Εθνικο Μετσοβειο Πολυτεχνειο

Σχολη Εφαρμοσμενων Μαθηματικων και Φυσικων Επιστημων

Οι Ομάδες Πλεξίδων και εφαρμογές τους στην κρυπτογραφία και τα πολυμερή

Διπλωματικη Εργασια

Μαντοπούλου - Παλούκα Δανάη

Επιβλέπουσα Καθηγήτρια: Λαμπροπούλου Σοφία

Αθήνα, Ιούλιος 2013

Οι Ομάδες Πλεξίδων και εφαρμογές τους στην κρυπτογραφία και τα πολυμερή

Μαντοπούλου - Παλούκα Δανάη

Αθήνα, Ιούλιος 2013

Στην Δάφνη

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την Καθηγήτρια του Τομέα Μαθηματικών της Σχολής Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών του ΕΜΠ κα. Λαμπροπούλου Σοφία για την πολύτιμη καθοδήγησή της, καθώς επίσης και για τον χρόνο που διέθεσε καθ'όλη την διάρκεια εκπόνησης της παρούσας εργασίας.

Θα ήθελα επίσης να ευχαριστήσω την διδάκτορα του ΕΜΠ Παναγιώτου Ελένη, χωρίς την πολύτιμη βοήθεια της οποίας το τελευταίο κομμάτι αυτής της εργασίας δεν θα είχε γραφτεί.

Τέλος εκφράζω τις ευχαριστίες μου στην Τ. ΣΟ. για την ευχάριστη συντροφιά της τις ώρες συγγραφής της εργασίας και σε όλους όσους βοήθησαν με τον τρόπο τους αυτή η εργασία να τελειώσει μερικούς μήνες αργότερα.

Εισαγωγή

Οι ομάδες των πλεξίδων (braid groups) ορίστηκαν το 1925 από τον Emil Artin. Από τότε μελετώνται εκτενώς από τοπολόγους και αλγεβριστές και έχουν οδηγήσει σε πλούσιες θεωρίες με αρκετές προεκτάσεις. Πέρα από την στενή σχέση τους με τις ομάδες μεταθέσεων και με άλγεβρες όπως οι άλγεβρες Hecke, οι ομάδες των πλεξίδων χρησιμοποιούνται ως βασικό εργαλείο για την μελέτη των κόμβων και των κρίκων. Επιπλέον, έχουν ευρύτατο πεδίο εφαρμογών στη χημεία, τη βιολογία και την επιστήμη των υπολογιστών.

Στην παρούσα διπλωματική εργασία ασχολούμαστε με τον ορισμό των ομάδων των πλεξίδων και με την λύση του word problem πάνω σε αυτές. Παρουσιάζουμε δεξιοδικά τις λύσεις που έδωσαν, πρώτα ο Garside και στην συνέχεια ο Dehornoy. Επιπλέον, ακολουθώντας τα βήματα του Dehornoy, αποδεικνύουμε την ύπαρξη μιας ολικής διάταξης στην ομάδα των πλεξίδων. Αυτά παρουσιάζονται στο Κεφάλαια 1 και 2. Στο τρίτο κεφάλαιο αναφερόμαστε σε δύο κρυπτογραφικά πρωτόκολλα που χρησιμοποιούν τις ομάδες των πλεξίδων και πιο συγκεκριμένα την δυσκολία επίλυσης του conjugacy problem πάνω σε αυτές. Κλείνουμε με μια αναφορά σε δυνατές εφαρμογές των ομάδων πλεξίδων στην μελέτη της δομής των πολυμερών.

Introduction

Braid groups, after being explicitly introduced by Emil Artin in 1925, have been extensivly studied by topologists and algebraists, which has led to rich theories with numerus ramifications. Beyond their close relation to permutation groups and algebras, like Hecke algebras, they are beeing used as a useful tool for the study of knots and links. Moreover, they have a wide field of applications like the ones in chemistry, biology or even computer science.

In this dissertation we present the basic definitions of braid group theory and we study the solution of the word problem. We introduce in detail the solutions that first Garside gave, and after the one from Dehoroy. Furthurmore, following Dehornoy's steps, we prove the existance of a linear ordering in the braid group. The above are presented in Chapters 1 and 2. In the third chapter we mention two cryptographic protocols which use braid goups and especially the difficulty of solving the conjugacy problem. Finally, we note a possible application of braid groups in the study of the structure of polymers.

Περιεχόμενα

Κατάλογος Σχημάτων

ΚΕΦΑΛΑΙΟ 1

Βασικές έννοιες και Ορισμοί

Θα ξεκινήσουμε με κάποιους στοιχειώδεις ορισμούς και θεωρήματα από την Θεωρία των Ομάδων όπως αυτοί παρουσιάζονται στο [20] και θα συνεχίσουμε εξετάζοντας πιο συγκεκριμένα την Ομάδα των Πλεξίδων (Braid Group).

1.1 Γενικά

Ορισμός 1.1. Ομάδα $\langle G, * \rangle$ είναι ένα σύνολο G εφοδιασμένο με μια διμελή πράξη $*$, τέτοια ώστε να ικανοποιούνται τα ακόλουθα:

(i) Το σύνολο G να είναι κλειστό ως προς την διμελή πράξη $*$, δηλαδή κάθε διατεταγμένο ζεύγος (a, b) του συνόλου να αντιστοιχίζεται μέσω της διμελούς πράξης σε ένα στοιχείο που να ανήκει επίσης στο σύνολο.

(ii) Η πράξη αυτή να είναι προσεταιριστική (δηλ. $(a * b) * c = a * (b * c), \forall a, b, c \in G$).

(iii) Υπάρχει ένα στοιχείο ε στο G τέτοιο ώστε $\varepsilon * x = x * \varepsilon$, $\forall x \in G$ το στοιχείο αυτό θα καλείται **ταυτοτικό** για την $*$ στο G (**μοναδιαίο** σε πολλαπλασιαστικό συμβολισμό και **μηδενικό** σε προσθετικό).

(iv) Για κάθε στοιχείο $x \in G$, υπάρχει ένα στοιχείο x^{-1} στο G με την ιδιότητα $x * x^{-1} = x^{-1} * x = \varepsilon$. Το στοιχείο x^{-1} θα καλείται **συμμετρικό** του x ως προς την πράξη $*$ (**αντίστροφο** σε πολλαπλασιαστικό συμβολισμό και **αντίθετο** σε προσθετικό).

Θα σημειώσουμε εδώ ότι μία ομάδα δεν είναι απλώς ένα σύνολο G, αλλά σχηματίζεται από δύο οντότητες, το σύνολο G *μαζί* με τη διμελή πράξη $*$. Για λόγους όμως απλότητας στην συνέχεια θα εγκαταλείψουμε τον συμβολισμό

$< G, * >$ και θα αναφερόμαστε στην ομάδα μόνο με το κεφαλαίο γράμμα που συμβολίζει το σύνολο.

Παράδειγμα 1.1. Το σύνολο όλων των μή αρνητικών ακεραίων (συμπεριλαμβανομένου του 0) με πράξη την + *δεν* είναι ομάδα. Υπάρχει το ταυτοτικό στοιχείο για την + που είναι το μηδέν αλλά δεν υπάρχουν τα αντίστροφα.

Παράδειγμα 1.2. Αντίθετα, το σύνολο $\mathbb{Z}$ των ακεραίων με πράξη την +, είναι ομάδα.

Παράδειγμα 1.3. Το σύνολο όλων των πραγματικών συναρτήσεων με πεδίο ορισμού το $\mathbb{R}$, με πράξη την πρόσθεση συναρτήσεων είναι ομάδα.

Ορισμός 1.2. Μία ομάδα G λέγεται **αβελιανή** ή **αντιμεταθετική** αν για κάθε $a,\, b \in\, G$ ισχύει: $a * b = b * a$.

Η ομάδα που θα ασχοληθούμε στην συνέχεια της παρούσας εργασίας *δεν* είναι αβελιανή. Ο αναγνώστης είναι πιθανώς εξοικειωμένος με μή-αντιμετθετικές πράξεις όπως για παράδειγμα ο πολλαπλασιασμός πινάκων, για τους οποίους εν γένει δεν ισχύει ότι $AB = BA$. Τα κρυπτογραφικά πρωτόκολλα που θα παρουσιάσουμε βασίζονται ακριβώς σε αυτό το γεγονός, ότι δηλαδή το conjugacy problem είναι γενικά δύσκολα επιλύσιμο σε μή-αντιμεταθετικές ομάδες.

Θα μιλήσουμε για το conjugacy problem αναλυτικά σε επόμενο κεφάλαιο. Εδω θα πούμε μόνο ότι το συγκεκριμένο πρόβλημα διατυπώνεται και ως εξής: Έστω G μιά ομάδα και έστω $g, h \in G$ βρείτε εάν υπάρχει $x \in G$ τέτοιο ώστε: $x^{-1}gx = h$. Παρατηρούμε εδώ ότι αν η ομάδα είναι αβελιανή τότε: $x^{-1}gx = x^{-1}xg = g$ και η λύση είναι όλη G αν $g = h$ και το κενό σύνολο αν $g \neq h$.

Ορισμός 1.3. Το **κέντρο μιας ομάδας** G είναι το σύνολο όλων των $a \in G$, για τα οποία ισχύει $ax = xa$ για κάθε $x \in G$, δηλαδή το σύνολο όλων των στοιχείων της G που αντιμετατίθονται με κάθε στοιχείο της G.

Εύκολα παρατηρούμε ότι στις αβελιάνες ομάδες το κέντρο ταυτίζεται με ολόκληρη την ομάδα. Ο παραπάνω ορισμός δίνεται διότι στην μελέτη των ομάδων πλεξίδων οδηγούμαστε σε ένα πολύ όμορφο αποτέλεσμα που αφορά το κέντρο της συγκεκριμένης ομάδας, το οποίο θα εξεταστεί σε επόμενο κεφάλαιο.

Παράδειγμα 1.4. Έστω το σύνολο $M_n(\mathbb{R})$ όλων των πινάκων $n \times n$. Το υποσύνολο του, $GL_n(\mathbb{R})$, που αποτελείται από όλους τους αντιστρέψιμους πίνακες με πράξη τον πολλαπλασιασμό, είναι ομάδα και μάλιστα μη-αντιμεταθετική.

Ορισμός 1.4. Αν G είναι μια πεπερασμένη ομάδα, η **τάξη** $|G|$ της G είναι το πλήθος των στοιχείων της G.

Ορισμός 1.5. Αν ένα υποσύνολο H μιας ομάδας G είναι κλειστό ως προς την πράξη της ομάδας και είναι και αυτό ομάδα, τότε το H θα λέμε ότι είναι **υποομάδα** της G. Θα γράφουμε $H \leq G$ για να συμβολίσουμε ότι η H είναι

υποομάδα της G και γράφοντας $H < G$ θα εννοούμε ότι η H είναι **γνήσια** υποομάδα της G, δηλαδή $H \leq G$ αλλά $H \neq G$. . Επίσης παρατηρούμε ότι $\forall\, G$ το μονοσύνολο $\{\varepsilon\}$ είναι υποομάδα, η οποία θα καλείται **τετριμμένη υποομάδα** της G.

