται μικρότερο σύνολο εισόδων το ο οποίο να επηρεάζει όλες τις πύλες (αλλιώς δεν μπορεί να γίνει ανάλυση σε υποκυκλώματα). Έστω επίσης H το σύνολο των μεταβλητών που εμφανίζονται στις εισόδους τους. Υποθέτουμε ότι το πλήθος αυτών των πυλών είναι μικρότερο από $d \log n$, όπου $d = k2^c$.

Με αυτές τις επιλογές, παρατηρούμε ότι κάθε πύλη *OR* του πρώτου επιπέδου έχει τουλάχιστον μία μεταβλητή εισόδου από το σύνολο H. Αυτό ισχύει γιατί αν



$H = \{x_1, x_2\}$

(α΄)

$f = (\overline{x_1} \cdot \overline{x_2} \cdot A_1) + (\overline{x_1} \cdot x_2 \cdot A_2) + (x_1 \cdot \overline{x_2} \cdot A_3) + (x_1 \cdot x_2 \cdot A_4)$

(β΄)

Για το επαγωγικό βήμα της απόδειξης, θέλουμε να αναλύσουμε το αρχικό κύκλωμα σε υποκυκλώματα με φράγμα εισόδου (*fan-in*) $c-1$. Αυτό γίνεται επιλέγοντας όσο γίνεται τις λιγότερες μεταβλητές – σύνολο H– που επηρεάζουν όλες τις πύλες *OR* και περιορίζοντάς τις με όλους τους συνδυασμούς τιμών. Έτσι, παράγονται κυκλώματα (σχήμα δεξιά) συνιστώσες του αρχικού κυκλώματος, με φράγμα εισόδου $c-1$ για τα οποία ισχύει η επαγωγική υπόθεση. Επίσης, με αυτόν τον τρόπο παράγονται αρκούντως λίγα υποκυκλώματα, ώστε η f να εξαρτάται τελικά από το πολύ σταθερού πλήθους μεταβλητές.

Σχήμα 2.6: Το επαγωγικό βήμα για την απόδειξη του Ισχυρισμού 2: ανάλυση του αρχικού κυκλώματος σε μικρότερα κυκλώματα με φράγμα εισόδου $c-1$.

υπήρχε μία πύλη, g, χωρίς καμία μεταβλητή από το H, τότε το σύνολο των εισόδων της θα ήταν ξένο προς τα σύνολα εισόδων όλων των πυλών του M. Τότε όμως, το $M \cup \{g\}$ θα ήταν σύνολο πυλών με ξένα ανά δύο σύνολα εισόδων, οπότε το M δεν θα μπορούσε να είναι μεγιστικό· άτοπο.

Με δεδομένη αυτή την παρατήρηση, ξέρουμε ότι κάθε ανάθεση τιμών στις μεταβλητές του συνόλου H επηρεάζει κάθε πύλη *OR* του πρώτου επιπέδου. Το πλήθος όλων των δυνατών αναθέσεων, είναι $l = 2^{|H|}$. Εφαρμόζοντάς τις στο αρχικό *AND-OR* κύκλωμα, σταθεροποιείται τουλάχιστον μία είσοδος σε κάθε πύλη *OR*. Οπότε, για κάθε ανάθεση, προκύπτει ένα νέο κύκλωμα του οποίου όλες οι πύλες *OR* έχουν φράγμα εισόδου, το πολύ $c-1$. Έστω $A_1, \ldots, A_l$ τα κυκλώματα που προκύπτουν από αυτή τη διαδικασία. Από επαγωγική υπόθεση, η πιθανότητα του ενδεχομένου η τιμή του κυκλώματος A_j^r να εξαρτάται από περισσότερες από e_{c-1} μεταβλητές είναι το πολύ $\mathcal{O}\left(\frac{1}{n^k}\right)$.

Ο στόχος είναι να εκφράσουμε το αρχικό κύκλωμα συναρτήσει των $A_1, \ldots, A_l$ με τρόπο ώστε να μην αυξηθεί η τάξη μεγέθους της παραπάνω πιθανότητας. Για να γίνει αυτό, επεξεργαζόμαστε, αντί για το αρχικό κύκλωμα, τη λογική συνάρτηση την οποία εκφράζει.

Έστω τώρα, f, η συνάρτηση που εκφράζεται από το αρχικό *AND-OR* κύκλωμα. Από το Θεώρημα Επέκτασης του Boole (βλ. Θεώρημα 1.2), έχουμε ότι η f εκφράζεται ως πολυγραμμικός συνδυασμός των κυκλωμάτων $A_1, \ldots, A_l$[3]. Το πλήθος των όρων του αθροίσματος είναι όσα και τα κυκλώματα, l. Για παράδειγμα, αν $H = \{x_1, x_2\}$ και το κύκλωμα A_i αντιστοιχεί στον περιορισμό $(x_1 x_2)_2 = (i-1)_{10}$, τότε,

$$f = (\overline{x_1} \cdot \overline{x_2} \cdot A_1) + (\overline{x_1} \cdot x_2 \cdot A_2) + (x_1 \cdot \overline{x_2} \cdot A_3) + (x_1 \cdot x_2 \cdot A_4)$$

Από τα παραπάνω γίνεται φανερό ότι μετά από την εφαρμογή του τυχαίου περιορισμού, η πιθανότητα του ενδεχομένου η συνάρτηση του περιορισμένου κυκλώματος, f^r, να εξαρτάται από περισσότερες από $l^r \cdot e_{c-1}$ μεταβλητές, είναι το πολύ $l^r \cdot \mathcal{O}\left(\frac{1}{n^k}\right)\cdot$ όπου l^r είναι το πλήθος των όρων που διατηρούνται μετά τον περιορισμό. Οπότε, το ζητούμενο είναι το πλήθος, l^r, των όρων στο άθροισμα που εκφράζει την f^r, να είναι σταθερό, δηλαδή να μην εξαρτάται από το n.

Έστω, λοιπόν, h η τυχαία μεταβλητή που εκφράζει το πλήθος των μεταβλητών εισόδου από το H που δεν σταθεροποιήθηκαν από τον τυχαίο περιορισμό. Τότε, αν α είναι μια σταθερά,

$$\mathbb{P}[h > \alpha] = \sum_{i=\alpha}^{|H|} \binom{|H|}{i} \left(\frac{1}{\sqrt{n}}\right)^i \left(1 - \frac{1}{\sqrt{n}}\right)^{|H|-i} \leq$$

$$\sum_{i=\alpha}^{|H|} \binom{|H|}{i} \left(\frac{1}{\sqrt{n}}\right)^i \leq \left(\frac{1}{\sqrt{n}}\right)^\alpha \sum_{i=\alpha}^{|H|} \binom{|H|}{i} \leq n^{-\alpha/2} 2^{|H|}$$

Αφού εξετάζουμε την περίπτωση όπου οι πύλες *OR* που ανήκουν στο μεγιστικό σύνολο M είναι το πολύ $d \log_2 n$ και έχουν φράγμα εισόδου c, ισχύει $|H| \leq c \cdot d \cdot log_2 n$. Επομένως,

$$\mathbb{P}[h > a] \leq n^{-\alpha/2} 2^{cd \log_2 n} = n^{\frac{\alpha}{2} + cd}$$

Θέτοντας $-\alpha/2 + cd = -k$, παίρνουμε $\alpha = 2(k + cd)$ και άρα,

$$\mathbb{P}[h > 2(k + cd)] \leq \frac{1}{n^k}$$

Δηλαδή, με μεγάλη πιθανότητα, μετά από την εφαρμογή του τυχαίου περιορισμού το πλήθος των μεταβλητών από το σύνολο H που δεν σταθεροποιήθηκαν είναι σταθερό, ανεξάρτητο από το n.

Επομένως, η συνάρτηση του κυκλώματος μετά τον περιορισμό, f^r, με μεγάλη πιθανότητα εκφράζεται από το πολύ $2^h \leq m := 2^{2(k+cd)}$ μη μηδενικούς όρους.

[3] Η f προφανώς δεν εκφράζεται ως συνδυασμός κυκλωμάτων, αλλά ως συνδυασμός των συναρτήσεων που εκφράζουν αυτά τα κυκλώματα. Διατηρούμε αυτή τη ρητορική αυθαιρεσία για να μην περιπλακούν άσκοπα οι διατυπώσεις.

Τελικά, αν ορίσουμε $e_c = m \cdot e_{c-1}$, έχουμε:

$$\mathbb{P}\left[\text{Η } f^r \text{ εξαρτάται από περισσότερες από } e_c \text{ μεταβλητές}\right] \leq$$
$$\mathbb{P}\left[h > 2(k+cd)\right] + \mathbb{P}\left[\text{κάποιο } A_j^r \text{ εξαρτάται από περισσότερες από } e_{c-1} \text{ μεταβλητές}\right] \leq$$
$$\mathcal{O}\left(\frac{1}{n^k}\right) + m \cdot \mathcal{O}\left(\frac{1}{n^k}\right) = \mathcal{O}\left(\frac{1}{n^k}\right)$$

Με αυτό, ολοκληρώνεται η απόδειξη του Ισχυρισμού 2.

