# Κεφάλαιο 34

# Μη-ομοιόμορφες οικογένειες κυκλωμάτων

## 34.1 Μη-Ομοιόμορφες Οικογένειες Κυκλωμάτων

Στην ενότητα 28.3, μελετήσαμε ομοιόμορφες οικογένειες κυκλωμάτων, και τις ιεραρχίες που δημιουργούν, αν επιβάλουμε περιορισμούς στα μέτρα πολυπλοκότητας που ορίσαμε σε κυκλώματα (μέγεθος, βάθος κλπ). Μπορούμε επίσης να θεωρήσουμε μη-ομοιόμορφες οικογένειες κυκλωμάτων, για τις οποίες *δεν* υπάρχει αλγόριθμος κατασκευής του $C_n$ δεδομένου του $n$.

**Ορισμός 1** *Έστω $T : \mathbb{N} \to \mathbb{N}$ μία συνάρτηση πολυπλοκότητας (constructible). Η γλώσσα $L$ ανήκει στην κλάση $\mathbf{SIZE}(T(n))$, αν υπάρχει μία οικογένεια κυκλωμάτων $\{C_n\}_{n\in\mathbb{N}}$, τέτοια ώστε για κάθε $n \in \mathbb{N}$, $|C_n| \leq T(n)$ (όπου $|C_n|$ το μέγεθος του $C_n$), και για κάθε $x \in \{0,1\}^n$:*

$$x \in L \Leftrightarrow C_n(x) = 1$$

*Επίσης, ορίζουμε ως $\mathbf{P}_{/\mathbf{poly}}$ την κλάση των γλωσσών που αποφασίζονται από οικογένειες κυκλωμάτων πολυωνυμικού μεγέθους, δηλαδή:*

$$\mathbf{P}_{/\mathbf{poly}} = \bigcup_{c\in\mathbb{N}} \mathbf{SIZE}(n^c)$$

Για τις κλάσεις $\mathbf{SIZE}(T(n))$ ισχύουν θεωρήματα ιεραρχίας, παρόμοια με τα αυτά των ντετερμινιστικών κλάσεων πολυπλοκότητας. Λόγω της 'πεπερασμένης' φύσης του μοντέλου (κάθε κύκλωμα έχει πεπερασμένο αριθμό δυνατών εισόδων), οι αποδείξεις τέτοιων αποτελεσμάτων δεν χρειάζονται διαγωνιοποίηση, αρκούν απλά μετρητικά επιχειρήματα, και επίσης δεν δημιουργούνται τα

προβλήματα μη-αποκρισιμότητας που επάγονται από το Θεώρημα Rice για τις TM, οπότε υπάρχει η δυνατότητα ύπαρξης αλγορίθμων ανάλυσης κυκλωμάτων, δηλαδή αλγορίθμων που δέχονται την κωδικοποίηση ενός κυκλώματος ως είσοδο, και παράγουν μια μη-τετριμμένη ανάλυσή του.

Επειδή ο υπολογισμός κάθε TM που αποφασίζει μία γλώσσα στην κλάση $\mathbf{P}$, με μία είσοδο $x$, μπορεί να κωδικοποιηθεί ως ένα κύκλωμα πολυωνυμικού μεγέθους:

**Θεώρημα 1** $\mathbf{P} \subseteq \mathbf{P_{/poly}}$.

Όμως, κάθε εναδική (unary) γλώσσα ανήκει στην κλάση $\mathbf{P_{/poly}}$ (*άσκηση*). Ας θεωρήσουμε την σχετική με το Halting Problem γλώσσα $U_H$:

$$U_H = \{1^n \mid \text{το } n \text{ κωδικοποιεί ένα ζεύγος } (M, x) \text{ τέτοιο ώστε } M(x)\downarrow\}$$

Η γλώσσα $U_H$ προφανώς ανήκει στην $\mathbf{P_{/poly}}$, αλλά δεν είναι αποφασίσιμη. Έτσι καταλήγουμε στην γνησιότητα του εγκλεισμού:

**Θεώρημα 2** $\mathbf{P} \subsetneq \mathbf{P_{/poly}}$

Παραθέτουμε μερικά άλλα βασικά αποτελέσματα που αφορούν την $\mathbf{P_{/poly}}$:

**Θεώρημα 3 (Karp-Lipton)** *Αν* $\mathbf{NP} \subseteq \mathbf{P_{/poly}}$, *τότε* $\mathbf{PH} = \Sigma_2^p$

**Θεώρημα 4 (Meyer)** *Αν* $\mathbf{EXP} \subseteq \mathbf{P_{/poly}}$, *τότε* $\mathbf{EXP} = \Sigma_2^p$

**Θεώρημα 5** $\mathbf{BPP} \subsetneq \mathbf{P_{/poly}}$

### 34.1.1 Μηχανές Turing με Συμβουλή (Advice)

Μπορούμε να συσχετίσουμε τις μη-ομοιόμορφες οικογένειες κυκλωμάτων με το (ομοιόμορφο) μοντέλο της Μηχανής Turing προσθέτοντας 'συμβουλή', δηλαδή επιπλέον bits που παρέχονται στην μηχανή, τα οποία εξαρτώνται μόνο από το μήκος της εισόδου.

**Ορισμός 2** *Έστω* $T, a : \mathbb{N} \to \mathbb{N}$ *συναρτήσεις πολυπλοκότητας (constructible). Η κλάση των γλωσσών που αποφασίζονται από DTM που χρειάζονται χρόνο το πολύ* $T(n)$ *και συμβουλή* $a(n)$ *συμβολίζεται με* $\mathbf{DTIME}(T(n)/a(n))$. *Μία γλώσσα* $L$ *ανήκει στην* $\mathbf{DTIME}(T(n)/a(n))$ *αν υπάρχει μια οικογένεια* $\{\beta_n\}_{n\in\mathbb{N}}$, $\beta_n \in \{0,1\}^{a(n)}$ *για κάθε* $n \in \mathbb{N}$, *και μία DTM* $M$ *τέτοια ώστε για κάθε* $x \in \{0,1\}^n$:

$$x \in L \Leftrightarrow M(x, \beta_n) = 1$$

*και η* $M$ *χρειάζεται χρόνο* $O(T(n))$.

Χρησιμοποιώντας το μοντέλο των Μηχανών Turing με συμβουλή, μπορούμε να χαρακτηρίσουμε την $\mathbf{P}_{/\mathbf{poly}}$ ως εξής:

**Θεώρημα 6** $\mathbf{P}_{/\mathbf{poly}} = \bigcup_{c,d\in\mathbb{N}} \mathbf{DTIME}(n^c/n^d)$

## 34.2 Κάτω Φράγματα

Η κλάση $\mathbf{P}_{/\mathbf{poly}}$ σχετίζεται άμεσα με το πρόβλημα $\mathbf{P}$ *vs* $\mathbf{NP}$, αφού αν βρεθεί μία γλώσσα στην κλάση $\mathbf{NP}$ που δεν ανήκει στην $\mathbf{P}_{/\mathbf{poly}}$, τότε $\mathbf{P} \neq \mathbf{NP}$. Αυτή η θεώρηση οδήγησε σε μια μεγάλη προσπάθεια εύρεσης μιας τέτοιας γλώσσας, και την ενδελεχή μελέτη υποκλάσεων της $\mathbf{P}_{/\mathbf{poly}}$. Παράδειγμα τέτοιας κλάσης είναι η $\mathbf{ACC}^0[m]$, που είναι το μη-ομοιόμορφο ανάλογο της $\mathbf{AC}^0$, με επιπλέον χρήση MOD- μετρητικών πυλών (πύλες που λαμβάνουν την τιμή 0 αν το άθροισμα όλων των εισόδων τους, $x_i$, ισούται με 0 ($\sum x_i \mod m = 0$).

Αναπτύχθηκαν πολλές τεχνικές εύρεσης κάτω φραγμάτων γι΄ αυτές τις υποκλάσεις, με πιο σημαντικές την *μέθοδο των τυχαίων περιορισμών* (random restriction method) και την πολυωνυμική μέθοδο (polynomial method), τις οποίες θα αναλύσουμε παρακάτω.