Ισοδύναμα:
Ένα υποσύνολο H μιας ομάδας G είναι υποομάδα της G αν και μόνο αν

1. Το σύνολο είναι κλειστό ως προς τη διμελή πράξη της G.
2. Το ταυτοτικό στοιχείο ε της G ανήκει στο H.
3. Για κάθε $a \in H$ ισχύει $a^{-1} \in H$.

Η απόδειξη της παραπάνω ισοδυναμίας είναι σχετικά απλή και βασίζεται στον ορισμό της υποομάδας και στις ιδιότητες που προκύπτουν για το ταυτοτικό στοιχείο και τα αντίστροφα. Ο αναγνώστης που ενδιαφέρεται μπορεί να την βρεί στο [20].

Παράδειγμα 1.5. Έστω $n \in \mathbb{N}$. Ορίζουμε με $\mathbb{Z}_{\boldsymbol{n}}$ την ομάδα, με πράξη την πρόσθεση modulo n, που τα στοιχεία της είναι οι κλάσεις υπολοίπου της διαίρεσης ενός ακεραίου με n.Σε αντίθεση με τις υπόλοιπες ομάδες που δώσαμε προηγούμενως ως παραδείγματα η $\mathbb{Z}_n$ είναι *πεπερασμένης* τάξης και μάλιστα $|\mathbb{Z}_n| = n$.Για να μην υπάρξει περίπτωση σύγχυσης θα συμβολίζουμε τα στοιχεία της ομάδας $\mathbb{Z}_n$ με μία παύλα από πάνω. Έστω η ομάδα $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Μπορούμε εύκολα να παρατηρήσουμε ότι η μόνη γνήσια, μη τετριμμένη υποομάδα της $\mathbb{Z}_4$ είναι η $\{\bar{0}, \bar{2}\}$. Πράγματι έστω το υποσύνολο $\{\bar{0}, \bar{3}\}$. Για το $\bar{3}$ έχουμε: $\bar{3} + \bar{3} = \bar{2}$, άρα δεν είναι κλειστό ως προς την πράξη της πρόσθεσης και άρα δεν είναι υποομάδα.Συνεχίζοντας με το προηγούμενο παράδειγμα έχουμε ότι για $H = \{\bar{0}, \bar{2}\}$, το οποίο είναι όντως κλειστό ως προς την πράξη της πρόσθεσης, περιέχει το ταυτοτικό που είναι το $\bar{0}$ και το αντίστροφο του $\bar{2}$ που είναι ο εαυτός του.

Πρόταση 1.1. *Έστω G μια ομάδα και έστω $a \in G$. Τότε το*

$$H = \{a^n | n \in \mathbb{Z}\}$$

είναι μια υποομάδα της G και μάλιστα είναι η μικρότερη υποοομάδα της G που περιέχει το a, δηλαδή, κάθε υποομάδα που περιέχει το a περιέχει και την H.
*Η υποομάδα H που μόλις ορίσαμε λέγεται **κυκλική υποομάδα** της G που παράγεται από το a και συμβολίζεται με $< \boldsymbol{a} >$*

Απόδειξη. Ελέγχουμε τις συνθήκες του ισοδύναμου του Ορισμού 1.5. Αφού $a^r a^s = a^{r+s}$ για κάθε $r,\ s\ \in \mathbb{Z}$ άρα βλέπουμε ότι το γινόμενο δύο στοιχείων της H ανοίκει πάλι στην H και άρα είναι κλειστό ως προς την πράξη. Επίσης $a^0 = \varepsilon$, άρα $\varepsilon \in H$ και αν $a^r \in H$ τότε $a^{-r} \in H$ και έχουμε $a^r a^{-r} = a^0 = \varepsilon$. Άρα $H \leq G$. □

Ορισμός 1.6. Έστω G μια ομάδα και $a_i \in G$ για $i \in I$. Η μικρότερη υποομάδα της G που περιέχει το $\{a_i | i \in I\}$ λέγεται η υποομάδα που παράγεται από το $\{a_i | i \in I\}$. Αν αυτή η υποομάδα είναι ολόκληρη η G, τότε λέμε ότι το $\{a_i | i \in I\}$ παράγει την G και τα a_i λέγονται **γεννήτορες** της G. Αν υπάρξει πεπερασμένο σύνολο $\{a_i | i \in I\}$ που παράγει την G τότε η G λέγεται **πεπερασμένα παραγόμενη**.

Έστω A οποιοδήποτε (όχι απαραίτητα πεπερασμένο) σύνολο με στοιχεία a_i, $i \in I$. Σκεφτόμαστε το A ως ένα **αλφάβητο** και τα a_i ως τα **γράμματα** του αλφαβήτου. Κάθε σύμβολο της μορφής a_i^n, όπου $n \in \mathbb{Z}$, είναι μια συλλαβή και κάθε πεπερασμένη ακολουθία w από συλλαβές είναι μία **λέξη**. Ορίζουμε την **κενή λέξη** ε, η οποία δεν έχει καμμία συλλαβή.

Υπάρχουν δύο φυσιολογικοί τρόποι απλοποίησης λέξεων:

- Η αντικατάσταση κάθε συλλαβής $a_i^m a_i^n$ απο την a_i^{m+n}.
- Η αντικατάσταση κάθε συλλαβής a_i^0 από την κενή λέξη ε, δηλαδή η την διαγραφή της a_i^0 από την λέξη. Οι παραπάνω τρόποι ονομάζονται **στοιχειώδεις συστολές**

Ορισμός 1.7. Ονομάζουμε **ανηγμένη λέξη** την λέξη στην οποία δεν μπορούμε να εφαρμόσουμε καμμία στοιχειώδη συστολή.

Παράδειγμα 1.6. Έστω $A = \{a_1, a_2, a_3\}$. Η ανηγμένη μορφή της λέξης $a_2^3 a_2^{-1} a_3 a_1^2 a_1^{-7}$ είναι η $a_2^2 a_3 a_1^{-5}$.

Έστω $F[A]$ το σύνολο όλων των ανηγμένων λέξεων που προκύπτουν από ένα αλφάβητο A. Θα δείξουμε ότι στο $F[A]$ ορίζεται δομή ομάδας με έναν πολύ φυσιολογικό τρόπο.

Πράγματι έστω w_1, w_2 στοιχεία του $F[A]$. Ορίζουμε την πράξη $\cdot$ με $w_1 \cdot w_2$ να ορίζεται ως η ανηγμένη μορφή εκείνης της λέξης που προκύπτει αν τοποθετήσουμε την w_2 μετά την w_1. Δηλαδή η λέξη $w_1 w_2$. Είναι προφανές οτι η πράξη αυτή είναι καλά ορισμένη και προσεταιριστική. Επίσης παρατηρούμε ότι αν w μια λέξη τότε αν σχηματίσουμε την w^{-1} γράφοντας με την αντίθετη σειρά τις συλλαβές της w και υψώνοντάς τες την κάθε μία στην -1 τότε η λέξη που θα προκύψει θα είναι επίσης ανηγμένη και θα ισχύει:

$$ww^{-1} = w^{-1}w = \varepsilon.$$

Ορισμός 1.8. Η ομάδα $F[A]$ που μόλις περιγράψαμε θα καλείται η **ελεύθερη ομάδα** που παράγεται από το A.

Επίσης, αν G είναι μία ομάδα και $A = \{a_i\}$ ένα σύνολο γεννητόρων της και αν η G είναι ισόμορφη με την $F[A]$ μεσω της απεικόνισης $\phi : G \to F[A]$, όπου $\phi(a_i) = a_i$, τότε η G λέγεται **ελεύθερη ως προς** A και τα a_i λέγονται **ελεύθεροι γεννήτορες** της G. Μιά ομάδα λέγεται **ελεύθερη** αν είναι ελεύθερη ως προς ένα μη κενό σύνολο A.

Ορισμός 1.9. Μια απεικόνιση ϕ μιας ομάδας $\langle G, * \rangle$ σε μια ομάδα $\langle G', \cdot \rangle$ λέγεται **ομομορφισμός** αν:

$$\phi(a * b) = \phi(a) \cdot \phi(b)$$

για κάθε $a, b \in G$.

Θα επιστρέψουμε στην ομάδα $\mathbb{Z}_n$ των υπολοίπων modulo n. Θεωρούμε μια απεικόνιση ϕ από το σύνολο $\mathbb{Z}$ των ακεραίων στην $\mathbb{Z}_n$ που ορίζεται από την $\phi(m) = r$, όπου r είναι το υπόλοιπο της διαίρεσης όταν ο m δια n. Η απεικόνιση που μόλις ορίσαμε είναι ομομορφισμός. Πράγματι αρκεί να δείξουμε ότι:

$$\phi(s + t) = \phi(s) + \phi(t)$$

για κάθε s, $t \in \mathbb{Z}$. Απο τον αλγόριθμο της διαίρεσης έχουμε:

$$s = q_1 n + r_1 \tag{1.1}$$

και

$$t = q_2 n + r_2 \tag{1.2}$$

όπου $0 \leqslant r_i < n$ για $i = 1, 2$. Αν

$$r_1 + r_2 = q_3 n + r_3 \tag{1.3}$$

με $0 \leqslant r_3 < n$ τότε, προσθέτοντας κατά μέλη τις (1.1) και (1.2) βλέπουμε ότι

$$s + t = (q_1 + q_2 + q_3)n + r_3,$$

άρα $\phi(s + t) = r_3$.
Από τις (1.1) και (1.2) βλέπουμε ότι $\phi(s) = r_1$ και $\phi(t) = r_2$, ενώ από την (1.3) βλέπουμε ότι το άθροισμα $r_1 + r_2 = r_3$ στην $\mathbb{Z}_n$ και το ζητούμενο έχει αποδειχθεί.

Θεώρημα 1.1. *Έστω ϕ ένας ομομορφισμός μιάς ομάδας G σε μια ομάδα G'.*

1. *Αν ε είναι το ταυτοτικό στοιχείο της G, τότε $\phi(\varepsilon)$ είναι το ταυτοτικό στοιχείο ε' της G'.*
2. *Αν $a \in G$ τότε $\phi(a^{-1}) = \phi(a)^{-1}$.*

Απόδειξη. Έστω ϕ ένας ομομορφισμός της G στην G'. Τότε

$$\phi(a) = \phi(a\varepsilon) = \phi(a)\phi(\varepsilon)$$

Πολλαπλασιάζουμε με $\phi(a)^{-1}$ από αριστερά και έχουμε ότι $\varepsilon' = \phi(\varepsilon)$. Άρα το $\phi(\varepsilon)$ πρέπει να είναι το ταυτοτικό στοιχείο ε' της G'. Παρόμοια από την ισότητα:

$$\varepsilon' = \phi(\varepsilon) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$$

έχουμε ότι $\phi(a^{-1}) = \phi(a)^{-1}$. □

Ορισμός 1.10. Ένας ομομορφισμός που είναι *ένα προς ένα* και *επί* θα καλείται **ισομορφισμός**. Ένας ισομορφισμός μιας ομάδας με τον εαυτό της λέγεται **αυτομορφισμός**. Τέλος ένας ομομορφισμός που είναι μόνο *επί* θα καλείται **επιμορφισμός**.