□ (Ισχυρισμός 2)

Με δεδομένο τον Ισχυρισμό 2, ο Ισχυρισμός 1 –και συνεπώς, το Θεώρημα 2.4– προκύπτει σχεδόν άμεσα: Έτσι όπως ορίσαμε αρχικά το πιθανοθεωρητικό πλαίσιο, συμπεραίνουμε ότι υπάρχει περιορισμός που αφήνει αρκετές μεταβλητές μη σταθεροποιημένες (βλ. Πρόταση 2.5). Από τον Ισχυρισμό 2 έχουμε ότι κάθε υποκύκλωμα *AND-OR* στα επίπεδα 2 και 1 εξαρτάται από το πολύ σταθερού πλήθους μεταβλητές.

Αυτό μας δίνει τη δυνατότητα να «αντιμεταθέσουμε» τα επίπεδα 1 και 2 αυξάνοντας το μέγεθος του κυκλώματος, κατά μία σταθερά το πολύ (βλ. Παρατήρηση 2). Μετά από αυτό, τα επίπεδα 2 και 3 στο νέο κύκλωμα έχουν ίδιου τύπου πύλες και μπορούν να συγχωνευθούν και να μειωθεί το βάθος του κυκλώματος κατά 1.

Οπότε τελικά, παίρνουμε ένα κύκλωμα πολυωνυμικού μεγέθους, βάθους $t-1$ και σταθερού φράγματος εισόδου το οποίο υπολογίζει συνάρτηση ισοτιμίας· άτοπο, γιατί έχουμε υποθέσει ότι το t είναι το ελάχιστο βάθος κυκλώματος με αυτή την ιδιότητα.

□ (Ισχυρισμός 1)

□ (Θεώρημα 2.4)

Συμπερασματικά, από την Πρόταση 2.2 και το Θεώρημα 2.4, μπορούμε να πούμε ότι για τα λογικά κυκλώματα πολυωνυμικού μεγέθους που αποτελούνται από πύλες λογικής σύζευξης (*AND*) και διάζευξης (*OR*), και τα οποία θα μπορούσαν να εκφράσουν συναρτήσεις ισοτιμίας, η λογαριθμική τάξη μεγέθους, $\mathcal{O}(\log n)$, ως προς το πλήθος των μεταβλητών εισόδου, είναι κάτω φράγμα του βάθους.

3 Βελτίωση με Αλγεβρική Οπτική.

Στο πλαίσιο του προβλήματος που επεξεργαζόμαστε, η προσπάθεια βελτίωσης ενός αποτελέσματος γενικά κινείται προς μια κατεύθυνση είτε ποιοτική, είτε ποσοτική. Στην πρώτη περίπτωση, με δεδομένο κάποιο φράγμα, αναζητούνται κυκλώματα με ισχυρότερες ιδιότητες, ενώ στη δεύτερη γίνεται προσπάθεια βελτίωσης του φράγματος για δεδομένου τύπου κυκλώματα.

Στο κεφάλαιο αυτό, παρουσιάζεται μια ποσοτική βελτίωση του κάτω φράγματος που αναδείχθηκε στο προηγούμενο κεφάλαιο, συνδυάζοντας πιθανοθεωρητική πολυωνυμική προσέγγιση και αλγεβρική μέθοδο. Το αποτέλεσμα αυτό οφείλεται στους Alexander Razborov [33] και Roman Smolensky [34]. Ο Razborov έδειξε ότι κυκλώματα σταθερού βάθους και πολυωνυμικού μεγέθους με πύλες *AND*, *OR*, MOD_2 (δηλ. *XOR*) μπορούν να προσεγγιστούν από πολυώνυμα πολυλογαριθμικού βαθμού, αλλά με μεγάλη πιθανότητα, αυτό δεν μπορεί να γίνει για κυκλώματα που εκφράζουν τη συνάρτηση MOD_3[4]. Ο Smolensky χρησιμοποιώντας αλγεβρικές μεθόδους, γενίκευσε το αποτέλεσμα αυτό για συναρτήσεις MOD_p όπου p πρώτος αριθμός.

Το πρώτο στάδιο της απόδειξης συνιστά εφαρμογή της *μεθόδου πολυωνύμου* [35] [36]. Η τεχνική αυτή έχει ευρεία εφαρμογή σε προβλήματα κυκλωμάτων μικρής πολυπλοκότητας (μικρού βάθους ή μεγέθους), συνθέτοντας κυρίως επιχειρήματα μη εφικτότητας (impossibility).

Η γενική ιδέα είναι ότι συναρτήσεις που εκφράζονται από μικρής πολυπλοκότητας κυκλώματα, μπορούν να εκφραστούν προσεγγιστικά και από μικρής πολυπλοκότητας πολυώνυμα πάνω από κάποια αλγεβρική δομή. Κατόπιν, εφόσον αποδειχθεί κάτι τέτοιο, εκμεταλλευόμαστε αλγεβρικές ιδιότητες των πολυωνύμων για να καταλήξουμε στο επιδιωκόμενο αποτέλεσμα.

Στη συνέχεια, όπως και στο προηγούμενο κεφάλαιο, επικεντρωνόμαστε στην περίπτωση κυκλωμάτων σταθερού βάθους με πολυωνυμικό μέγεθος, με δύο ειδών πύλες –*AND* και *OR*– καθώς και στην προσέγγιση συναρτήσεων ισοτιμίας, π_n.

Θα δείξουμε λοιπόν, ότι οι συναρτήσεις ισοτιμίας δεν ανήκουν στην κλάση AC^0.

Θεώρημα 3.1.
Έστω $\pi_n : \{0,1\}^n \to \{0,1\}$, *συνάρτηση ισοτιμίας.*
Τότε, $\pi_n \notin AC^0, \forall n \in \mathbb{N}$.

Απόδειξη.
Η επιχειρηματολογία της απόδειξης αναπτύσσεται ως εξής:

1. Αρχικά αποδεικνύουμε ότι κάθε συνάρτηση που υπολογίζεται από κάποιο κύκλωμα AC^0, μπορεί να προσεγγιστεί από κάποιο πολυώνυμο p πολύ μικρού βαθμού, δηλ. πολυλογαριθμικού ως προς n. Με τον όρο προσέγγιση εννοούμε ότι για όλα *σχεδόν* (δηλ. πλην ελαχίστων) τα διανύσματα $(a_1, \ldots, a_n) \in \{0,1\}^n$, ισχύει $f(a_1, \ldots, a_n) = p(a_1, \ldots, a_n)$.

[4] Η συνάρτηση MOD_p ορίζεται ως $MOD_p(x_1, \ldots, x_n) \equiv x_1 + \cdots + x_n \mod p$.

2. Στο δεύτερο στάδιο της απόδειξης, χρησιμοποιώντας ένα αλγεβρικό επιχείρημα δείχνουμε ότι οι συναρτήσεις ισοτιμίας είναι αδύνατο να προσεγγιστούν από τέτοια πολυώνυμα.

Είναι σαφές ότι μια λογική συνάρτηση μπορεί να εκφραστεί ως πολυώνυμο. Η αναπαράσταση που θα χρησιμοποιήσουμε εδώ θα είναι πολυώνυμα πραγματικών τιμών της μορφής $\{0,1\}^n \to \{0,1\}$ θεωρώντας ότι το 0 αντιστοιχεί στην λογική τιμή *ψεύδους* (false) και το 1 στη λογική τιμή *αλήθειας* (true).

Αρχικά παρατηρούμε ότι μία πύλη *AND* μπορεί να εκφραστεί ως πολυώνυμο βαθμού τουλάχιστον n:

$$AND\,(x_1, \cdots, x_n) = x_1 \cdot x_2 \cdot \cdots \cdot x_n = \prod_{i=1}^{n} x_i$$

Όμοια για μια πύλη *OR*:

$$OR\,(x_1, \cdots, x_n) = 1 - AND(\overline{x_1}, \cdots, \overline{x_n}) = 1 - \prod_{i=1}^{n} (1 - x_i)$$

Για να αντιμετωπιστεί το πρόβλημα του μεγάλου βαθμού, ιδανικά θα θέλαμε με κατάλληλο τρόπο να αφαιρέσουμε παράγοντες από τα μονώνυμα του πολυωνύμου της πύλης ώστε να μειωθεί ο βαθμός χωρίς το πολυώνυμο να απέχει σημαντικά από τη συνάρτηση της πύλης *OR*. Κάτι τέτοιο θα μπορούσε να επιτευχθεί με δοκιμαστικές προσθαφαιρέσεις παραγόντων μέχρι μικρό βαθμό και καλή προσέγγιση. Όμως, επειδή αφενός αυτό είναι εξαιρετικά δύσκολο (δηλ. χρονοβόρο) και αφετέρου μας ενδιαφέρει η ύπαρξη τέτοιων πολυωνύμων και όχι ο ρητός προσδιορισμός τους, καταφεύγουμε σε μια πιθανοθεωρητική διαδικασία δραστικής μείωσης του βαθμού του πολυωνύμου προσέγγισης.

Ο πυρήνας της ιδέας, οφείλεται στους Valiant και Varizani [37], οι οποίοι με την τεχνική αυτή σε διαφορετικό πλαίσιο, απέδειξαν ότι αν υπάρχει πολυωνυμικού χρόνου λύση στο πρόβλημα εύρεσης μοναδικής ικανοποίησης μιας λογικής έκφρασης (*USAT*), τότε οι κλάσεις *NP*[5] και *RP*[6] ταυτίζονται.