### 34.2.1 Μέθοδος των Τυχαίων Περιορισμών

Η βασική ιδέα της μεθόδου είναι να μειώσουμε τον αριθμό εισόδων του κυκλώματος, αντικαθιστώντας μερικές από τις εισόδους με σταθερές. Η αντικατάσταση αυτή γίνεται πιθανοτικά, βάσει κάποιας κατανομής πιθανότητας. Τότε, μπορεί να αποδειχθεί ότι η συνάρτηση $f$, που υπολογίζεται από το κύκλωμα, με μεγάλη πιθανότητα θα είναι σταθερή.

Υπάρχουν όμως συναρτήσεις των οποίων η τιμή αλλάζει κάθε φορά που κάποια μεταβλητή τους αλλάζει. Ένα κλασσικό παράδειγμα είναι η συνάρτηση $PARITY : \{0,1\}^n \to \{0,1\}$, όπου $PARITY(x_1,\ldots,x_n) = \sum_{i=1}^{n} x_i \mod 2$. Τέτοιες συναρτήσεις δεν θα μπορούν να υπολογιστούν από κυκλώματα σταθερού βάθους και πολυωνυμικού μεγέθους. Το επόμενο κάτω φράγμα οφείλεται στους Furst, Saxe, Sipser, Ajtai.

**Θεώρημα 7** $PARITY \notin AC^0$.

Ο Håstad βελτίωσε το παραπάνω αποτέλεσμα δείχνοντας ότι κυκλώματα βάθους $d$ χρειάζονται $2^{\Omega(n^{1/(d-1)})}$ μέγεθος για να υπολογίσουν την συνάρτηση $PARITY$.

### 34.2.2 Πολυωνυμική Μέθοδος

Αυτή η μέθοδος αναπαριστά τα κυκλώματα με πολυώνυμα χαμηλού βαθμού. Για παράδειγμα, μια πύλη $AND$ μπορεί να αντικατασταθεί από το πολυώνυμο $p(x_1, x_2) = x_1x_2$, και μια πύλη $OR$ από το $p(x_1, x_2) = x_1 + x_2 - x_1x_2$.

Οι τεχνικές που χρησιμοποιούν αυτή την μέθοδο αναπαριστούν τα κυκλώματα με πολυώνυμα *πιθανοτικά*, έτσι ώστε το πολυώνυμο (που επιλέγεται πάλι βάσει μιας κατανομής πιθανότητας) να αναπαριστά το κύκλωμα με μεγάλη πιθανότητα.

Οι Razborov και Smolensky έδειξαν ότι κάθε κύκλωμα σταθερού βάθους που υπολογίζει μια γλώσσα στην κλάση $ACC^0[m]$ μπορεί να αναπαρασταθεί πιθανοτικά από ένα πολυώνυμο χαμηλού βαθμού στο σώμα $\mathbb{F}_2$. Από την άλλη, έδειξαν ότι υπάρχουν συναρτήσεις οι οποίες *δεν* μπορούν να αναπαρασταθούν με πολυώνυμα χαμηλού βαθμού με καλή πιθανότητα, οπότε δεν μπορούν να υπολογιστούν από κυκλώματα της κλάσης.

**Θεώρημα 8 (Razborov-Smolensky)** *Για διαφορετικούς πρώτους αριθμούς $p$ και $q$, η συνάρτηση $MOD_p$ δεν ανήκει στην $\mathbf{ACC}^0[q]$.*

Ένα άλλο παράδειγμα είναι ο περιορισμός των οικογενειών κυκλωμάτων σε *μονότονα* κυκλώματα, δηλαδή κυκλώματα που δεν έχουν πύλες $NOT$ ($inverters$). Για μονότονες οικογένειες κυκλωμάτων, ισχύει το εξής κάτω φράγμα για το πρόβλημα της κλίκας:

**Θεώρημα 9 (Razborov-Andreev-Alon-Boppana)** *Υπάρχει μία σταθερά $\varepsilon > 0$, τέτοια ώστε για κάθε $k \leq n^{1/4}$ το πρόβλημα της $k$-κλίκας δεν υπολογίζεται από μονότονα κυκλώματα μεγέθους μικρότερου από $2^{\varepsilon\sqrt{k}}$.*