Ορισμός 1.11. Έστω $\phi : G \to G'$ ένας ομομορφισμός ομάδων. Το υποσύνολο της G που απεικονίζεται μέσω του ϕ στο ταυτοτικό στοιχείο ε' της G', λέγεται **πυρήνας** του ϕ και συμβολίζεται με $ker(\phi)$.

$$ker(\phi) = \{g \in G | \phi(g) = \varepsilon'\}$$

Θεώρημα 1.2. *Έστω G μιά ομάδα. Το σύνολο όλων των αυτομορφισμών της G αποτελεί ομάδα με πράξη τη σύνθεση απεικονίσεων. Την ομάδα αυτή θα την συμβοίζουμε με $\boldsymbol{Aut(G)}$. Δηλαδή:*

$$Aut(G) = \{\phi : G \to G \,|\, \phi \textit{ αυτομορφισμός}\}.$$

1.2 Ομάδες Μεταθέσεων

Ορισμός 1.12. Μετάθεση ενός συνόλου A λέγεται μιά συνάρτση από το A στο A που είναι ταυτόχρονα ένα - προς - ένα και επί.

Ας θεωρήσουμε το σύνολο $A = \{1, 2, 3, 4, 5, 6\}$ και έστω μια μετάθεση του συνόλου $\tau : A \to A$ τέτοια ώστε: $\tau(1) = 4$, $\tau(2) = 5$, $\tau(3) = 1$, $\tau(4) = 3$, $\tau(5) = 6$, $\tau(6) = 2$.
Ο τρόπος που από εδώ και στο εξής θα συμβολίζουμε τις μεταθέσεις θα είναι:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$$

Παρατηρούμε ότι για ένα σύνολο με n στοιχεία οι πιθανές μεταθέσεις του είναι $n!$. Εστω A ένα μη κενό σύνολο, και έστω S_A η συλλογή όλων των μεταθέσεων του A. Στην συνέχεια θα δείξουμε ότι το σύνολο S_A αποτελεί ομάδα με πράξη τη σύνθεση των μεταθέσεων. Στην συνέχεια του κειμένου, όποτε αναφερόμαστε στην σύνθεση μεταθέσεων θα την καλούμε **πολλαπλασιασμό μεταθέσεων**.

Θεώρημα 1.3. *Το σύνολο S_A είναι ομάδα με πράξη του πολλαπλασιασμό μεταθέσεων.*

Απόδειξη. Αρχικά θα δείξουμε ότι ο πολλαπλασιασμός μεταθέσεων αποτελεί μια διμελή πράξη, και άρα το σύνολο S_A είναι κλειστό ως προς την πράξη αυτή, και στη συνέχεια θα αποδείξουμε ένα - ένα τα αξιώματα της ομάδας.
Έστω τ, μ μεταθέσεις του A. Η σύνθεση $\tau\mu$ ορίζεται σχηματικά ως εξής:

$$A \xrightarrow{\mu} A \xrightarrow{\tau} A$$

δηλαδή διαβάζουμε τον πολλαπλασιασμό μεταθέσεων από *δεξιά προς τα αριστερά* σεβόμενοι την γνωστή σύνθεση συναρτήσεων όπου $(f \circ g)(x) = f(g(x))$. Αρκεί να δείξουμε ότι η $\tau\mu$ είναι ένα-προς-ένα και επί, άρα είναι και αυτή μετάθεση.
Έστω $a_1,\ a_2\ \in A$ και

$$(\tau\mu)(a_1) = (\tau\mu)(a_2)$$

τότε

$$\begin{aligned} \tau(\mu(a_1)) = \tau(\mu(a_2)) &\xrightarrow{\text{η } \tau \text{ είναι 1-1}} \\ \mu(a_1) = \mu(a_2) &\xrightarrow{\text{η } \mu \text{ είναι 1-1}} \\ a_1 = a_2. & \end{aligned}$$

Άρα η $\tau\mu$ είναι ένα-προς-ένα.
Έστω τώρα κάποιο $a \in A$. Αφού η τ είναι επί του A θα υπάρχει ένα $a' \in A$ τέτοιο ώστε $\tau(a') = a$. Επίσης, αφού η μ είναι επί του A θα υπάρχει ένα $a'' \in A$ τέτοιο ώστε $\mu(a'') = a'$. Άρα:

$$a = \tau(a') = \tau(\mu(a'')) = (\tau\mu)(a'')$$

και άρα η $\tau\mu$ είναι επί του A. Θα αποδείξουμε στη συνέχεια τα τρία αξιώματα της ομάδας:

(i) Αρχικά πρέπει να δείξουμε ότι ο πολλαπλασιασμός μεταθέσεων είναι προσεταιριστικός. Δηλαδή πρέπει να δείξουμε ότι για οποιεσδήποτε μεταθέσεις τ, μ, σ ισχύει ότι

$$[(\tau\mu)\sigma](a) = [\tau(\mu\sigma)](a)$$

για κάθε $a \in A$. Το οποίο ισχύει από την σύνθεση απεικονίσεων.

(ii) Ορίζουμε τώρα την ταυτοτική μετάθεση id τέτοια ώστε $id(a) = a$ για κάθε $a \in A$. Προφανώς η id δρά ως ταυτοτικό στοιχείο και το δεύτερο αξίωμα της ομάδας ικανοποιείται.

(iii) Για μια μετάθεση τ ορίζουμε ως τ^{-1} την αντίστροφη απεικόνιση της τ, δηλαδή την μετάθεση με την οποία αντιστρέφεται η κατεύθυνση της απεικόνισης τ. Για παράδειγμα έστω η μετάθεση τ του συνόλου $A = \{1, 2, 3, 4, 5, 6\}$ που δώσαμε στην αρχή της παραγράφου:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix}$$

Τότε:

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$$

Η ύπαρξη ακριβώς ενός τέτοιου στοιχείου είναι συνέπεια του γεγονότος ότι η τ είναι ένα-προς-ένα και επί. Σχηματικά έχουμε:

$$
\begin{aligned}
1 &\xrightarrow{\tau} 4 \xrightarrow{\tau^{-1}} 1 \\
2 &\longrightarrow 5 \longrightarrow 2 \\
3 &\longrightarrow 1 \longrightarrow 3 \\
4 &\longrightarrow 3 \longrightarrow 4 \\
5 &\longrightarrow 6 \longrightarrow 5 \\
6 &\longrightarrow 2 \longrightarrow 6
\end{aligned}
$$

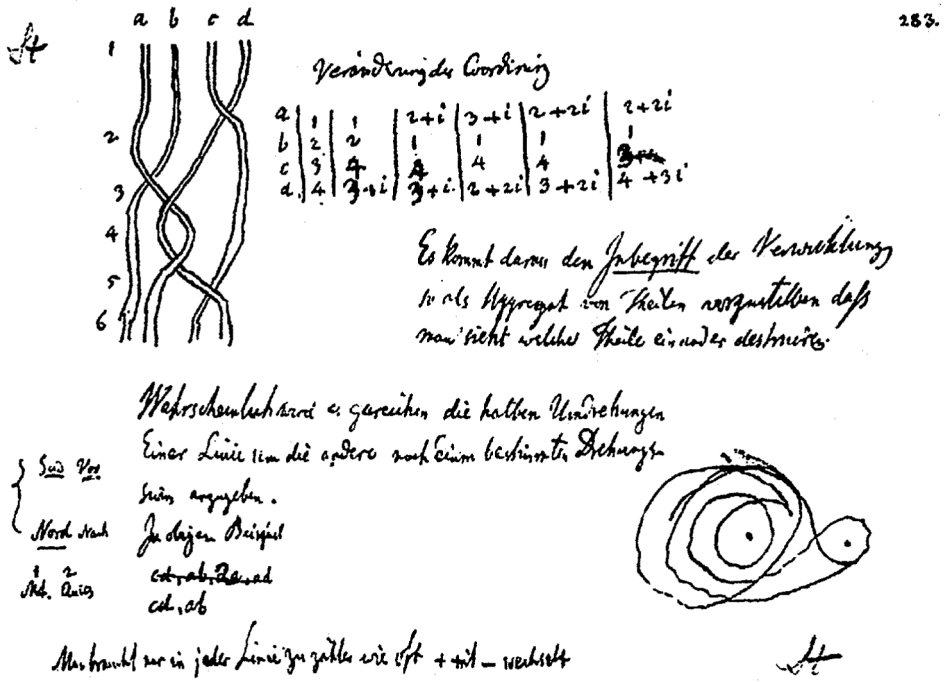
□

Στο εξής θα συμβολίζουμε με $\boldsymbol{\Sigma_n}$ την ομάδα μεταθέσεων n στοιχείων.

1.3 Η ομάδα των πλεξίδων

1.3.1 Ιστορικά

Από τους δακτυλίους του Κρόνου μέχρι την αλυσίδα του DNA και από την γνωστή γυναικεία κοτσίδα μέχρι τις παραδοσιακές ζώνες των Μεξικανών καουμπόυ, για τις οποίες οι K. Murasugi και B. I. Kurpita αφιερώνουν ένα κεφάλαιο στο [28] μελετώντας τες, οι πλεξίδες βρίσκονται σχεδόν παντού. Οι πλεξίδες για τις οποίες θα μιλήσουμε παρακάτω ελάχιστα διαφέρουν από την εικόνα που ενδεχομένως έχει στο νού του ο αναγνώστης διαβάζοντας τα παραπάνω παραδείγματα.

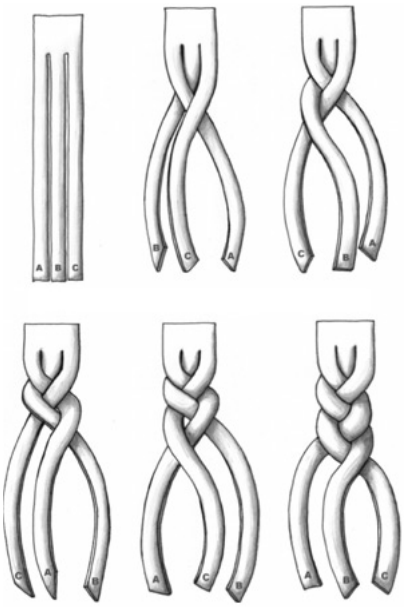


Σχήμα 1.1: Πλεξίδες στα χειρόγραφα του Gauss

Σύμφωνα με τον M. Epple[18], η πρώτη καταγεγραμμένη μαθηματική μορφή της έννοιας των πλεξίδων συναντάται στα γραπτά του Gauss, όταν στις αρχές του $19^{ου}$ αιώνα παρατηρούσε την τροχιά του αστεροειδούς Ceres. Αρκετά χρόνια αργότερα ακολουθεί ένα άρθρο του Adolf Hurwitz που δημοσιεύτηκε το 1891 το οποίο αναφερόταν σε διακλαδωμένα καλύμματα επιφανειών. Η πρώτη σε βάθος μελέτη των πλεξίδων αλλά και ο πρώτος αυστηρός μαθηματικός ορισμός τους έγινε το 1925 όταν, σύμφωνα με το [30], μια κλωστοϋφαντουργία παρήγγειλε στον Emil Artin να μελετήσει και να μοντελοποιήσει το

πλέξιμο των κλωστών. Ο Artin στο [3] διαπίστωσε ότι οι πλεξίδες με σταθερό αριθμό n κλωστών συνιστούν ομάδα, την οποία ονόμασε n^{η} ομάδα πλεξίδων και χρησιμοποίησε για πρώτη φορά τον συμβολισμό B_n. Έκτοτε οι πλεξίδες και οι ομάδες τους μελετώνται εκτενώς από τοπολόγους και αλγεβριστές και έχουν οδηγήσει σε πλούσιες θεωρίες με αρκετές προεκτάσεις.