Η μεταφορά της ιδέας [38] στο παρόν συγκείμενο, έχει ως εξής: αν στην πολυωνυμική έκφραση της *OR* αντικατασταθούν τα x_i με λογικές εκφράσεις των οποίων το μέγεθος φθίνει πολύ γρήγορα ως προς i, τότε το πλήθος των παραγόντων μειώνεται δραστικά και επομένως το ίδιο και ο βαθμός του πολυωνύμου. Επίσης, η κατασκευή του τυχαίου πολυωνύμου, θα πρέπει να είναι τέτοια ώστε με ικανοποιητική πιθανότητα προσομοιώνει την πύλη *OR*.

Για τη συνέχεια, αν p είναι το πολυώνυμο που προσεγγίζει την πύλη *OR*, ονομάζουμε *πιθανότητα σφάλματος* έναν αριθμό $\epsilon \in (0,1)$ για τον οποίο ισχύει

$$\mathbb{P}\,[OR \equiv p] = 1 - \epsilon$$

[5] *NP* είναι το σύνολο των προβλημάτων που λύνονται σε πολυωνυμικό χρόνο από Μη-Ντετερμινιστική Μηχανή Turing.

[6] *RP* είναι το σύνολο των υπολογιστικών προβλημάτων που λύνονται σε πολυωνυμικό χρόνο από Πιθανοθεωρητική Μηχανή Turing.

Πρόταση 3.2.
Για οποιοδήποτε $\epsilon \in (0,1)$ υπάρχει τυχαίο πολυώνυμο λογαριθμικού βαθμού το οποίο προσεγγίζει τη λογική συνάρτηση OR: $\{0,1\}^n \to \{0,1\}$, με πιθανότητα σφάλματος το πολύ ϵ.

Απόδειξη.

Έχοντας ως στόχο να προσομοιώσουμε την πύλη *OR* γίνεται μια ευρηματική κατασκευή με την ακόλουθη ιδέα. Ξεκινάμε από την παραπάνω έκφραση της *OR* ως άρνηση της *AND*, $1 - \prod_{i=1}^{n}(1 - x_i)$. Θέλουμε αφενός το νέο πολυώνυμο να έχει μικρό βαθμό και αφετέρου με καλή πιθανότητα να ικανοποιείται το κύριο χαρακτηριστικό της λογικής διάζευξης, δηλαδή να αρκεί για ένα j να ισχύει $x_j = 1$ για να πάρει όλο το πολυώνυμο τιμή 1. Η ιδέα είναι να αντικατασταθούν τα x_i στο παραπάνω γινόμενο, με τυχαία αθροίσματα, έστω q_i, μεταβλητών με προοδευτικά μειούμενο αριθμό όρων. Αν η μείωση αυτή είναι περίπου στο μισό σε κάθε σε κάθε αύξηση του i, τότε ο βαθμός του νέου πολυωνύμου θα περιοριστεί σε λογαριθμική τάξη, αφού γρήγορα θα εξαντληθούν οι όροι. Επίσης, με κατάλληλα τυχαία επιλογή των όρων των αθροισμάτων, ελπίζουμε ότι κάποιο q_i θα έχει ακριβώς την τιμή 1. Δεν μας νοιάζει τι τιμή έχουν τα υπόλοιπα, αφού το γινόμενο $\prod(1 - q_i)$ θα έχει μηδενιστεί.

Ορίζουμε, λοιπόν, μια φθίνουσα ακολουθία συνόλων δεικτών: Αν $S_0 = \{1, \ldots, n\}$, τότε $S_{i+1} \subseteq S_i$, και κάθε στοιχείο $j \in S_i$ βρίσκεται στο S_{i+1} με πιθανότητα $1/2$ (βλ. Σχήμα 3.1).

Έστω τα σύνολα $S_0, S_1, \ldots, S_{\log n+2}$ και το τυχαίο πολυώνυμο $q_i = \sum_{j \in S_i} x_j$. Είναι προφανές ότι σε λογαριθμικής τάξης πλήθος βημάτων το μέγεθος των συνόλων S_i έχει εξαντληθεί. Αν $p = \prod_{i=0}^{\log n+2}(1 - q_i)$, θα δείξουμε ότι η πύλη *OR* προσεγγίζεται από το πολυώνυμο $1 - p$.

Εξετάζουμε τις περιπτώσεις στις οποίες παίρνει τιμές η συνάρτηση *OR*. Όταν $OR(x_1, \ldots, x_n) = 0$, τότε αναγκαστικά $x_i = 0$ για κάθε i. Σε αυτή την περίπτωση όλα τα q_i είναι 0 και κατά συνέπεια $1 - p = 0$. Τα πολυώνυμα q_i έχουν βαθμό 1 και άρα ο βαθμός του πολυωνύμου $1 - p$ είναι $\mathcal{O}(\log n)$.

Διατυπώνουμε τη δεύτερη περίπτωση ως λήμμα το οποίο θα αποδείξουμε αργότερα.

Λήμμα 3.3.
Έστω $OR(x_1, \ldots, x_n) = 1$ και q_i τα τυχαία πολυώνυμα όπως ορίστηκαν παραπάνω. Με πιθανότητα τουλάχιστον $1/2$ υπάρχει q_i με τιμή ακριβώς 1.

Με δεδομένο το Λήμμα 3.3, αν υπάρχει i ώστε $q_i = 1$, τότε $p = 0$. Αυτό σημαίνει ότι ακριβώς μία από τις μεταβλητές που συνιστούν αυτό το q_i πρέπει να είναι ίση με 1. Δεν μας ενδιαφέρει τι τιμή παίρνουν τα υπόλοιπα $q_j, j \neq i$, αφού μας αρκεί ένα για να μηδενιστεί το πολυώνυμο p. Οπότε σε αυτή την περίπτωση, $\mathbb{P}[1 - p = 1] \geq 1/2$.

Δηλαδή, το πολυώνυμο $1 - p$ προσεγγίζει τη συνάρτηση *OR* με πιθανότητα τουλάχιστον $1/2$, η οποία όμως είναι πολύ μικρή για να θεωρηθεί ικανοποιητική. Αυτό διορθώνεται εύκολα αναπαράγοντας, με ανεξάρτητο τρόπο, όσα χρειάζονται περισσότερα τυχαία πολυώνυμα, μέχρι σταθερού πλήθους t. Αν $p_1, \ldots, p_t$ τα νέα τυχαία

$$
\begin{array}{ll}
S_0 = \{1,2,3,4,5,6,7,8,9,10\} & q_0 = x_1 + x_2 + x_3 + \cdots + x_{10} \\
S_1 = \{1,2,5,6,7\} & q_1 = x_1 + x_2 + x_5 + x_6 + x7 \\
S_2 = \{1,2,6\} & q_2 = x_1 + x_2 + x_6 \\
S_3 = \{6\} & q_3 = x_6 \\
S_4 = \{6\} & q_4 = x_6 \\
S_5 = \{\} & q_5 = 0 \\
 & \\
 & q_i = \sum_{j \in S_i} x_j \\
\mathbb{P}\left[i \in S_k | i \in S_{k-1}\right] = \frac{1}{2} & p = \prod_{i=0}^{\log 10+2} (1 - q_i) \\
 & \\
 & \mathbb{P}\left[OR \equiv 1 - p\right] \geq 1/2
\end{array}
$$

Ο στόχος είναι το πολυώνυμο προσέγγισης να έχει μικρό βαθμό σε σχέση με τον βαθμό του πολυωνύμου που εκφράζει την $OR = 1 - \prod_{i=1}^{n}(1 - x_i)$. Δημιουργούμε ακολουθία τυχαίων πολυωνύμων, q_i, που ο βαθμός τους μειώνεται ραγδαία. Από το σχήμα (δεξιά) φαίνεται ότι η πιθανότητα ένα από αυτά να έχει τιμή 1, είναι σημαντική· αν αυτή είναι τουλάχιστον $1/2$, τότε $\mathbb{P}\left[OR \equiv 1 - p\right] \geq 1/2$.

Σχήμα 3.1: Η βασική κατασκευή του τυχαίου πολυωνύμου προσέγγισης της πύλης OR.

πολυώνυμα, τότε το πολυώνυμο $1 - p_1 p_2 \ldots p_t$ έχει (τον ικανοποιητικά μικρό) βαθμό $\mathcal{O}\left(t \log n\right)$. Επίσης,

$$\mathbb{P}\left[p_1 \ldots p_t = 1\right] = \prod_{i=1}^{t} \mathbb{P}\left[p_i \neq 0\right] = \left(1 - 1/2\right)^t = 2^{-t}$$

Επομένως,

$$\mathbb{P}\left[1 - p_1 \ldots p_t = 1\right] \geq 1 - 2^{-t}$$

Για δοσμένη πιθανότητα σφάλματος ϵ το επιθυμητό t προσδιορίζεται εύκολα: $2^{-t} \leq \epsilon \Rightarrow t \geq \log 1/\epsilon$.