Σχετικά πρόσφατα αποδείχθηκε ότι κάτω φράγματα για την κλάση **NEXP** σχετίζονται στενά με το πρόβλημα ικανοποιησιμότητας κυκλώματος: Δοθέντος κυκλώματος $C_n$, υπάρχει $x \in \{0,1\}^n$ τέτοιο ώστε $C_n(x) = 1$;

Ο προφανής τρόπος να λύσουμε αυτό το πρόβλημα (να δοκιμάσουμε επαναληπτικά τις $2^n$ πιθανές εισόδους μήκους $n$), στις περισσότερες περιπτώσεις είναι και ο καλύτερος που γνωρίζουμε. Οποιαδήποτε βελτίωση θα οδηγήσει σε κάτω φράγμα για την **NEXP**, όπως φαίνεται και από το ακόλουθο θεώρημα:

**Θεώρημα 10** *Έστω μία υπερπολυωνυμική συνάρτηση $s(n)$. Αν το πρόβλημα ικανοποιησιμότητας κυκλώματος με $n$ εισόδους και μέγεθος $poly(n)$ μπορεί να λυθεί σε χρόνο $2^n \cdot poly(n)/s(n)$, τότε $\mathbf{NEXP} \not\subseteq \mathbf{P}_{/\mathbf{poly}}$.*

Το παραπάνω θεώρημα, σε συνδυαμό με πρόσφατη πρόοδο στο πρόβλημα ικανοποιησιμότητας κυκλώματος για την κλάση $\mathbf{ACC}^0$, οδήγησε στο ακόλουθο αποτέλεσμα:

**Θεώρημα 11**

$$\mathbf{NEXP} \not\subseteq \mathbf{ACC}^0$$

όπου $ACC^0 = \bigcup_{(m_1,...,m_l)} ACC^0[m_1, ..., m_l]$

## 34.3 Κάτω Φράγματα και Αλγόριθμοι

Η παραπάνω θεώρηση καταδεικνύει ότι η ύπαρξη αλγορίθμων επάγει κάτω φράγματα. Πρόσφατα αποτελέσματα δείχνουν ότι και το αντίστροφο είναι δυνατό, δηλαδή τεχνικές για κάτω φράγματα να επάγουν αλγορίθμους. Τα αποτελέσματα αυτά σχετίζονται με τον νεότευκτο κλάδο της Fine-Grained Complexity, στο πλαίσιο του οποίου ο πολυωνυμικός χρόνος, που ταυτίζεται με την αποδοτικότητα στην κλασσική Θεωρία Πολυπλοκότητας, δεν θεωρείται αποδοτικός ανεξαρτήτως του πολυωνύμου. Αντιθέτως, αναζητούνται κάτω φράγματα για συγκεκριμένα πολυώνυμα (π.χ. αν υπάρχει υποτετραγωνικός αλγόριθμος για κάποιο πρόβλημα).

### 34.3.1 Αλγόριθμοι από Κάτω Φράγματα

Μία από τις πρώτες εφαρμογές των κάτω φραγμάτων αφορά το πρόβλημα των Πανζευκτικών Ελαχίστων Διαδρομών (All-Pairs Shortest Paths). Ο κλασσικός αλγόριθμος δυναμικού προγραμματισμού που το επιλύει (Floyd-Warshall) χρειάζεται $O(n^3)$ χρόνο, όπου $n$ το πλήθος των κόμβων του γραφήματος. Χρησιμοποιώντας την πολυωνυμική μέθοδο, μπορούμε να απομονώσουμε επαναλαμβανόμενα υπο-προβλήματα, να τα κωδικοποιήσουμε ως κυκλώματα, και χρησιμοποιώντας τις τεχνικές του θεωρήματος Razborov-Smolensky, να μετατρέψουμε τα κυκλώματα σε πολυώνυμα, τα οποία μπορούν να υπολογιστούν με προηγμένους αριθμητικούς αλγορίθμους.