Το 1983, ο Vaughan Jones, δουλεύοντας πάνω σε άλγεβρες τελεστών ανακάλυψε νέες αναπαραστάσεις των ομάδων πλεξίδων, από τις οποίες εξήγαγε το γνωστό πολυώνυμο των κόμβων (Jones polynomial). Η ανακάλυψη του Jones είχε σαν αποτέλεσμα τη ραγδαία αύξηση του ενδιαφέροντος για τις ομάδες των πλεξίδων. Ανάμεσα στα πιο πρόσφατα αποτελέσματα στο πεδίο αυτό είναι η ύπαρξη μιας ολικής διάταξης στην ομάδα B_n των πλεξίδων, που την απέδειξε ο P. Dehornoy το 1991 και η γραμμικότητα[1] της B_n που αποδείχθηκε ανεξάρτητα από τους Daan Krammer[25] και Stephen Bigelow[5].



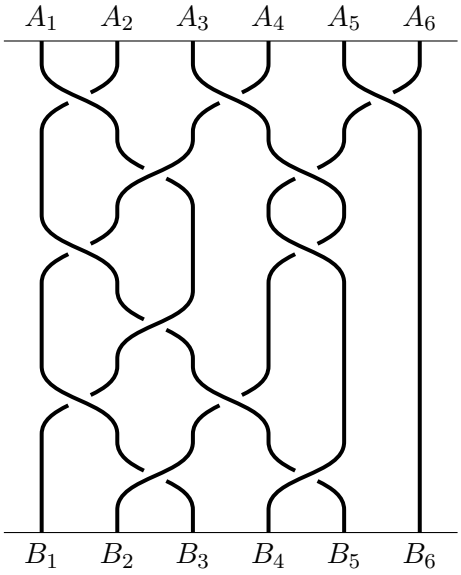
Σχήμα 1.2: Η πλέξη της γνωστής γυναικείας κοτσίδας

1.3.2 Βασικές Εννοιες

Αρχικά θα δώσουμε έναν γεωμετρκό και όχι τόσο αυστηρό ορισμό των πλεξίδων. Θεωρούμε τον χώρο $\mathbb{R}^3$ και έστω τα σημεία $A_i = (i, 0, 0)$ και $B_i = (i, 0, 1)$. Μια πολυγωνική καμπύλη, την οποία από εδώ και στο εξής

[1] Μια ομάδα καλείται γραμμική εάν είναι ισομορφική με μια υποομάδα της $GL(n, K)$ όπου $n \in \mathbb{N}$ και K σώμα.

θα καλούμε **κλωστή,** που ενώνει ένα από τα σημεία A_i με κάποιο B_j θα ονομάζεται **καθοδική** αν κατά την κίνηση ενός σημείου από το A_i στο B_j κατά μήκος της κλωστής, η z-συντεταγμένη του μειώνεται μονότονα. Με άλλα λόγια, οποιοδήποτε οριζόντιο επίπεδο τέμνει την καθοδική καμπύλη ακριβώς μία φορά. Μπορούμε από δω και στο εξής να φανταζόμαστε τις κλωστές ως ελαστικές και τα σημεία A_i, B_i ως γάντζους πάνω στους οποίους είναι στερεωμένες οι κλωστές.



Σχήμα 1.3: Ένα παράδειγμα πλεξίδας

Θεωρούμε ότι η φορά της «πλέξης» είναι από πάνω προς τα κάτω. Θα θεωρήσουμε ως στοιχειώδεις πλέξεις τις διασταυρώσεις γειτονικών κλωστών και θα ορίσουμε ως θετική, την διασταύρωση κατά την οποία η δεξιά κλωστή περνά πάνω από την αριστερή και ως αρνητική την αντίστροφη.
Δύο πλεξίδες οι οποίες μπορούν να μετασχηματιστούν η μία στην άλλη χωρίς να χρειαστεί να «λύσουμε» τα άκρα τους, θα τις θεωρούμε ισοδύναμες και δεν θα κάνουμε καμία διάκριση μεταξύ τους. Επίσης, μπορούμε να ορίσουμε διαισθητικά και με εναν φυσιολογικό τρόπο μια πράξη μεταξύ των πλεξίδων με ίσο αριθμό κλωστών. Τοποθετώντας την πρώτη πλεξίδα πάνω απο την δεύτερη προκύπτει μια καινούργια πλεξίδα. Την σύνθεση αυτή των πλεξίδων θα την ονομάσουμε στην συνέχεια πολλαπλασιασμό. Τέλος μπορούμε να παρατηρήσουμε ότι οποιαδήποτε πλεξίδα μπορεί να «λυθεί» εφαρμόζοντας από κάτω προς τα πάνω τις αντίστροφες πλέξεις της και αυτό που θα προκύψει είναι μιά πλεξίδα(!) χωρίς καμία πλέξη.

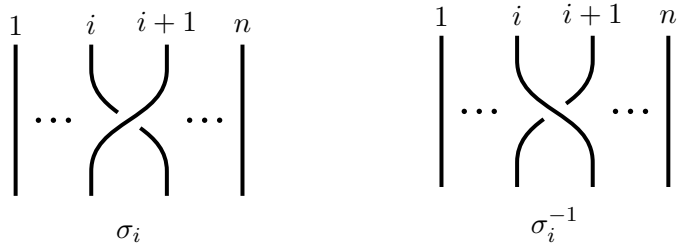
Σε αυτό το σημείο μπορούμε να πούμε πως έχουμε όλα τα απαραίτητα

«συστατικά» προκειμένου να ορίσουμε, με μαθηματικό πλέον τρόπο μια δομή ομάδας στο σύνολο των πλεξίδων με n κλωστές. Θα συνεχίσουμε με τον ορισμό της ομάδας των πλεξίδων όπως αυτός διατυπώθηκε από τον Emil Artin[4].

Ορισμός 1.13. Για $n \geq 2$ η **Ομάδα των Πλεξίδων** (braid group), που στο εξής θα την συμβολίζουμε με $\boldsymbol{B_n}$ ορίζεται από την παράσταση:

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \;\; \text{για } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \;\; \text{για } |i-j| = 1 \end{array} \right\rangle \tag{1.4}$$

Η παραπάνω παράσταση καλείται *παράσταση του Artin* και οι αντίστοιχοι γεννήτορες, *γεννήτορες του Artin*. Τα σ_i, σ_i^{-1} παριστάνουν αυτό που διαισθητικά ορίσαμε πρίν ως την στοιχειώδη θετική και αρνητική πλέξη αντίστοιχα. Είναι προφανές ότι η B_n αποτελεί ομάδα με πράξη τον πολλαπλασιασμό των πλεξίδων και γεννήτορες τα $\sigma_1, \ldots, \sigma_{n-1}$. Οι σχέσεις στην παράσταση του $Artin$ είναι γνωστές ως **σχέσεις πλεξίδων** και απο δώ και στο εξής έτσι θα αναφερόμαστε σε αυτές.



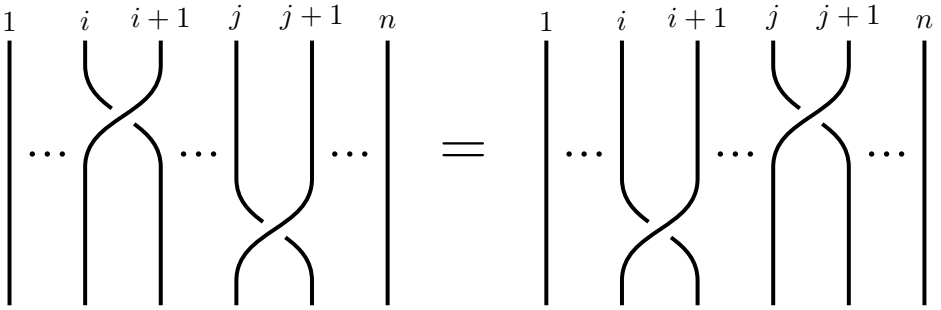
σ_i $\qquad\qquad$ σ_i^{-1}

Σχήμα 1.4: Οι γεννήτορες του Artin

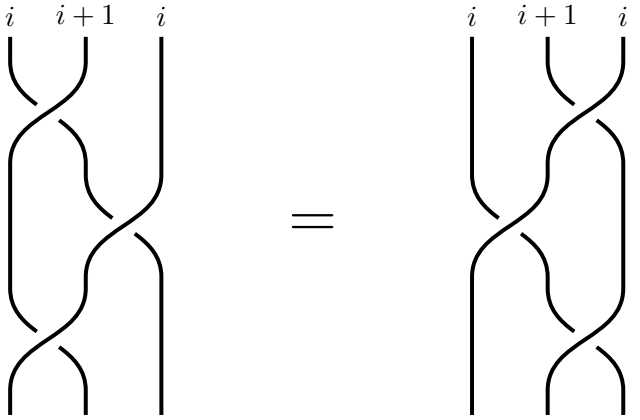
Στο παραπάνω σχήμα (Σχ. 1.4) βλέπουμε τον θετικό γεννήτορα σ_i και τον αντίστροφό του σ_i^{-1}. Η ομάδα των πλεξίδων δεν είναι εν γένει αντιμεταθετική, από τις σχέσεις των πλεξίδων βλέπουμε ότι $\sigma_i\sigma_j = \sigma_j\sigma_i$ μόνο αν $|i-j| \neq 1$.(βλ. Σχ.1.5)

Το Σχήμα 1.6 παρουσιάζει την δεύτερη σχέση πλεξίδων. Εδώ μπορούμε να εφαρμόσουμε αυτό που προηγουμένως ορίσαμε διαισθητικά ως ισοδυναμία πλεξίδων. Πράγματι, αν θεωρήσουμε τις κλωστές που σχηματίζουν τις πλεξίδες ελαστικές, τότε μπορούμε να μετατρέψουμε την πρώτη πλεξίδα στην δεύτερη χωρίς να χρειαστεί να λύσουμε τα άκρα των κλωστών τους.