□ (Πρόταση 3.2)

Η προσέγγιση ενός κυκλώματος μίας πύλης AND γίνεται με ανάλογο τρόπο. Αν $p = p_1 \ldots p_t$ το πολυώνυμο προσέγγισης της OR, τότε,

$$\begin{aligned} AND\left(x_1, \ldots, x_n\right) &= \overline{OR\left(\overline{x_1}, \ldots, \overline{x_n}\right)} \Rightarrow \\ AND\left(x_1, \ldots, x_n\right) &\approx p\left(1 - x_1, \ldots, 1 - x_n\right) \end{aligned}$$

Στη συνέχεια αποδεικνύουμε το Λήμμα 3.3:

Απόδειξη Λήμματος 3.3.
Έστω $T \subseteq S_0$ το σύνολο των δεικτών των μεταβλητών με τιμή 1. Αναδιατυπώνοντας το ζητούμενο, θέλουμε να δείξουμε ότι η πιθανότητα να υπάρχει ένα $i \in \{0, 1, \ldots, \log n + 2\}$ ώστε $|T \cap S_i| = 1$, είναι τουλάχιστον $1/2$. Για την εκτίμηση αυτής της πιθανότητας διαχωρίζουμε δύο περιπτώσεις:

(1) Για κάθε $i \in \{0, 1, \ldots, \log n + 2\}$, $|T \cap S_i| > 1$. Αυτό είναι το κακό ενδεχόμενο γιατί αν ισχύει, τότε σίγουρα δεν υπάρχει κανένα i με τη ζητούμενη ιδιότητα.

(2) Υπάρχει $i \in \{0, 1, \ldots, \log n + 2\}$ ώστε $|T \cap S_i| \leq 1$.

Παρατηρούμε ότι το πρώτο ενδεχόμενο ισοδυναμεί με $|T \cap S_{\log n+2}| > 1$. Αυτό ισχύει γιατί, αφού η ακολουθία S_i είναι φθίνουσα, έχουμε

$$T \cap S_{\log n+2} \subseteq T \cap S_i, \forall i \Rightarrow$$
$$1 < |T \cap S_{\log n+2}| \leq |T \cap S_i|, \forall i \Rightarrow$$
$$\left\{|T \cap S_{\log n+2}| > 1\right\} \subseteq \{\forall i, |T \cap S_i| > 1\}$$

Επίσης, αν η τομή των T, S_i έχει περισσότερα από ένα στοιχεία για κάθε i, τότε προφανώς αυτό ισχύει και για την $T \cap S_{\log n+2}$. Επομένως, ισχύει και ο αντίστροφος εγκλεισμός.

Αρκεί, λοιπόν, να εκτιμήσουμε την πιθανότητα, $\mathbb{P}\left[|T \cap S_{\log n+2}| > 1\right]$. Αρχικά παρατηρούμε ότι κάθε μεταβλητή εισόδου που αντιστοιχεί στο S_0, επιβιώνει της τυχαίας διαδικασίας μέχρι τέλους, ανεξάρτητα από τις υπόλοιπες, στο $S_{\log n+2}$ με πιθανότητα $2^{-(\log n+2)}$. Δηλαδή, η τυχαία μεταβλητή $|S_{\log n+2}|$ ακολουθεί την διωνυμική κατανομή, n δοκιμών Bernoulli με πιθανότητα επιτυχίας $2^{-(\log n+2)}$. Επομένως, έχουμε:

$$\mathbb{P}\left[|T \cap S_{\log n+2}| > 1\right] \leq \mathbb{P}\left[|T \cap S_{\log n+2}| \geq 1\right] =$$
$$1 - \mathbb{P}\left[|T \cap S_{\log n+2}| < 1\right] = 1 - \binom{n}{0}\left(\frac{1}{2^{\log n+2}}\right)^0\left(1 - \frac{1}{2^{\log n+2}}\right)^n =$$
$$1 - \left(\frac{4n-1}{4n}\right)^n \leq 1 - \frac{3}{4} \Rightarrow$$
$$\mathbb{P}\left[|T \cap S_{\log n+2}| > 1\right] \leq \frac{1}{4}$$

Για τη δεύτερη περίπτωση, όπου υπάρχει i, ώστε $|T \cap S_i| \leq 1$, διαχωρίζουμε δύο υποπεριπτώσεις:

(2A) $|T \cap S_0| = |T| = 1$.
Σε αυτή την περίπτωση $q_0 = \sum_{j \in S_0} x_j = 1$ και συνεπώς $1 - p = 1 = OR$.
Σημειώνουμε επίσης, ότι δεν υπάρχει περίπτωση $|T| = 0$, γιατί εξετάζουμε την περίπτωση όπου $OR = 1$, οπότε τουλάχιστον ένα x_i έχει την τιμή 1.

(2B) $|T \cap S_0| = |T| > 1$ και υπάρχει i, ώστε $|T \cap S_i| \leq 1$.

Στην περίπτωση (2B), έστω i ο δείκτης για τον οποίο $|T \cap S_{i-1}| > 1$ και $|T \cap S_i| \leq 1$. Τότε,

$$\mathbb{P}\left[\{|T \cap S_i| = 1\} \,\middle|\, \{|T \cap S_i| \leq 1\} \cap \{|T \cap S_{i-1}| > 1\}\right] =$$
$$\frac{\mathbb{P}\left[\{|T \cap S_i| = 1\} \cap \{|T \cap S_{i-1}| > 1\}\right]}{\mathbb{P}\left[\{|T \cap S_i| \leq 1\} \cap \{|T \cap S_{i-1}| > 1\}\right]}$$

Αν θέσουμε $t = |T \cap S_{i-1}|$, τότε ο αριθμητής είναι η πιθανότητα από τα t στοιχεία του $T \cap S_{i-1}$ να επιβιώσει στο επόμενο βήμα, στο $T \cap S_i$ ακριβώς ένα στοιχείο, δηλαδή: $\binom{t}{1}(1/2)^1(1/2)^{t-1}$. Ο παρονομαστής αναλύεται σε δύο ξένα ενδεχόμενα: $\{|T \cap S_i| = 1\} \cap \{|T \cap S_{i-1}| > 1\}$ και $\{|T \cap S_i| = 0\} \cap \{|T \cap S_{i-1}| > 1\}$. Το πρώτο είναι το ίδιο με αυτό στον αριθμητή, ενώ το δεύτερο σημαίνει την επιβίωση κανενός, από τα t, στοιχείο του $T \cap S_{i-1}$ στο $T \cap S_i$, που η πιθανότητά του είναι $\binom{t}{0}(1/2)^0(1/2)^t$

Συνεπώς, η παραπάνω δεσμευμένη πιθανότητα γίνεται:

$$\frac{\binom{t}{1}2^{-t}}{\binom{t}{0}2^{-t} + \binom{t}{1}2^{-t}} = \frac{t}{1+t} \geq \frac{2}{3}$$

Συνοψίζοντας τα παραπάνω παρατηρούμε ότι η τομή του ενδεχόμενου (2Β) με την άρνηση του (1) ισοδυναμεί με το ότι υπάρχει $i \in \{0, \ldots, \log n + 2\}$ για το οποίο $|T \cap S_i| = 1$.

Συνδυάζοντας τις παραπάνω εκτιμήσεις, έχουμε ότι η πιθανότητα να μην ισχύει η (κακή) περίπτωση (1) είναι τουλάχιστον $3/4$ και η πιθανότητα να ισχύει η περίπτωση (2Β) είναι τουλάχιστον $2/3$. Η τομή τους μας δίνει,

$$\mathbb{P}\left[\exists i \in \{0, \ldots, \log n + 2\} : |T \cap S_i| = 1\right] \geq \frac{1}{2}$$

□ (Λήμμα 3.3)

Από την Πρόταση 3.2 λοιπόν, έχουμε ότι το πολυώνυμο $1 - p$ μπορεί να προσεγγίσει ένα κύκλωμα μίας πύλης για οποιαδήποτε δοσμένη πιθανότητα σφάλματος, ϵ,

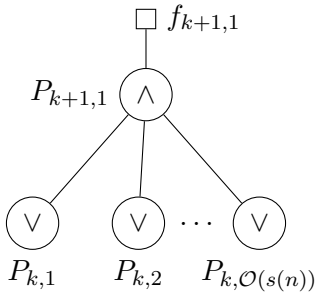
$$\mathbb{P}\left[1 - p \equiv OR\right] \geq 1 - \epsilon$$

Γενικεύοντας για μια οποιαδήποτε συνάρτηση της κλάσης AC^0, αποδεικνύουμε την επόμενη πρόταση:

Πρόταση 3.4.
Έστω λογική συνάρτηση $f : \{0,1\}^n \to \{0,1\}$ που ανήκει στην κλάση AC^0. Για οποιοδήποτε $\epsilon \in (0,1)$, υπάρχει πολυώνυμο με βαθμό πολυλογαριθμικής τάξης, το οποίο ταυτίζεται με την f σε τουλάχιστον $(1-\epsilon)\cdot 2^n$ σημεία του $\{0,1\}^n$.

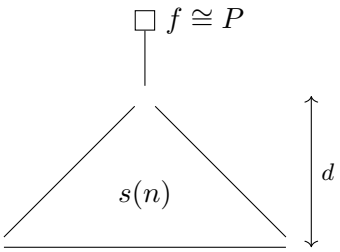
Απόδειξη.
Έστω $s(n)$ το πολυωνυμικής τάξης μέγεθος του κυκλώματος που εκφράζει την f και d το βάθος του. Κάθε πύλη του κυκλώματος της f, την προσεγγίζουμε με πολυώνυμα που παράγονται από την προηγούμενη κατασκευή (Πρόταση 3.2). Η σύθεσή τους, σύμφωνα με τη δομή του κυκλώματος, μας δίνει ένα πολυώνυμο που προσεγγίζει την f (βλ. Σχήμα 3.2).