**Θεώρημα 12** *Το πρόβλημα των Πανζευκτικών Ελαχίστων Διαδρομών επιλύεται σε χρόνο:*

$$\frac{n^3}{2^{\Omega(\sqrt{\log n})}}$$

Ένα άλλο σημαντικό πρόβλημα είναι αυτό των Ορθογώνιων Διανυσμάτων:

**Ορισμός 3** *Δίνονται δύο σύνολα διανυσμάτων $A, B \subseteq \{0,1\}^d$, $|A| = |B| = n$. Υπάρχουν $x \in A$ και $y \in B$ τέτοια ώστε $x \cdot y = 0$;*

Ο απλοϊκός αλγόριθμος έχει πολυπλοκότητα $O(n^2 d)$ (*Άσκηση: Δώστε έναν τέτοιο αλγόριθμο*). Χρησιμοποιώντας ξανά την πολυωνυμική μέθοδο, μπορούμε να επάγουμε καλύτερο αλγόριθμο:

**Ορισμός 4** *Το πρόβλημα των Ορθογώνιων Διανυσμάτων λύνεται σε χρόνο:*

$$n^{2-\frac{1}{O(\log \frac{d}{\log n})}}$$

### 34.3.2 Εικασίες στην Fine-Grained Complexity

Όπως στην κλασσική Θεωρία Πολυπλοκότητας τα περισσότερα αποτελέσματα βασίζονται σε εικασίες (όπως π.χ. ότι δεν υπάρχει πολυωνυμικός αλγόριθμος για το $SAT$), έτσι και στην Fine-Grained Complexity οι οικογένειες αναγωγών που προκύπτουν βασίζονται σε αντίστοιχες εικασίες. Η πιο σημαντική από αυτές είναι η Εκθετική Υπόθεση (Exponential-Time Hypothesis), που διατυπώθηκε από τους Impagliazzo και Paturi το 2001, με σκοπό την μελέτη των εκθετικών αλγορίθμων.

**Ορισμός 5 (Εκθετική Υπόθεση-ETH)** *Υπάρχει $\varepsilon > 0$ τέτοιο ώστε το $3SAT$ να χρειάζεται τουλάχιστον $2^{\varepsilon n}$ χρόνο για να λυθεί, όπου $n$ ο αριθμός των μεταβλητών της φόρμουλας.*

Η παραπάνω υπόθεση ουσιαστικά αιτείται ότι το $3SAT$ απαιτεί τουλάχιστον υποεκθετικό χρόνο επίλυσης. Μια ισχυρότερη παραλλαγή της, η Ισχυρή Εκθετική Υπόθεση, αναφέρεται στην πολυπλοκότητα του $kSAT$:

**Ορισμός 6 (Ισχυρή Εκθετική Υπόθεση-SETH )** *Για κάθε $\varepsilon > 0$ υπάρχει $k \geq 3$ τέτοιο ώστε το $kSAT$ να χρειάζεται τουλάχιστον $2^{(1-\varepsilon)n}$ χρόνο για να λυθεί.*

**Θεώρημα 13** $SETH \Rightarrow ETH.$

Επίσης, η Fine-Grained Complexity εισήγαγε εικασίες για προβλήματα που είναι ήδη στο $P$, όπως αυτό των Ορθογώνιων Διανυσμάτων που είδαμε παραπάνω:

**Ορισμός 7 (Εικασία Ορθογώνιων Διανυσμάτων-OVC )** *Δεν υπάρχει $\varepsilon > 0$ ώστε το πρόβλημα των Ορθογώνιων Διανυσμάτων να μπορεί να λυθεί σε χρόνο $O(n^{2-\varepsilon}poly(d))$.*

**Θεώρημα 14** $SETH \Rightarrow OVC.$

Το παραπάνω θεώρημα είναι αρκετά ενδιαφέρον, αφού συνδέει μια εικασία που αφορά υποεκθετικούς αλγορίθμους με μια που αφορά πολυωνυμικούς. Η εικασία OVC συνδέεται επίσης με πολλά άλλα προβλήματα τετραγωνικού χρόνου, όπως αυτό της Μέγιστης Κοινής Υπακολουθίας (LCS), και γνωρίζουμε ότι αν υπάρξει στο μέλλον υποτετραγωνικός αλγόριθμος για κάποιο από αυτά, η OVC θα καταρριφθεί, όπως και η SETH, λόγω των παραπάνω θεωρημάτων.