Προηγουμένως αναφέραμε ότι προκειμένου να ¨λύσουμε¨ μια πλεξίδα αρκεί να εφαρμόσουμε στην αντίθετη φορά της πλέξης τις αντίστροφες διασταυρώσεις των κλωστών. Αλγεβρικά αυτό μεταφράζεται με το να υψώσουμε στην -1 την δοθείσα πλεξίδα και το αποτέλεσμα να το πολλαπλασιάσουμε με την αρχική. Θα δώσουμε ένα παράδειγμα:



Σχήμα 1.5: $\sigma_i\sigma_j = \sigma_j\sigma_i$



Σχήμα 1.6: Η δεύτερη σχέση πλεξίδων $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$

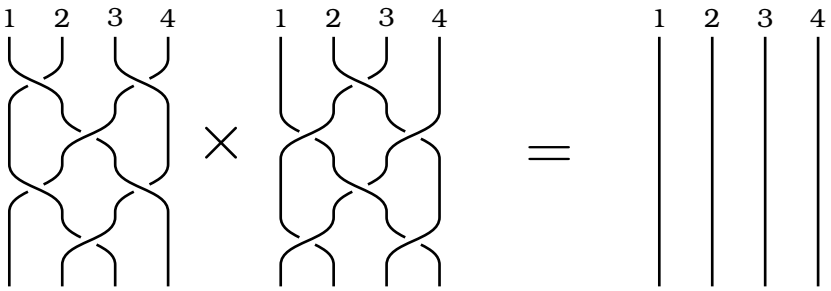
Παράδειγμα 1.7. Έστω η πλεξίδα $\beta = \sigma_1^{-1}\sigma_3^{-1}\sigma_2\sigma_1^{-1}\sigma_3^{-1}\sigma_2$ τότε η αντίστροφή της είναι η

$$\begin{aligned}\beta^{-1} &= (\sigma_1^{-1}\sigma_3^{-1}\sigma_2\sigma_1^{-1}\sigma_3^{-1}\sigma_2)^{-1}\\ &= \sigma_2^{-1}\sigma_3\sigma_1\sigma_2^{-1}\sigma_3\sigma_1.\end{aligned}$$

1.3.3 Η ομάδα των πλεξίδων και η ομάδα μεταθέσεων

Σε αυτήν την παράγραφο θα δείξουμε ότι υπάρχει μια φυσική απεικόνιση από την ομάδα των πλεξίδων B_n στην ομάδα των μεταθέσεων Σ_n. Το γεγονός αυτό βασίζεται στο ότι αν στις σχέσεις των πλεξίδων προσθέσουμε την $\sigma_i^2 = 1$, τότε έχουμε μια παράσταση[2] για την ομάδα μεταθέσεων Σ_n.

[2]Η παράσταση αυτή είναι γνωστή και ως παράσταση Coxeter των ομάδων μεταθέσεων.



Σχήμα 1.7: $\beta\beta^{-1} = 1$

Έστω β μια πλεξίδα n κλωστών. Μπορούμε, όπως περίπου κάναμε προηγουμένως, να θεωρήσουμε ότι κάθε κλωστή ξεκινάει από ένα σημείο i, διασταυρώνεται με κάποιες κλωστές και καταλήγει σε ένα σημείο b_i. Θεωρούμε την μετάθεση $\pi \in \Sigma_n$, τέτοια ώστε:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

Παρατηρούμε εδώ ότι μπορούμε να ορίσουμε την απεικόνιση
$\rho : B_n \to \Sigma_n$, με $\rho(\beta) = \pi$. Εύκολα μπορεί να δείξει κανείς ότι η απεικόνιση αυτή είναι ένας ομομορφισμός της B_n στην Σ_n, ο οποίος μάλιστα είναι και *επί*.

Παράδειγμα 1.8. Έστω η πλεξίδα $\beta = \sigma_1\sigma_3\sigma_2^{-1}\sigma_1\sigma_3\sigma_2^{-1}$, με $b_1 = 4$, $b_2 = 3$, $b_3 = 2$, $b_4 = 4$. Τότε η μετάθεση π που αντιστοιχεί στην β είναι η:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Έστω τώρα, αντίστροφα, ότι σε κάθε μετάθεση $\pi \in \Sigma_n$ αντιστοιχούμε μία πλεξίδα, η οποία κατασκευάζεται ως εξής: ενώνουμε με μία ευθεία γραμμή το κάθε σημείο i με το αντίστοιχο b_i και φροντίζουμε ώστε όλες οι πιθανές διασταυρώσεις να είναι θετικές.

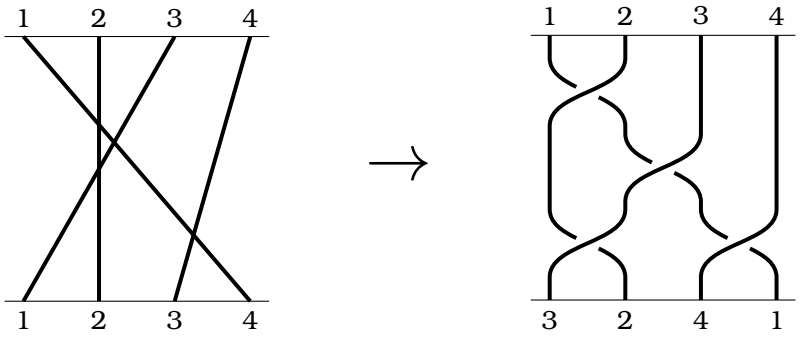
Ορισμός 1.14. Τις πλεξίδες που κατασκευάζονται με τον παραπάνω τρόπο θα τις ονομάζουμε **μεταθετικές πλεξίδες** (permutation braids). Το υποσύνολο αυτό των πλεξίδων θα το συμβολίζουμε με $\widetilde{\Sigma_n}$ και προφανώς έχουμε $|\widetilde{\Sigma_n}| = n!$

Με άλλα λόγια θα μπορούσαμε να πούμε ότι το σύνολο των μεταθετικών πλεξίδων αποτελείται απ' όλες εκείνες τις πλεξίδες, όπου κάθε διασταύρωση είναι θετική και κάθε ζεύγος κλωστών διασταυρώνεται το πολύ μία φορά.

Παράδειγμα 1.9. Έστω τώρα η μετάθεση:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

το παρακάτω σχήμα (βλ. Σχ. 1.7) θα μας βοηθήσει να διασαφηνίσουμε λίγο καλύτερα τον ορισμό.



Σχήμα 1.8: Η κατασκευή μιας πλεξίδας μετάθεσης

Να παρατηρήσουμε σε αυτό το σημείο ότι ο *επιμορφισμός* ρ που ορίσαμε προηγουμένως διαμερίζει την B_n σε $n!$ κλάσεις ισοδυναμίας, οι εκπρόσωποι των οποίων δεν είναι άλλοι από τις μεταθετικές πλεξίδες. Τις πλεξίδες που ανήκουν στον πυρήνα του επιμορφισμού ρ θα τις ονομάζουμε **αμιγείς πλεξίδες** (pure braids). Προφανώς για τις αμιγείς πλεξίδες ισχύει ότι $b_i = i,\ \forall i \in \{1, 2 \ldots, n\}$.

Μια ιδιαίτερη περίπτωση μεταθετικής πλεξίδας είναι αυτή της οποίας όλα τα ζεύγη κλωστών διασταυρώνονται ακριβώς μία φορά. Η συγκεκριμένη πλεξίδα θα μας απασχολήσει πολύ σε επόμενο κεφάλαιο και παίζει σημαντικό ρόλο στην θεωρία των πλεξίδων.

ΚΕΦΑΛΑΙΟ 2

Η λύση του word problem

Σε αυτό το κεφάλαιο θα διατυπώσουμε το γνωστό «πρόβλημα της λέξης» (word problem), καθώς και το «πρόβλημα της συζυγίας»(conjugacy problem). Τα προβλήματα αυτά, εκτός του ότι θεωρούνται γενικά δύσκολα προβλήματα της Θεωρίας των Ομάδων, στην προκειμένη περίπτωση θα μας βοηθήσουν στην εφαρμογή των Ομάδων Πλεξίδων στην Κρυπτογραφία. Στις επόμενες ενότητες αναλύουμε δεξιοδικά δύο από τις σημαντικότερες λύσεις του word problem, που απέχουν αρκετά χρόνια μεταξύ τους. Η πρώτη είναι αυτή του Garside όπως διατυπώθηκε το 1969 στο [22] και η δεύτερη του Dehornoy[11]. Το conjugacy problem, αν και μας χρησιμεύει στην δημιουργία των πρωτοκόλλων δεν αναφερόμαστε στη λύση του.

2.1 Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

Τα προβλήματα που θα διατυπώσουμε παρακάτω χωρίζονται σε δύο γενικές κατηγορίες. Σχηματικά θα μπορούσαμε να πούμε ότι στην πρώτη κατηγορία κατατάσουμε τα προβλήματα που η απάντηση τους είναι «ναι» ή «όχι», ενώ στην δεύτερη ως απάντηση έχουμε την εύρεση του ζητούμενου στοιχείου.

1. **Προβλήματα Απόφασης** (Decision Problems):
   Δοθείσης μιάς ιδιότητας P και ενός αντικειμένου O να βρείτε εάν το αντικείμενο έχει την παραπάνω ιδιότητα.

2. **Προβλήματα Εύρεσης** (Search Problems):
   Δοθείσης μιάς ιδιότητας P και της πληροφορίας ότι υπάρχουν αντικείμενα με την παραπάνω ιδιότητα, βρείτε τουλάχιστον ένα αντικείμενο με αυτήν.

Ορισμός 2.1. Έστω μια ομάδα G. Δύο στοιχεία g, h στην G θα καλούνται **συζυγή** αν υπάρχει στοιχείο $x \in G$ με:

$$xgx^{-1} = h$$

ΠΡΟΒΛΗΜΑΤΑ ΣΥΖΥΓΙΑΣ:

1. **Conjugacy Decision Problem** Έστω δύο στοιχεία $g, h \in G$ βρείτε έαν υπάρχει κάποιο στοιχείο $x \in G$ τέτοιο ώστε: $xgx^{-1} = h$.

2. **Conjugacy Search Problem** Έστω δύο στοιχεία $g, h \in G$, τα οποία είναι συζυγή. Βρείτε ένα $x \in G$ τέτοιο ώστε: $xgx^{-1} = h$.

3. **Generalized Conjugacy Search Problem** Έστω δύο πλεξίδες $\beta_1, \beta_2 \in B_n$, τέτοιες ώστε $\beta_2 = \beta' \beta_1 \beta'^{-1}$ για κάποια $\beta' \in B_m$ με $m \leqslant n$. Βρείτε μια πλεξίδα $\beta'' \in B_m$ τέτοια ώστε $\beta_2 = \beta'' \beta_1 \beta''^{-1}$.
   Η διατύπωση του παραπάνω προβλήματος γίνεται ειδικά για τις ομάδες των πλεξίδων διότι θα μας χρειαστεί στην συγκεκριμένη του μορφή στο κεφάλαιο με τις εφαρμογές των πλεξίδων στην κρυπτογραφία.

Ορισμός 2.2. Η **κανονική μορφή** μιάς ομάδας G, με ένα σύνολο γεννητόρων S, είναι μια επιλογή μιας *συγκεκριμένης λέξης* για κάθε στοιχείο $g \in G$. Να σημειώσουμε ότι η επιλογή αυτής της λέξης οφείλει να ικανοποιεί δύο ιδιότητες:

1. Κάθε στοιχείο της ομάδας πρέπει να έχει μία ακριβώς κανονική μορφή

2. Δύο οποιαδήποτε στοιχεία που έχουν την ίδια κανονική μορφή πρέπει να είναι ίσα.

Όπως θα δούμε στην συνέχεια οι κανονικές μορφές των στοιχείων των ομάδων, μπορούν να αποδειχθούν χρήσιμοι μηχανισμοί απόκρυψης σε κρυπτογραφικά πρωτόκολλα.