Για να έχουμε συνολική πιθανότητα σφάλματος το πολύ ϵ, απαιτούμε την αντίστοιχη πιθανότητα για κάθε πύλη να είναι $\frac{\epsilon}{s(n)}$. Για να εκτιμήσουμε τον βαθμό του συνολικού πολυωνύμου, αρχικά εξετάζουμε τις πύλες του δεύτερου επιπέδου. Κάθε



$$P_{k+1,1} = \prod_{i=0}^{\mathcal{O}(\log s(n))} \left(1 - \sum_{j \in S_i} (1 - P_{1j})\right)$$

(α΄)



$$\deg P = \mathcal{O}\left(\log\left(\tfrac{s}{\epsilon}\right) \log^d(s)\right)$$

(β΄)

Μια ενδιάμεση πύλη δέχεται είσοδο από το πολύ $\mathcal{O}(s(n))$ πύλες του χαμηλότερου επιπέδου. Αν $f_{k+1,1}$ είναι η λογική συνάρτηση που υπολογίζει το υποκύκλωμα του σχήματος στα αριστερά, τότε το πολυώνυμο προσέγγισης της $f_{k+1,1}$ είναι το $P_{k+1,1}$ το οποίο περιέχει το γινόμενο –το πολύ όλων– των πολυωνύμων προσέγγισης του χαμηλότερου επιπέδου. Αν P είναι το πολυώνυμο προσέγγισης, με πιθανότητα σφάλματος ϵ, της f που υπολογίζεται από το συνολικό κύκλωμα, πολυωνυμικού μεγέθους, $s(n)$, και σταθερά φραγμένου βάθους d, τότε ο βαθμός του P είναι πολυλογαριθμικός ως προς n.

Σχήμα 3.2: Ο βαθμός του πολυωνύμου προσέγγισης της f είναι πολυλογαριθμικός.

τέτοια πύλη, προσεγγίζεται από ένα πολυώνυμο P_{21}, όπου πρώτος δείκτης αναφέρεται στο επίπεδο της πύλης και ο δεύτερος είναι ένας αύξων αριθμός. Αν η πύλη είναι *OR*, το P_{21} έχει μορφή,

$$P_{21} = 1 - \prod_{i=0}^{\mathcal{O}(\log(s(n)))} \left(1 - \sum_{j \in S_j} P_{1j}\right)$$

Αν η πύλη είναι AND, η μορφή του είναι ανάλογη:

$$P_{21} = \prod_{i=0}^{\mathcal{O}(\log(s(n)))} \left(1 - \sum_{j \in S_j} (1 - P_{1j})\right)$$

Σε κάθε περίπτωση, το πλήθος των πυλών από τις οποίες λαμβάνει είσοδο η πύλη που εξετάζουμε είναι το πολύ όσο το μέγεθος του κυκλώματος, $s(n)$· οπότε το πλήθος των παραγόντων στο γινόμενο είναι $\mathcal{O}(\log s(n))$. Ο βαθμός αυτού του πολυωνύμου είναι όσο ο μέγιστος βαθμός των P_{1j} πολλαπλασιασμένος επί $\mathcal{O}(\log s(n))$. Δηλαδή,

$$\deg P_{21} = \mathcal{O}(\log s(n)) \times \mathcal{O}\left(\log \frac{s(n)}{\epsilon} \log n\right) = \mathcal{O}\left(\log^2 s(n)\right)$$

Συνεχίζοντας ακριβώς με τον ίδιο τρόπο μέχρι το τελευταίο επίπεδο, προκύπτει ότι ο βαθμός του πολυωνύμου, P, που προσεγγίζει την f με πιθανότητα σφάλματος το πολύ ϵ είναι,

$$\deg P = \mathcal{O}\left(\log\left(\frac{s}{\epsilon}\right)\log^d(s)\right)$$

Το μέγεθος του κυκλώματος έχουμε υποθέσει ότι είναι πολυωνυμικό, οπότε ο βαθμός του P έχει πολυλογαριθμική εξάρτηση από το πλήθος των ανεξάρτητων μεταβλητών εισόδου, n.

Ανακεφαλαιώνοντας, για κάθε λοιπόν λογική συνάρτηση $f \in AC^0$ και για κάθε θετική πιθανότητα ϵ, υπάρχει τυχαίο πολυώνυμο p μικρού βαθμού, τέτοιο ώστε για κάθε $(x_1,\ldots,x_n) \in \{0,1\}^n$, η πιθανότητα να ισχύει $f(x_1,\ldots,x_n) = p(x_1,\ldots,x_n)$ είναι τουλάχιστον $1-\epsilon > 0$. Από αυτό συμπεραίνουμε ότι αναγκαστικά υπάρχει ένα πολυώνυμο το οποίο ταυτίζεται με την f για τουλάχιστον $(1-\epsilon)\cdot 2^n$ στοιχεία του $\{0,1\}^n$. Για να γίνει αυτό σαφές, υποθέτουμε ότι p είναι το τυχαίο πολυώνυμο που παράγεται με την προηγούμενη διαδικασία. Έστω S_p το σύνολο των σημείων για τα οποία $f \equiv p$, και X_i η δείκτρια τυχαία μεταβλητή, η οποία παίρνει την τιμή 1 όταν $f(x_i) = p(x_i)$. Η μέση τιμή της X_i είναι $\mathbb{E}[X_i] = 1-\epsilon$ για κάθε i. Τότε,

$$|S_p| = \sum_{i=1}^{2^n} X_i \Rightarrow$$

$$\mathbb{E}[|S_p|] = \mathbb{E}\left[\sum_{i=1}^{2^n} X_i\right] = \sum_{i=1}^{2^n}\mathbb{E}[X_i] = (1-\epsilon)\cdot 2^n$$

Εφόσον λοιπόν, η μέση τιμή του πλήθους των σημείων στα οποία η f ταυτίζεται με το p είναι $(1-\epsilon)\cdot 2^n$ και $1-\epsilon > 0$, αναγκαστικά υπάρχει μη τυχαία επιλογή πολυωνύμου το οποίο ταυτίζεται με την f σε όλα τα στοιχεία ενός συνόλου με πληθάριθμο τουλάχιστον $(1-\epsilon)\cdot 2^n$. Δηλαδή, υπό αυτή την έννοια, $f(x) = p(x)$ σχεδόν για κάθε $x \in \{0,1\}^n$. Σημειώνουμε εδώ, ότι αυτή η επιχειρηματολογία συνιστά εφαρμογή της Πιθανοθεωρητικής Μεθόδου με την εκμετάλλευση της γραμμικότητας της μέσης τιμής.

□ (Πρόταση 3.4)

Προχωρώντας στο δεύτερο στάδιο της απόδειξης, υπενθυμίζουμε ότι θέλουμε να αποδείξουμε ότι οι συναρτήσεις ισοτιμίας δεν προσεγγίζονται από πολυώνυμα λογαριθμικού βαθμού. Θα αποδείξουμε ότι τέτοια πολυώνυμα δεν μπορούν να έχουν βαθμό μέχρι $\sqrt{n}/2$, καταλήγοντας έτσι στο συμπέρασμα ότι οι συναρτήσεις ισοτιμίας δεν ανήκουν στην κλάση AC^0.

Για τη συνέχεια, είναι καλύτερο να χρησιμοποιήσουμε μια διαφορετική αναπαράσταση για τις λογικές συναρτήσεις, όπου το -1 αντιστοιχεί στην τιμή *αλήθειας* (true) και το $+1$ στην τιμή *ψεύδους* (false). Η απεικόνιση που συνδέει τις δύο αναπαραστάσεις είναι, $\phi : \{\pm 1\} \to \{0,1\}, \phi(x) = \frac{1-x}{2}$. Σε αυτό το πλαίσιο, το νέο πολυώνυμο

προσέγγισης γίνεται,

$$q : \{\pm 1\}^n \to \{\pm 1\},$$
$$q(y_1, \ldots, y_n) = \phi^{-1}(p(\phi(y_1), \ldots, \phi(y_n))) =$$
$$1 - 2p\left(\frac{1-y_1}{2}, \ldots, \frac{1-y_n}{2}\right)$$

Το πολυώνυμο αυτό έχει τον ίδιο βαθμό με το p και προσεγγίζει τη συνάρτηση ισοτιμίας. Αυτό ισχύει γιατί

$$\phi^{-1}(\pi_n(\phi(y_1), \ldots, \phi(y_n))) =$$
$$1 - 2\left(\sum_{i=1}^{n} \frac{1-y_i}{2} \mod 2\right) = 1 - 2\left(\frac{1}{2}\sum_{i=1}^{n}(1-y_i) \mod 2\right)$$

Υπενθυμίζουμε ότι $\pi_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \mod 2$.
Το $1 - y_i$ έχει τιμή ή 0 ή 2. Επομένως, το $\sum_{i=1}^{n}(1-y_i)$ ισούται με $2k$, όπου k είναι το πλήθος των y_i που ισούνται με -1. Οπότε,

$$\phi^{-1}(\pi_n(\phi(y_1), \ldots, \phi(y_n))) = \begin{cases} 0, \text{ όταν } k \text{ άρτιος} \\ 1, \text{ όταν } k \text{ περιττός} \end{cases}$$

Επίσης, η νέα αναπαράσταση της συνάρτησης ισοτιμίας είναι,

$$\pi_n : \{\pm 1\}^n \to \{-1, +1\}, \pi_n(y_1, \ldots, y_n) = \prod_{i=1}^{n} y_i$$

Σημειώνουμε εδώ ότι, χωρίς βλάβη της διαδικασίας, για να μην περιπλακεί ο συμβολισμός, γράφουμε π_n για τη συνάρτηση ισοτιμίας στον χώρο $\{\pm\}^n$.