2.1.1 Word Problem

Ο πρώτος που επισήμανε τη σημασία του προβλήματος της λέξης ήταν ο Max Dehn στο [10], ο οποίος μάλιστα το έλυσε για την θεμελιώδη ομάδα των επιφανειών. Ο Artin είναι ο πρώτος που έλυσε το πρόβλημα της λέξης για την ομάδα των πλεξίδων (και ο πρώτος που το διατύπωσε), Στην συνέχεια ακολούθησε ο Garside, του οποίου τη λύση θα δούμε στην συνέχεια, ο οποίος όχι μόνο έλυσε το word problem εισάγοντας μια καινούργια λέξη, το τετράγωνο της οποίας είναι το κέντρο της B_n, αλλά έδωσε επίσης και μία λύση για το πρόβλημα της συζυγίας. Έκτοτε πολλοί βελτίωσαν τη λύση του Garside, φτιάχοντας πιό γρήγορους αλγόριθμούς, όπως ο Thurston στο [19] ή εισάγοντας νέους γεννήτορες, όπως οι Birman - Ko - Lee στο [8]. Η λύση που διαφέρει σε μέθοδο απ'ολες τις προαναφερθήσες είναι αυτή του Dehornoy που θα την

εξετάσουμε στην συνέχεια, ο οποίος εισάγει μια εντελώς καινούργια μέθοδο επίλυσης του προβλήματος της λέξης, η οποία όμως αδυνατεί (μέχρι στιγμής) να δώσει κάποια λύση στο πρόβλημα της συζυγίας.

Word Problem (I): Έστω G μια ομάδα και έστω ένα στοιχείο $g \in G$, βρείτε αν ισχύει: $g = \varepsilon$.

Το παραπάνω πρόβλημα διατυπώνεται ισοδύναμα ως εξής:

Word Problem (II): Έστω g_1, g_2 στοιχεία στην G. Βρείτε αν ισχύει: $g_1 = g_2$.

Προφανώς τα δύο προβλήματα είναι ισοδύναμα θέτοντας $g = g_1 g_2^{-1}$.

2.2 Κανονική Μόρφη Garside

Στην παρούσα ενότητα θα αποδείξουμε το ακόλουθο θεώρημα:

Θεώρημα 2.1 (Θεώρημα 5 στο [22])**.** *Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$*

όπου:

- Δ *η* ***θεμελιώδης λέξη***
- $m \in \mathbb{Z}$
- $\bar{A}$ ***θετική λέξη****, μοναδικά εκφρασμένη.*

Το παραπάνω θεώρημα μας εξασφαλίζει τη δυνατότητα με άμεσο και γρήγορο τρόπο να συγκρίνουμε δύο οποιεσδήποτε λέξεις στην B_{n+1} και επί της ουσίας αποτελεί λύση του **word problem**.
Προκειμένου να παρουσιάσουμε την απόδειξη του θεωρήματος θα χρειαστούμε κάποιους ορισμούς και συμβολισμούς καθώς και κάποια βοηθητικά λήμματα και θεωρήματα. Για λόγους απλότητας και για να αποφύγουμε τη συχνή χρήση του δείκτη $n-1$ του γεννήτορα σ_{n-1} θα δουλέψουμε στην ομάδα B_{n+1} ακολουθώντας το παράδειγμα του ίδιου του Garside.

2.2.1 Βασικές Εννοιες, Ορισμοί και Συμβολισμοί

Ορισμός 2.3. Μια λέξη W που αποτελείται από μια ακολουθία γεννητόρων όπου κανένας αντίστροφος γεννήτορας δεν εμφανίζεται θα καλείται **θετική λέξη**.

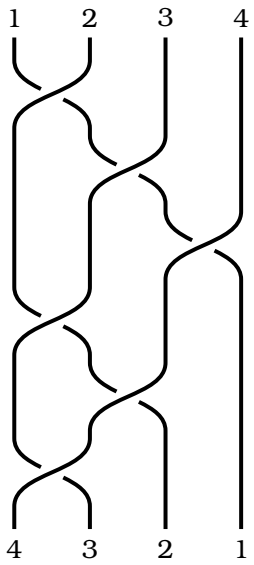
Θα συμβολίζουμε με $\mathbf{L(W)}$ το μήκος της λέξης W.

Ορισμός 2.4. Δύο θετικές λέξεις A, B θα λέμε ότι είναι **θετικά ίσες** αν:

1. Είναι ταυτοτικά ίσες $(A \equiv B)$,
2. Αν μπορεί να μετασχηματιστεί η μία στην άλλη μετα απο μία ακολουθία θετικών λέξεων, τέτοιες ώστε κάθε λέξη της ακολουθίας να προκύπτει από την προηγούμενη μέσω μιας μοναδικής εφαρμογής τών σχέσεων πλεξίδων, έτσι ώστε σε κανένα στάδιο του μετασχηματισμού να μην γίνεται χρήση αντίστροφων γεννητόρων.

Αν A θετικά ίση με την B θα γράφουμε $\mathbf{A \doteq B}$.

Ορισμός 2.5. Ορίζουμε με $\Delta_r \equiv \Pi_r \Pi_{r-1} \dots \Pi_1$ τη **θεμελιώδη λέξη τάξης r+1**, όπου με Π_s συμβολίζουμε την αύξουσα ακολουθία γεννητόρων $(\sigma_1 \sigma_2 \dots \sigma_s)$.
Όταν αναφερόμαστε στην B_{n+1} θα συμβολίζουμε την Δ_n με Δ.



Σχήμα 2.1: Η θεμελιώδης λέξη Δ_4

Ορισμός 2.6. Αν $P \equiv x_1 x_2 \dots x_t$ μια οποιαδήποτε λέξη, όπου το κάθε x_i είναι ένας γεννήτορας ή ο αντίστροφός του, όχι κατ' ανάγκη διαφορετικοί μεταξύ τους, ορίζουμε ως **αναστροφή** της P την λέξη $x_t \dots x_2 x_1$ και θα την συμβολίζουμε με $\boldsymbol{revP}$.

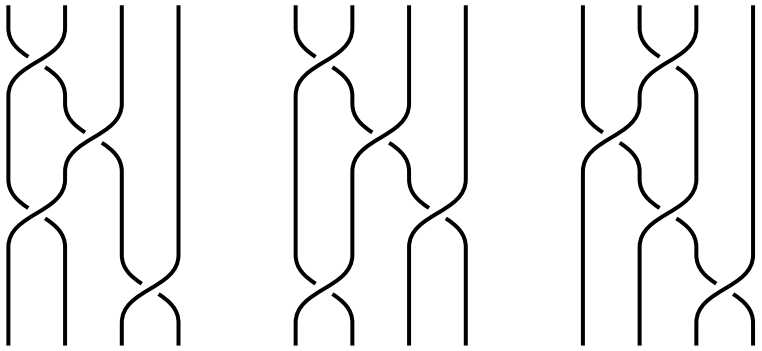
Παρατήρηση 2.1. Παρατηρούμε ότι για P, Q τυχαίες λέξεις έχουμε:
$revPQ = revP\, revQ$.
Πράγματι έστω $P = x_1 \dots x_t$ και $Q = y_1 \dots y_s$, τότε:
$PQ = x_1 \dots x_t y_1 \dots y_s \Rightarrow\ revPQ = y_s \dots y_1 x_t \dots x_1 = revQ\, revP$
Επίσης αν $P \doteq Q$ τότε $revP \doteq revQ$

Ορισμός 2.7. Έστω W μια θετική λέξη και έστω $W_1, W_2, \dots, W_m$ το σύνολο όλων των διακεκριμένων θετικών λέξεων που είναι θετικά ίσες ως προς την W. Το σύνολο αυτό θα το συμβολίζουμε με $\mathbf{D(W)}$.

$$D(W) = \{W_i \mid (W_i \quad \text{θετικές λέξεις} \wedge (W_i \doteq W) \wedge (W_i \neq W_j), \forall i, j \in \{1 \dots m\}\}$$

Προκειμένου να αποσαφηνίσουμε λιγάκι τον παραπάνω ορισμό θα δώσουμε ένα παράδειγμα:

- Έστω η λέξη $W = \sigma_1\sigma_2\sigma_1\sigma_3$ στην B_4 τότε το $D(W)$ είναι το σύνολο: $\{\sigma_1\sigma_2\sigma_1\sigma_3, \sigma_1\sigma_2\sigma_3\sigma_1, \sigma_2\sigma_1\sigma_2\sigma_3\}$. Βλ. Σχ 2.2



Σχήμα 2.2: Οι ισοδύναμες λέξεις

Ο παραπάνω ορισμός καθώς και κάποιοι που θα ακολουθήσουν συνδέονται άμεσα με την αναπαράσταση ομάδων μέσω των γεννητόρων τους σε διαγράμματα Cayley[1] . Στην παρούσα εργασία για λόγους απλότητας αλλά και γιατί τα αποτελέσματα και τα θεωρήματα που θα χρησιμοποιήσουμε περιορίζονται σε ένα καθαρά αλγεβρικό επίπεδο, θα αποφύγουμε να αναφερθούμε στην γραφική αναπαράσταση των διαγραμμάτων αυτών.

Ορισμός 2.8. Οι λέξεις $W, W_1, \ldots, W_m$ θα καλούνται **μονοπάτια** του $D(W)$.

Ορισμός 2.9. Έστω W μια οποιαδήποτε θετική λέξη. Αν A, X δυο θετικές λέξεις τέτοιες ώστε $W \doteq AX$ με $L(A), L(X) \geqslant 0$ θα καλούμε το $D(A)$ **κόμβο** του $D(W)$. Συχνά συμβολίζουμε με $\dot{A}$ τον κόμβο $D(A)$. Αν $L(A) = t$ θα λέμε ότι ο κόμβος $\dot{A}$ είναι **τάξης** t.

Ορισμός 2.10. Έστω W, A, X, B θετικές λέξεις στην ομάδα B_{n+1}

- Αν $W \doteq AXB$ με $L(A), L(B) \geqslant 0$ θα λέμε ότι η X είναι **υπο-μονοπάτι** του $D(W)$.
- Αν $L(A) = 0$ θα λέμε ότι η X είναι **αρχικό υπο-μονοπάτι** της $D(W)$.
- Αν $W \doteq PXQ$, όπου P, Q θετικές λέξεις με $L(P), L(Q) \geqslant 0$ θα λέμε ότι το υπο-μονοπάτι X **ξεκινά** στον κόμβο $\dot{P}$
- Αν $W \doteq RQ \doteq PXQ$θα λέμε ότι το υπο-μονοπάτι X **τελειώνει** στον κόμβο $\dot{R}$.

Ορισμός 2.11. Έστω W μια λέξη μήκους l στην B_{n+1} και έστω ότι το $D(W)$ αποτελείται από m λέξεις: $W_1 \equiv \sigma_i\sigma_j\sigma_k..., W_2 \equiv \sigma_p\sigma_q\sigma_r..., \ldots, W_m \equiv \sigma_x\sigma_y\sigma_z...$

[1]Παραπέμπουμε τον αναγνώστη που ενδιαφέρεται για τα διαγράμματα Cayley στο άρθρο του *"On theory of groups"*, Proc. London Math Soc 1 (1878) 126-33

Τότε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των λέξεων: $W_1, W_2, \ldots, W_m$ και των αριθμών $P_1 \equiv ijk..., P_2 \equiv pqr..., \ldots, P_m \equiv xyz...$, όπου κάθε αριθμός εκφράζεται στην κλίμακα n και αποτελείται από l ψηφία. Οι αριθμοί $P_i, i \in \{1, ..., m\}$ είναι διακεκριμένοι μεταξύ τους. Έστω P_r ο μικρότερος εξ' αυτών, τότε η αντίστοιχη λέξη W_r θα καλείται **βάση** του $D(W)$.

Ορισμός 2.12. Αν οποιοδήποτε υπο-μονοπάτι του $D(W)$ είναι η Δ, δηλαδή αν $W \doteq A\Delta B$, με $L(A), L(B) \geqslant 0$ θα λέμε ότι η Δ είναι **παράγοντας** της W ή ότι η W **περιέχει** την Δ.

Ορισμός 2.13. Αν W είναι μια οποιαδήποτε θετική λέξη στην B_{n+1} που δεν περιέχει την Δ θα λέμε ότι η W είναι **πρώτη** ως προς την Δ.

Ορισμός 2.14. Στην B_{n+1} έστω $\mathcal{R}$ η απεικόνιση του συνόλου των γεννητόρων στον εαυτό του, $\mathcal{R}$:$\{\sigma_1, \ldots, \sigma_n\} \mapsto \{\sigma_1, \ldots, \sigma_n\}$, όπου $\mathcal{R}\sigma_i = \sigma_{n+1-i}$. Τότε έπειτα απο έλεγχο των σχέσεων η $\mathcal{R}$ επεκτείνεται σε έναν αυτομορφισμό στην B_{n+1}. Αυτόν τον αυτομορφισμό συνεχίζουμε να τον συμβολίζουμε με $\boldsymbol{\mathcal{R}}$ και καλείται **ανάκλαση** στην B_{n+1}.

Παρατηρούμε ότι αν $P \doteq Q$, τότε $\mathcal{R}P \doteq \mathcal{R}Q$.

Τα δύο ακόλουθα θεωρήματα αφορούν στις θετικές λέξεις της B_{n+1} και θα μας φανούν χρήσιμα στην απόδειξη κάποιων επόμενων λημμάτων. Η απόδειξη τους γίνεται με επαγωγή στο μήκος των λέξεων Q, U και για λόγους συντομίας παραλείπεται απο την παρούσα διπλωματική. Ο αναγνώστης που ενδιαφέρεται μπορεί να βρεί τις αποδείξεις στο [22].

Θεώρημα 2.2. *Στην B_{n+1}, δοθέντος ότι $\sigma_i X \doteq \sigma_k Y$ για $i, k = 1, 2, \ldots, n$ συνεπάγεται ότι:*

(i) Αν $i = k$, τότε $X \doteq Y$.

(ii) Αν $|i - k| \geqslant 2$, τότε $X \doteq \sigma_k Z$ και $Y \doteq \sigma_i Z$ για κάποια λέξη Z.

(iii) Αν $|i - k| = 1$, τότε $X \doteq \sigma_k \sigma_i Z$ και $Y \doteq \sigma_i \sigma_k Z$ για κάποια λέξη Z.

Θεώρημα 2.3. *Στην B_{n+1}, δοθέντος ότι $X\sigma_i \doteq Y\sigma_k$ για $i, k = 1, 2, \ldots, n$ συνεπάγεται ότι:*

(i) Αν $i = k$, τότε $X \doteq Y$

(ii) Αν $|i - k| \geqslant 2$, τότε $X \doteq Z\sigma_k$ και $Y \doteq Z\sigma_i$ για κάποια Z.

(iii) Αν $|i - k| = 1$, τότε $X \doteq Z\sigma_k\sigma_i$ και $Y \doteq Z\sigma_i\sigma_k$ για κάποια Z.

Πόρισμα 2.1. *Στην B_{n+1} αν $A \doteq P, B \doteq Q$ και $AXB \doteq PYQ$ με $L(A), L(B) \geqslant 0$, τοτε $X \doteq Y$.*

Απόδειξη. Πράγματι έχουμε ότι $AXB \doteq PYQ$ και $A \doteq P$ από Θεώρημα 2.2 έχουμε $XB \doteq YQ$ όμοια επειδή $B \doteq Q$ από Θεώρημα 2.3 έχουμε ότι $X \doteq Y$. □

Λήμμα 2.1. *Στην B_{n+1} για $1 < s \leqslant t \leqslant n$ ισχύει* $\sigma_s \Pi_t = \Pi_t \sigma_{s-1}$.

Απόδειξη.

$$\begin{aligned}
\sigma_s \Pi_t &= \sigma_s(\sigma_1 \dots \sigma_{s-2})\sigma_{s-1}\sigma_s(\sigma_{s+1} \dots \sigma_t) \\
&= (\sigma_1 \dots \sigma_{s-2})\sigma_s\sigma_{s-1}\sigma_s(\sigma_{s+1} \dots \sigma_t) \\
&= (\sigma_1 \dots \sigma_{s-2})\sigma_{s-1}\sigma_s\sigma_{s-1}(\sigma_{s+1} \dots \sigma_t) \\
&= (\sigma_1 \dots \sigma_{s-2})\sigma_{s-1}\sigma_s(\sigma_{s+1} \dots \sigma_t)\sigma_{s-1} \\
&= \Pi_t \sigma_{s-1}
\end{aligned}$$

□

Στη συνέχεια θα αποδείξουμε κάποια λήμματα και θεωρήματα που αφορούν στις ιδιότητες της θεμελιώδους λέξης Δ.

Λήμμα 2.2. *Στην B_{n+1} ισχύουν:*

(i) $\sigma_1 \Delta_t \doteq \Delta_t \sigma_t (t = 1, \dots, n)$

(ii) $\sigma_s \Delta \doteq \Delta \mathcal{R} \sigma_s$

(iii) $\sigma_s^{-1} \Delta = \Delta (\mathcal{R}\sigma_s)^{-1}$

(iv) $\sigma_s \Delta^{-1} = \Delta^{-1} \mathcal{R} \sigma_s$

(v) $\sigma_s^{-1} \Delta^{-1} = \Delta^{-1} (\mathcal{R}\sigma_s)^{-1}$

Απόδειξη. (i) Με επαγωγή στο t. Για $t = 1$ έχουμε:

$$\sigma_1 \Delta_1 \equiv \sigma_1 \sigma_1 \doteq \Delta_1 \sigma_1$$

Για $t = 2, \dots, n$:

$$\begin{aligned}
\sigma_1 \Delta_t &\equiv \sigma_1 \Pi_t \Pi_{t-1} \Delta_{t-2} \\
&\doteq \sigma_1 \Pi_t (\sigma_1 \dots \sigma_{t-1}) \Delta_{t-2} \\
&\doteq \sigma_1 (\sigma_2 \dots \sigma_t) \Pi_t \Delta_{t-2} \quad \text{(από Λήμμα 2.1)} \\
&\doteq \Pi_t \Pi_{t-1} \sigma_t \Delta_{t-2} \\
&\doteq \Pi_t \Pi_{t-1} \Delta_{t-2} \sigma_t \\
&\doteq \Delta_t \sigma_t
\end{aligned}$$

(ii) Με επαγωγή στο s απο το (i) για $s = 1$ έχουμε:

$$\sigma_1\Delta \doteq \Delta\sigma_n \equiv \Delta\mathcal{R}\sigma_1$$

Για $s = 2, \ldots, n$:

$$\begin{aligned}
\sigma_s\Delta &\equiv \sigma_s\Pi_n\Pi_{n-1}\ldots\Pi_{n-s+2}\Delta_{n-s+1} \\
&\doteq \Pi_n\Pi_{n-1}\ldots\Pi_{n-s+2}\sigma_1\Delta_{n-s+1} \quad \text{(από Λήμμα 2.1)} \\
&\doteq \Pi_n\Pi_{n-1}\ldots\Pi_{n-s+2}\Delta_{n-s+1}\sigma_{n-s+1} \quad \text{(από (i))} \\
&\equiv \Delta\sigma_{n-s+1} \\
&\doteq \Delta\mathcal{R}\sigma_s
\end{aligned}$$

Λειπουν οι αποδείξεις των (iii),(iv),(v) □

Πόρισμα 2.2. *Στην B_{n+1} ισχύουν:*

1. *$P\Delta^{2m} \doteq \Delta^{2m}P$, $P\Delta^{2m+1} \doteq \Delta^{2m+1}\mathcal{R}P$ για κάθε θετική λέξη P, $m \in \mathbb{N}$*
2. *$Q\Delta^{2m} = \Delta^{2m}Q, Q\Delta^{2m+1} = \Delta^{2m+1}\mathcal{R}Q$ για κάθε λέξη Q, $m \in \mathbb{Z}$*

Απόδειξη. Θα αρκεστούμε στο να αποδείξουμε το (i) καθώς το παραπάνω πόρισμα αποτελεί άμεση εφαρμογή του Λήμματος 2.1

$$\begin{aligned}
P\Delta^{2m} &\equiv \underbrace{P\Delta^2\Delta^2\ldots\Delta^2}_{\text{m φορες}} \\
&\equiv \underbrace{P(\Delta\Delta)(\Delta\Delta)\ldots(\Delta\Delta)}_{\text{m φορες}} \\
&\doteq \Delta\mathcal{R}P\Delta\underbrace{(\Delta\Delta)\ldots(\Delta\Delta)}_{\text{m-1 φορες}} \quad \text{(από Λήμμα 2.2)} \\
&\doteq \Delta\Delta\mathcal{R}(\mathcal{R}P)(\Delta\Delta)\ldots(\Delta\Delta)\,(\mathcal{R}\mathcal{R}P = P) \\
&\doteq \Delta^{2m}P.
\end{aligned}$$

□

Λήμμα 2.3. *Στην B_{n+1} έχουμε ότι $rev\Delta \doteq \Delta$.*

Απόδειξη. Με επαγωγή έχουμε:

$$rev\Delta_1 \equiv\ rev\sigma_1 \doteq \sigma_1 \equiv \Delta_1$$

Έστω ότι ισχύει για r: $rev\Delta_r \doteq \Delta_r$. Τότε:

$$\begin{aligned}
rev\Delta_{r+1} &\equiv rev\{(\sigma_1\ldots\sigma_{r+1})\Delta_r\} \\
&\equiv rev\Delta_r rev(\sigma_1\ldots\sigma_{r+1}) \\
&\doteq \Delta_r(\sigma_{r+1}\ldots\sigma_1) \\
&\doteq \{\Pi_r\Pi_{r-1}\ldots\Pi_1\}\sigma_{r+1}\ldots\sigma_1 \\
&\doteq \Pi_r\sigma_{r+1}\Pi_{r-1}\sigma_r\ldots\Pi_2\sigma_3\Pi_1\sigma_2\sigma_1 \\
&\equiv \Delta_{r+1}
\end{aligned}$$

□

Λήμμα 2.4. *Στην B_{n+1} υπάρχουν θετικές λέξεις X_r, Y_r τέτοιες ώστε: $\sigma_r X_r \doteq \Delta \doteq Y_r \sigma_r$ με $r = 1, 2, \ldots, n$.*