Πρόταση 3.5. *Δεν υπάρχει πολυώνυμο βαθμού $\sqrt{n}/2$ το οποίο να προσεγγίζει τη συνάρτηση ισοτιμίας. Δηλαδή, για $\epsilon > 0$, δεν υπάρχει τέτοιο πολυώνυμο το οποίο να ταυτίζεται με την π_n για τουλάχιστον $(1-\epsilon)\cdot 2^n$ σημεία του $\{-1, +1\}^n$.*

Απόδειξη.
Έστω ότι υπάρχει πολυώνυμο q, βαθμού $\sqrt{n}/2$, το οποίο ταυτίζεται με την π_n για κάθε σημείο ενός συνόλου $S \subset \{\pm 1\}^n$ με $|S| \geq (1-\epsilon)\cdot 2^n$.

Τα στοιχεία του S μπορούμε να τα συμβολίσουμε ως πίνακες διάστασης $n \times |S|$ με μηδενικά σε όλες τις θέσεις εκτός από μία στήλη –διαφορετική για κάθε στοιχείο– που θα έχει τιμές ± 1. Για παράδειγμα, αν $s_i = (+1, -1, \ldots, +1, -1,)$ είναι το $i-$στό στοιχείο του S, τότε αυτό μπορεί να εκφραστεί ως πίνακας μηδενικών στηλών, πλην της $i-$στης, στη μορφή $(0, 0, \ldots, 0, s_i^T, 0, \ldots, 0)$, δηλαδή

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & +1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 & +1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & -1 & 0 & \ldots & 0 \end{bmatrix}_{n \times |S|}$$

Με αυτόν τον τρόπο, το σύνολο $L(S) = \langle S \rangle$ είναι γραμμικός χώρος πάνω από το $\mathbb{R}$ με πράξεις, την συνηθισμένη πρόσθεση πινάκων και τον συνηθισμένο βαθμωτό πολλαπλασιασμό αριθμού με πίνακα. Το S είναι προφανώς γραμμικά ανεξάρτητο και άρα είναι βάση του $L(S)$. Επομένως, $\dim L(S) = |S|$.

Για να εκμεταλλευτούμε τις αλγεβρικές ιδιότητες των πολυωνύμων θέλουμε να αντιπαραβάλλουμε τον $L(S)$ με κάποιον υπόχωρο των πολυωνύμων. Παρατηρούμε ότι στο πολυώνυμο q, ο εκθέτης κάθε μεταβλητής είναι το πολύ 1. Αυτό ισχύει γιατί οι τιμές των μεταβλητών είναι ± 1 και άρα, αν μία μεταβλητή Y έχει εκθέτη n, τότε αν ο n είναι άρτιος, $Y^n \equiv 1$, αλλιώς, $Y^n = Y \cdot Y^{n-1} = Y$. Επομένως, μας ενδιαφέρει ο χώρος των πολυγραμμικών πολυωνύμων.

Έστω λοιπόν, $\mathcal{POL} \subset \mathbb{R}[Y_1, \ldots, Y_n]$, το σύνολο των πολυγραμμικών πολυωνύμων βαθμού $(n + \sqrt{n})/2$ με πραγματικούς συντελεστές, n μεταβλητών οι οποίες παίρνουν τιμές ± 1. Ο $\mathcal{POL}$ είναι γραμμικός χώρος υπέρ το $\mathbb{R}$ με πράξεις, τη συνηθισμένη πρόσθεση πολυωνύμων, η οποία σίγουρα δεν αυξάνει τον βαθμό, και τον συνηθισμένο βαθμωτό πολλαπλασιασμό πολυωνύμων με πραγματικούς αριθμούς. Κάθε στοιχείο του $\mathcal{POL}$ εκφράζεται ως γραμμικός συνδυασμός των μονωνύμων $\prod_{i \in T} Y_i$ όπου T είναι όλα τα υποσύνολα του $\{1, \ldots, n\}$ με $|T| \leq (n + \sqrt{n})/2$. Τα μονώνυμα αυτά είναι γραμμικώς ανεξάρτητα, οπότε η διάσταση του χώρου είναι

$$\dim \mathcal{POL} = \sum_{i=1}^{(n+\sqrt{n})/2} \binom{n}{i}$$

Παρατηρούμε, ότι για το παραπάνω άθροισμα ισχύει το εξής,

$$2^n = \sum_{i=0}^{n} \binom{n}{i} > \sum_{i=0}^{\frac{n+\sqrt{n}}{2}} \binom{n}{i}$$

Αποδεικνύουμε, τώρα, το ακόλουθο Λήμμα το οποίο θα χρησιμοποιήσουμε αργότερα.

Λήμμα 3.6. *Υπάρχει σταθερό $\epsilon \in (0,1)$, ανεξάρτητο του $n \in \mathbb{N}$, τέτοιο ώστε*

$$\dim \mathcal{POL} < (1 - \epsilon) \cdot 2^n$$

Απόδειξη.
Παρατηρούμε ότι,

$$\begin{aligned}
\sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} &= \sum_{i=0}^{n/2} \binom{n}{i} + \sum_{i=\frac{n}{2}+1}^{(n+\sqrt{n})/2} \binom{n}{i} \\
&\leq \sum_{i=0}^{n/2} \binom{n}{i} + \binom{n}{n/2} \sum_{i=\frac{n}{2}+1} 1 \\
&= \frac{1}{2} 2^n + \binom{n}{n/2} \frac{\sqrt{n}}{2}
\end{aligned}$$

Από την προσέγγιση του Stirling, ξέρουμε ότι ασυμπτωτικά το $n!$ είναι πολύ κοντά στην ποσότητα $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$. Επομένως,

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \approx \frac{\sqrt{2\pi 2n}(2n/e)^{2n}}{\left(\sqrt{2\pi n}\,(n/e)^n\right)^2} = \frac{2^{2n}}{\sqrt{\pi n}}$$

Άρα,

$$\sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} \leq \frac{1}{2}2^n + \frac{\sqrt{n}}{2}\frac{2^n}{\sqrt{\pi n/2}} = \left(\frac{1}{2} + \frac{1}{\sqrt{2\pi}}\right)2^n$$

Η ποσότητα $\frac{1}{2} + \frac{1}{\sqrt{2\pi}}$ είναι μικρότερη της μονάδας, επομένως υπάρχει αριθμός $\epsilon \in (0,1)$, ώστε

$$\sum_{i=0}^{(n+\sqrt{n})/2} \binom{n}{i} < (1-\epsilon)\cdot 2^n$$

□ (Λήμμα 3.6)

Μπορούμε να θεωρήσουμε ότι το ϵ που υποθέσαμε στην αρχή της απόδειξης είναι ακριβώς το ϵ του Λήμματος 3.6.

Θα δείξουμε ότι ο $L(S)$ μπορεί να εμφυτευτεί στον $\mathcal{POL}$ μέσω ενός γραμμικού ομομορφισμού $h : L(S) \to \mathcal{POL}$. Αρκεί να προσδιορίσουμε την απεικόνιση h στα στοιχεία της βάσης. Έστω $s = (s_1, \ldots, s_n)$ ένα στοιχείο της βάσης S, του $L(S)$ και T το σύνολο των θέσεων στο s όπου εμφανίζεται η τιμή -1. Τότε, ορίζουμε την h ως εξής:

$$h(s) = \begin{cases} \prod_{i\in T} s_i, & \text{όταν } |T| \leq n/2 \\ q(s_1,\ldots,s_n)\prod_{i\notin T} s_i, & \text{όταν } |T| > n/2 \end{cases}$$

Στην πρώτη περίπτωση έχουμε $\deg h \leq n/2$. Στη δεύτερη περίπτωση, αφού $|T| > n/2$, τότε το συμπλήρωμά του έχει το πολύ $n/2$ στοιχεία. Ο βαθμός του q, από υπόθεση, είναι $\sqrt{n}/2$, επομένως, σε κάθε περίπτωση $\deg h \leq (n+\sqrt{n})/2$.

Γενικότερα, αν $a = \begin{bmatrix} \pm a_1 & \ldots & \pm a_{|S|} \\ \vdots & \vdots & \vdots \\ \pm a_1 & \ldots & \pm a_{|S|} \end{bmatrix}_{n\times|S|} \in L(S)$, τότε

$$h(a) = \sum_{k=1}^{|S|} \alpha_k h(s_k)$$

όπου s_k είναι τα στοιχεία της βάσης του $L(S)$ (παρατηρήστε ότι τα στοιχεία κάθε στήλης έχουν την ίδια απόλυτη τιμή).

Η απεικόνιση h είναι προφανώς ομομορφισμός. Επίσης είναι καλά ορισμένη, διότι αν $s,t \in S$ και T_s, T_t είναι τα αντίστοιχα σύνολα των θέσεων όπου εμφανίζεται η

τιμή -1 και $h(s) \neq h(t)$, τότε αν και τα δύο πολυώνυμα εμπίπτουν στην πρώτη ή στη δεύτερη περίπτωση της κλαδικής έκφρασης της h, είναι προφανές ότι $s \neq t$ αφού έχουν την τιμή -1 σε διαφορετικές θέσεις λόγω του ότι $T_s \neq T_t$. Αν τώρα το ένα, έστω το $h(s)$, ανήκει στην πρώτη περίπτωση και το $h(t)$ ανήκει στη δεύτερη, και έχοντας υποθέσει ότι το q ταυτίζεται με την π_n για τα στοιχεία του S –δηλαδή, $q(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$ για κάθε $(x_1, \ldots, x_n) \in S$–, τότε

$$h(s) \neq h(t) \Rightarrow \prod_{i \in T_s} Y_i \neq q\left(Y_1, \ldots, Y_n\right) \prod_{i \notin T_t} Y_i \Rightarrow$$

$$\prod_{i \in T_s} Y_i \neq \prod_{i=1}^{n} Y_i \prod_{i \notin T_t} Y_i \Rightarrow \prod_{i \in T_s} Y_i \neq \prod_{i \in T_t} Y_i \Rightarrow$$

$$T_t \neq T_s \Rightarrow t \neq s$$

Τώρα, παρατηρούμε ότι τα στοιχεία $h(s), s \in S$ είναι γραμμικώς ανεξάρτητα και το πλήθος τους είναι, από την αρχική μας υπόθεση, $|S| \geq (1-\epsilon) \cdot 2^n$. Επομένως, από το Λήμμα 3.6, τελικά έχουμε,

$$(1-\epsilon) \cdot 2^n \leq \dim L(S) \leq \dim \mathcal{POL} < (1-\epsilon) \cdot 2^n$$

Άτοπο, άρα δεν υπάρχει πολυώνυμο $q \in \mathcal{POL}$ το οποίο να ταυτίζεται με τη συνάρτηση ισοτιμίας, π_n, σχεδόν για κάθε σημείο του $\{\pm 1\}^n$.

□ (Πρόταση 3.5)

Από την πρόταση αυτή, είναι άμεσο το συμπέρασμα ότι οι συναρτήσεις ισοτιμίας είναι αδύνατο να ανήκουν στην κλάση AC^0.

□ (Θεώρημα 3.1)

Κλείνουμε το κεφάλαιο αυτό με τον προσδιορισμό του βελτιωμένου κάτω φράγματος στο βάθος του κυκλώματος που απαιτείται για τον υπολογισμό συναρτήσεων ισοτιμίας.

Πόρισμα 3.7. *Έστω $f : \{0,1\}^n \to \{0,1\}$ λογική συνάρτηση που εκφράζεται από κύκλωμα πολυωνυμικού μεγέθους με πύλες AND και OR. Τότε, το βάθος d του κυκλώματος έχει τάξη μεγέθους*

$$d = \Omega\left(\frac{\log n}{\log \log n}\right)$$

Απόδειξη.
Έχουμε δει ότι ένα άνω φράγμα στον βαθμό του προσεγγιστικού πολυωνύμου στις συναρτήσεις της κλάσης AC^0 είναι $\mathcal{O}\left(\log\left(s/\epsilon\right) \cdot \log^d\left(s\right)\right)$ όπου d είναι το βάθος του κυκλώματος, s το μέγεθός του και ϵ η πιθανότητα σφάλματος.

Αν θεωρήσουμε το d μια άγνωστη, προς προσδιορισμό, συνάρτηση του n και με δεδομένο το κάτω φράγμα στον βαθμό των πολυωνύμων που μπορούν να προσεγγίσουν τη συνάρτηση ισοτιμίας, έχουμε

$$\log\left(s/\epsilon\right) \cdot \log^d\left(s\right) \geq \sqrt{n}$$

Έχοντας τη γενική υπόθεση ότι το s έχει πολυωνυμικής τάξης εξάρτηση από το n, η λύση ως προς d με όρους τάξεων μεγέθους μας δίνει:

$$d = \Omega\left(\frac{\log n}{\log\log n}\right)$$

το οποίο αποτελεί βελτίωση του κάτω φράγματος που αναδείχθηκε στο προηγούμενο κεφάλαιο στην Πρόταση 2.2.

□ (Πόρισμα3.7)

4 Επίλογος

Συνοψίζοντας, στα προηγούμενα κεφάλαια αναλύθηκαν δύο αποτελέσματα που αφορούν στην οριοθέτηση της υπολογιστικής ικανότητας των λογικών κυκλωμάτων πολυωνυμικού μεγέθους. Αποδεικνύεται ότι τέτοια κυκλώματα είναι αδύνατο να υπολογίσουν συναρτήσεις ισοτιμίας, όταν το βάθος τους είναι φραγμένο. Από την άλλη μεριά, αν ένα κύκλωμα έχει βάθος τουλάχιστον λογαριθμικό –και λίγο μικρότερο–, τότε μπορεί να υπολογίσει συναρτήσεις ισοτιμίας.

Η Πιθανοθεωρητική Μέθοδος παίζει καίριο ρόλο στη ανάπτυξη της επιχειρηματολογίας. Στο πρώτο αποτέλεσμα (Κεφάλαιο 2), η απόδειξη είναι επαγωγική ως προς το βάθος των κυκλωμάτων και έχει αναλυτική οπτική· δηλαδή αξιοποιούνται –ας πούμε– λειτουργικές ιδιότητες των εμπλεκομένων μαθηματικών αντικειμένων. Η βάση της επαγωγής αποδεικνύεται με συνδυαστικό τρόπο, ενώ στο επαγωγικό βήμα, με την τεχνική του τυχαίου περιορισμού αποδεικνύεται η ύπαρξη –μη τυχαίου– κυκλώματος επαγωγικά μικρότερου βάθους με ιδιότητα που είναι αδύνατον να ικανοποιεί, καταλήγοντας έτσι στο επιθυμητό συμπέρασμα.

Στο δεύτερο αποτέλεσμα (Κεφάλαιο 3), η οπτική είναι αλγεβρική· δηλαδή αξιοποιούνται δομικές ιδιότητες των αντικειμένων. Ειδικότερα, αρχικά αποδεικνύεται πιθανοθεωρητικά ότι κάθε συνάρτηση της κλάσης AC^0 σχεδόν ταυτίζεται με κάποιο –μη τυχαίο– πολυώνυμο μικρού βαθμού. Κατόπιν, μέσω μιας ομοιομορφικής απεικόνισης στον χώρο αυτών των πολυωνύμων γίνεται σαφές ότι η συνάρτηση ισοτιμίας δεν μπορεί να εκφραστεί από τέτοια κυκλώματα. Στο τελικό συμπέρασμα προκύπτει και μια μικρή βελτίωση του λογαριθμικού κάτω φράγματος του πρώτου αποτελέσματος κατά έναν παράγοντα $\log \log n$ στον παρονομαστή.

Τα αποτελέσματα αυτά θεωρούνται κομβικά στη μελέτη της πολυπλοκότητας κυκλωμάτων καθώς αποτελούν ουσιαστικά πρόδρομο του Θεωρήματος «Switching Lemma», το οποίο αποδείχτηκε στη διδακτορική διατριβή του Johan Håstad[39] και αποτελεί ένα από τα κορυφαία επιτεύγματα στην περιοχή. Η Πιθανοθεωρητική Μέθοδος έχει καθοριστικό ρόλο και σε αυτό το θεώρημα και γενικότερα διέπει ένα μεγάλο φάσμα της σχετικής έρευνας.

Το Switching Lemma, αποτελεί ουσιαστικά μια γενίκευση της διαδικασίας αντιστροφής (switching) των επιπέδων 1 και 2 που είδαμε στο Κεφάλαιο 2, έτσι ώστε το μέγεθος του κυκλώματος να μην αυξάνεται εκθετικά. Στο πλαίσιο της ορολογίας που κινούμαστε και με απλά λόγια, το Swithcing Lemma λέει ότι αν A είναι ένα *AND-OR* κύκλωμα μεγέθους $k+1$ και μη φραγμένου *fan-in* και A' το κύκλωμα που προκύπτει από τυχαίο περιορισμό πιθανότητας p, τότε η πιθανότητα το A' να μην μπορεί να εκφραστεί ως κύκλωμα *OR-AND* μεγέθους το πολύ $s+1$, φράσσεται άνω από την ποσότητα $(5pk)^s$. Το εντυπωσιακό σε αυτό το θεώρημα είναι, το μη αναμενόμενο γεγονός, ότι το πλήθος των μεταβλητών εισόδου δεν παίζει κανένα ρόλο (που ήταν η βασική ανησυχία και επιδίωξη στην πιθανοθεωρητική κατασκευή στο Κεφάλαιο 2). Χρησιμοποιώντας το Switching Lemma, ο Håstad προσδιόρισε και ένα σχεδόν βέλτιστο κάτω φράγμα στο μέγεθος κυκλωμάτων βάθους k με πύλες *AND*

και OR που μπορούν να υπολογίσουν συναρτήσεις ισοτιμίας και το οποίο είναι,

$$\exp\left(\Omega\left(n^{\frac{1}{k-1}}\right)\right)$$

Να σημειώσουμε εδώ, ότι το Switching Lemma, έχει σημαντική εφαρμογή και πέρα από την ανάλυση κυκλωμάτων, όπως στην γενικότερη ανάλυση λογικών συναρτήσεων στην υπολογιστική μάθηση, στην παραγωγή ψευδοτυχαίων αριθμών.

Η τεχνητή, λοιπόν, τυχαιότητα μοιάζει να είναι ένας βασικός και κρίσιμος άξονας παραγωγής αποδείξεων από την αρχή της θεμελίωσης της θεωρίας πολυπλοκότητας μέχρι και σήμερα· ενίοτε, δε μοιάζει με από μηχανής θεό, όπως στο πρόβλημα των φραγμάτων που μελετάμε

Μια άλλη εκδοχή της σχέσης ανάμεσα στην Πιθανοθεωρητική Μέθοδο, τη Θεωρία Πολυπλοκότητας και την ανάγκη προσδιορισμού κάτω φραγμάτων στην Ανάλυση Λογικών Κυκλωμάτων αφορά στο πρόβλημα του προσδιορισμού της σχέσης των κλάσεων P και BPP. Η τεχνική που εμπλέκεται σε αυτό ονομάζεται Απαλοιφή Τυχαιότητας (Derandomization). Η κλάση BPP[7] περιέχει προβλήματα που λύνονται από Τυχαιοποιημένες Μηχανές Turing σε πολυωνυμικό χρόνο με φραγμένη πιθανότητα σφάλματος. Προφανώς ισχύει $P \subseteq BPP$ και είναι φυσιολογικό να υποθέσει κανείς ότι $P \neq BPP$. Όμως, με δεδομένες κάποιες πολύ εύλογες και μάλλον ασθενείς υποθέσεις, αποδεικνύεται ότι κάθε πιθανοθεωρητικός αλγόριθμος μπορεί να μετατραπεί σε ντετερμινιστικό αλγόριθμο με κόστος χρόνου, το πολύ πολυωνυμικό. Αυτό πρακτικά σημαίνει ότι οι κλάσεις BPP και P ταυτίζονται. Όμως, αποδεικνύεται επίσης, ότι η διαδικασία αποτυχαιοποίησης προϋποθέτει την απόδειξη κάτω φραγμάτων λογικών κυκλωμάτων [40]. Οπότε το ότι $P = BPP$ παραμένει σήμερα εικασία.

Με άλλα λόγια, στο πεδίο που μελετάμε, η Ανάλυση Κυκλωμάτων και η Πιθανοθεωρητική Μέθοδος φαίνεται να έχουν πολύ ισχυρή διαπλοκή με την γενικότερη Θεωρία Πολυπλοκότητας. Θα μπορούσε μάλιστα κάποιος να πει ότι, αν και η εισαγωγή τυχαιότητας μοιάζει να είναι εργαλειακού χαρακτήρα, υπάρχει μια θεμελιώδης δομική σχέση με την πιθανοθεωρητική οπτική.

Κλείνοντας, σημειώνουμε ότι μέχρι σήμερα η καλύτερα μελετημένη και πιο κατανοητή κλάση προβλημάτων μοιάζει είναι η AC^0, χωρίς όμως να υπάρχει ραγδαία πρόοδος προς ανάλογα επιθυμητά αποτελέσματα σε μεγαλύτερες κλάσεις. Αλλά, σε κάθε περίπτωση, η αναζήτηση της Ιθάκης είναι σημαντικότερη από την ίδια την Ιθάκη [41].

[7] Bounded-error Probabilistic Polynomial-time

Αναφορές

[1] U. Schöning and R.J. Pruim. Gems of Theoretical Computer Science. Springer, 1998.

[2] Sanjeev Arora and Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 2009.

[3] A. M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, s2-42(1):230–265, 01 1937.

[4] John E. Savage. Models of Computation: Exploring the Power of Computing. Addison-Wesley Longman Publishing Co., Inc., USA, 1st edition, 1997.

[5] L. Fortnow. The Golden Ticket: P, NP, and the Search for the Impossible. BusinessPro collection. Princeton University Press, 2013.

[6] Arthur M. Jaffe. The Millennium Grand Challenge in Mathematics. Not. Amer. Math. Soc., 53(6):652–660, 2006.

[7] Ravi B. Boppana and Michael Sipser. The complexity of finite functions. In Jan van Leeuwen, editor, Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity, pages 757–804. Elsevier and MIT Press, 1990.

[8] J. E. Savage. Computational Work and Time on Finite Machines. Journal of the ACM, 19(4):660–674, October 1972.

[9] Nicholas Pippenger and Michael J. Fischer. Relations Among Complexity Measures. Journal of the ACM, 26(2):361–381, April 1979.

[10] U. Schöning and R.J. Pruim. Lower bounds for the parity function. In Gems of Theoretical Computer Science [1], chapter 11 & 12, pages 91–109.

[11] George Boole. Principles of symbolical reasoning. In Investigation of The Laws of Thought On Which Are Founded the Mathematical Theories of Logic and Probabilities, chapter V, page 74. , 1853. Also available from Dover, New York 1958, ISBN 0-486-60028-9.

[12] P.C. Rosenbloom. The Logic of Classes. In The Elements of Mathematical Logic, Dover series in mathematics and physics, chapter I, page 5. Dover Publications, 1950.

[13] C. E. Shannon. The synthesis of two-terminal switching circuits. The Bell System Technical Journal, 28(1):59–98, p.62, Jan 1949.

[14] Juris Hartmanis and Richard Edwin Stearns. On the computational complexity of algorithms. Trans. Amer. Math., pages 285–306, 1965.

[15] Ryan O'Donnell. Analysis of Boolean Functions. Cambridge University Press, USA, 2014.

[16] Stasys Jukna. Boolean Function Complexity: Advances and Frontiers. Springer Publishing Company, Incorporated, 2012.

[17] Joel H. Spencer Noga Alon. The Probabilistic Method. Wiley Series in Discrete Mathematics and Optimization. John Wiley & Sons, 4th edition, 2016.

[18] Miklós Bóna. Who knows what it looks like, but it exists. The probabilistic method. In A Walk Through Combinatorics: An Introduction to Enumeration and Graph Theory Fourth Edition, chapter 15, pages 381–416. World Scientific Publishing Company, 2016.

[19] Noga Alon and Michael Krivelevich. Extremal and probabilistic combinatorics. In The Princeton Companion to Mathematics, chapter IV.19, pages 562–575. Princeton University Press, 2008.

[20] P. Hoffman. The Man Who Loved Only Numbers: The Story of Paul Erdos and the Search for Mathematical Truth. Hyperion Books, 1998.

[21] P. Erdös. On a problem in graph theory. The Mathematical Gazette, 47(361):220–223, 1963.

[22] Joel H. Spencer Noga Alon. Linearity of expectation. In The Probabilistic Method [17], chapter 2, pages 19–30.

[23] Tibor Szele. Kombinatorikai vizsgálatok az irányitott teljes gráffal kapcsolatban. Matematikai és Fizikai Lapok, 50:223–256 (p.243), 1943.

[24] Joel H. Spencer Noga Alon. Alterations. In The Probabilistic Method [17], chapter 3, pages 31–44.

[25] Joel H. Spencer Noga Alon. The Local Lemma. In The Probabilistic Method [17], chapter 5, pages 69–88.

[26] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. Mathematical systems theory, 17(1):13–27, Dec 1984.

[27] M. Ajtai. Σ11-Formulae on finite structures. Annals of Pure and Applied Logic, 24(1):1–48, July 1983.

[28] B.A. Subbotovskaya. Realization of linear functions by formulas using &, ∨, ¯. Doklady Akademii Nauk SSSR, 136(3):553–555, 1961.

[29] Stasys Jukna. The effect of random restrictions. In Boolean Function Complexity: Advances and Frontiers [16], pages 167–170.

[30] G.Szpiro. Bella Abramovna Subbotovskaya and the Jewish People's University. Not. Amer. Math. Soc., 54(10):1326–1330, 2007.

[31] M. Shifman. Remembering Bella Abramovna. In You Failed Your Math Test, Comrade Einstein, pages 208–212. World Scientific Pub, 2005.

[32] O. B. Lupanov. Implementing the algebra of logic functions in terms of bounded depth formulas in the basis of &, $\vee$, $^{-}$. Doklady Akademii Nauk SSSR, 136:1041–1042, 1961.

[33] A. A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. Mathematical notes of the Academy of Sciences of the USSR, 41(4):333–338, April 1987. tex.day: 01.

[34] R. Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, STOC '87, pages 77–82, New York, NY, USA, 1987. ACM. event-place: New York, New York, USA.

[35] R. Beigel. The polynomial method in circuit complexity. In [1993] Proceedings of the Eigth Annual Structure in Complexity Theory Conference, pages 82–95, May 1993.

[36] Richard Ryan Williams. The Polynomial Method in Circuit Complexity Applied to Algorithm Design (Invited Talk). In Venkatesh Raman and S. P. Suresh, editors, 34th International Conference on Foundation of Software Technology and Theoretical Computer Science (FSTTCS 2014), volume 29 of Leibniz International Proceedings in Informatics (LIPIcs), pages 47–60, Dagstuhl, Germany, 2014. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[37] L. G. Valiant and V. V. Vazirani. NP is as Easy as Detecting Unique Solutions. Theoretical Computer Science, 47:85–93, January 1986.

[38] James Aspnes, Richard Beigel, Merrick Furst, and Steven Rudich. The expressive power of voting polynomials. Combinatorica, 14(2):1–14, 1994.

[39] Johan Håstad. Computational Limitations of Small-Depth Circuits. MIT Press, Cambridge, MA, USA, 1987.

[40] Sanjeev Arora and Boaz Barak. Derandomization. In Computational Complexity: A Modern Approach [2], chapter 20, pages 402–420.

[41] Κωνσταντίνος Καβάφης. Ιθάκη. «Γράμματα», Αλεξάνδρεια Αιγύπτου, 1911.