Απόδειξη. Με επαγωγή στο r:
Για $r = 1$ εξ' ορισμμού έχουμε ότι:

$$\begin{aligned} \Delta &\equiv \Pi_n \Pi_{n-1} \ldots \Pi_1 \\ &\doteq Y_1 \sigma_1 \quad \text{όπου } Y_1 = \Pi_n \Pi_{n-1} \ldots \Pi_2 \end{aligned} \tag{2.1}$$

Παρατηρούμε ότι αν $f(\sigma_2, \sigma_3, \ldots, \sigma_t)$ είναι μια οποιαδήποτε θετική λέξη που περιέχει μόνο τους γεννήτορες $\sigma_2, \sigma_3, \ldots, \sigma_t$ τότε από Λήμμα 2.1 έχουμε:

$$\Pi_t f(\sigma_1, \sigma_2, \ldots, \sigma_{t-1}) \doteq f(\sigma_2, \sigma_3, \ldots, \sigma_t) \Pi_t$$

Έστω τώρα ότι σ_t ένας οποιοσδήποτε εκ των γεννητόρων $\sigma_2, \sigma_3, \ldots, \sigma_n$. Συμβολίζοντας με $g(\sigma_1, \sigma_2, \ldots, \sigma_{t-1})$ το $\Pi_{t-1} \Pi_{t-2} \ldots \Pi_1$ έχουμε:

$$\begin{aligned} \Delta &\equiv \Pi_n \Pi_{n-1} \ldots \Pi_{t+1} \Pi_t g(\sigma_1, \sigma_2, \ldots, \sigma_{t-1}) \\ &\doteq \Pi_n \Pi_{n-1} \ldots \Pi_{t+1} g(\sigma_2, \sigma_3, \ldots, \sigma_t) \Pi_t \\ &\doteq \Pi_n \Pi_{n-1} \ldots \Pi_{t+1} g(\sigma_2, \sigma_3, \ldots, \sigma_t)(\sigma_1 \ldots \sigma_{t-1}) \sigma_t \end{aligned} \tag{2.2}$$

Από τις σχέσεις (2.1), (2.2) έχουμε ότι οι λέξεις Y_r υπάρχουν για κάθε $r = 1, 2, \ldots, n$. Θέτουμε $X_r = revY_r$ έχουμε για $r = 1, 2, \ldots, n$

$$\sigma_r X_r \equiv \sigma_r revY_r \equiv rev(Y_r \sigma_r) \doteq rev\Delta \doteq \Delta \quad \text{από Λήμμα 2.3}$$

□

Θεώρημα 2.4. *Στην B_{n+1} αν δυο θετικές λέξεις είναι ίσες τότε είναι και θετικά ίσες*

Η απόδειξη του παραπάνω θεωρήματος βασίζεται στο Θεώρημα του Öre[29] και παραλείπεται, μπορεί να βρεθεί στο [22].

2.2.2 Η απόδειξη του Θεωρήματος 2.1

Απόδειξη του Θεωρήματος 2.1. (i) Έστω P μια οποιαδήποτε θετική λέξη στην B_{n+1} . Από το σύνολο $D(P)$ επιλέγουμε ένα μονοπάτι με τα μέγιστα συνεχόμενα υπο-μονοπάτια Δ, έστω $t \geqslant 0$. Έστω τώρα ότι $P = \Delta^t A$. Τότε η A θα είναι πρώτη ως προς τη Δ γιατί διαφορετικά θα υπήρχε μονοπάτι του $D(P)$ με περισσότερα από t συνεχόμενα υπο-μονοπάτια, άτοπο. Συμβολίζουμε με $\bar{A}$ τη βάση του A και έχουμε: $P = \Delta^t \bar{A}$.

(ii) Έστω τώρα W μια οποιαδήποτε λέξη στην B_{n+1}, τότε:

$$W \equiv W_1(x_1)^{-1} W_2(x_2)^{-1} \ldots W_s(x_s)^{-1} W_{s+1}$$

όπου κάθε W_r είναι μια θετική λέξη με $L(W) \geqslant 0$ και κάθε x_r ένας γεννήτορας. Από το Λήμμα 2.4 για κάθε x_r υπάρχει μια θετική λέξη X_r τέτοια ώστε: $x_r X_r \doteq \Delta \Rightarrow (x_r)^{-1} = X_r \Delta^{-1}$
Συνεπώς έχουμε: $W = W_1 X_1 \Delta^{-1} W_2 X_2 \Delta^{-1} \dots W_s X_s \Delta^{-1} W_{s+1}$. Μετακινούμε τους παράγοντες Δ^{-1} στα αριστερά (από Πόρισμα 2.2) και έχουμε: $W = \Delta^{-s} P$, όπου P μια θετική λέξη. Από (i) εκφράζουμε την P στην μορφή $\Delta^t \bar{A}$ και έχουμε:

$$\begin{aligned} W &= \Delta^{-s} \Delta^t \bar{A} \\ &= \Delta^m \bar{A} \quad \text{με } t - s = m \end{aligned} \tag{2.3}$$

(iii) Θα αποδείξουμε τώρα την μοναδικότητα της μορφης (2.3):
Έστω

$$\Delta^m \bar{A} = \Delta^k \bar{B} \tag{2.4}$$

Υποθέτουμε ότι $k < m$ και $m - k = t$ όπου $t > 0$ από τη σχέση (2.4) έχουμε ότι $\Delta^t \bar{A} = \bar{B}$, από Θεώρημα 2.4 $\Delta^t \bar{A} \doteq \bar{B}$ και άρα η $\bar{B}$ περιέχει την Δ, άτοπο.
Άρα $k \not< m$.
Όμοια προκύπτει και ότι $m \not< k$ και συνεπάγεται ότι $k = m$. Από τη σχέση (2.4) έχουμε ότι $\bar{A} \doteq \bar{B}$ και από Θεώρημα 2.4 έχουμε ότι $\bar{A} = \bar{B}$, αλλά κάθε θετική λέξη έχει μοναδική βάση άρα $\bar{A} \equiv \bar{B}$.

□

Στην συνέχεια και με την βοήθεια της ακόλουθης πρότασης θα δώσουμε μια ενδιαφέρουσα απόδειξη για το κέντρο της B_{n+1}. Να σημειώσουμε ότι ο πρώτος που έδωσε μία απόδειξη για το κέντρο της Ομάδας των Πλεξίδων είναι ο W.L. Chow στο [9].

Πρόταση 2.1. *Έστω W μία θετική λέξη στην B_{n+1} τέτοια ώστε είτε:*

(i) $W \doteq \sigma_1 X_1 \doteq \sigma_2 X_2 \doteq \dots \doteq \sigma_n X_n \qquad$ *ή*

(ii) $W \doteq Y_1 \sigma_1 \doteq Y_2 \sigma_2 \doteq \dots \doteq Y_n \sigma_n$

Τότε $W \doteq \Delta Z$ για κάποια Z.

Το θεώρημα που ακολουθεί βασίζεται επίσης, στο γεγονός ότι έχουμε αποδείξει πλέον ότι κάθε λέξη στην B_{n+1} μπορεί να γραφεί μοναδικά στην μορφή $\Delta^m \bar{A}$.

Θεώρημα 2.5 (Το κέντρο της B_{n+1})**.** *Έστω η ομάδα B_{n+1}.*

1. *Όταν $n = 1$ το κέντρο της B_{n+1} παράγεται από την Δ.*
2. *Όταν $n > 1$ το κέντρο της B_{n+1} παράγεται από την Δ^2.*

Απόδειξη. Η πρώτη περίπτωση είναι τετριμμένη και το αποτέλεσμα είναι προφανές. Έστω τώρα ότι $n > 1$ και έστω W μια οποιαδήποτε λέξη στο κέντρο της B_{n+1}. Τότε, από τον ορισμό του κέντρου, αν X μια λέξη στην B_{n+1} έχουμε:

$$WX = XW \tag{2.5}$$

Υπάρχουν τρείς πιθανές μορφές της λέξης W:

(α') $W = \Delta^p \bar{A}$, όπου $L(\bar{A}) > 0$.

(β') $W = \Delta^{2m+1}$.

(γ') $W = \Delta^{2m}$.

Θα εξετάσουμε στην συνέχεια μία-μία τις τρείς πιθανές μορφές.

(α') Εξετάζουμε πρώτα την περίπτωση όπου $W = \Delta^p \bar{A}$, με $L(\bar{A}) > 0$. Έστω $\bar{A} = \sigma_i A_i$ με $L(A_i) \geqslant 0$ και έστω $|s - i| = 1$. Θεωρώντας αρχικά ότι το p είναι ζυγός θέτουμε $X \equiv \sigma_s \sigma_i$. Τότε από την σχέση (2.5) έχουμε:

$$\begin{aligned} \Delta^p \sigma_i A_i \sigma_s \sigma_i &= \sigma_s \sigma_i \Delta^p \sigma_i A_i \\ &= \Delta^p \sigma_s \sigma_i \sigma_i A_i \text{ (από Πόρισμα 2.2)} \end{aligned}$$

Άρα

$$\sigma_i A_i \sigma_s \sigma_i = \sigma_s \sigma_i \sigma_i A_i \xrightarrow{\text{Θεώρημα 2.4}} \sigma_i A_i \sigma_s \sigma_i \doteq \sigma_s \sigma_i \sigma_i A_i$$

Από Θεώρημα 2.2 έχουμε ότι $\sigma_i \sigma_i A_i \doteq \sigma_i \sigma_s A_s$ για κάποια A_s και έτσι από Πόρισμα 2.1 έχουμε:

$$\sigma_i A_i \doteq \sigma_s A_s \tag{2.6}$$

Αν ο p είναι περιττός καταλήγουμε στο ίδιο αποτέλεσμα θέτοντας $X \equiv \mathcal{R}(\sigma_s \sigma_i)$. Εφαρμόζοντας διαδοχικά τη σχέση (2.6) έχουμε:

$$\sigma_1 a_1 \doteq \sigma_2 A \doteq \ldots \doteq \sigma_n A_n \doteq \bar{A}$$

Άρα από την Πρόταση 2.1 η $\bar{A}$ περιέχει την Δ, το οποίο από τον ορισμό της $\bar{A}$ είναι αδύνατο. Άρα δεν υπάρχουν λέξεις της μορφής (α') στο κέντρο της B_{n+1}.

(β') Στην περίπτωση που $W = \Delta^{2m+1}$, θέτουμε $X \equiv \sigma_1$. Τότε, από την σχέση (2.5) έχουμε:

$$\begin{aligned} \Delta^{2m+1} \sigma_1 = \sigma_1 \Delta^{2m+1} &\xrightarrow{\text{Πόρισμα 2.2}} \\ &= \Delta^{2m+1} \mathcal{R} \sigma_1 \end{aligned}$$

Άρα $\sigma_1 = \mathcal{R}\sigma_1$, άτοπο καθώς $n > 1$.

(γ') Τέλος θεωρούμε την περίπτωση όπου $W = \Delta^{2m}$. Από το Πόρισμα 2.2 έχουμε ότι η σχέση (2.5) ικανοποιείται και άρα οποιαδήποτε λέξη της μορφής Δ^{2m} είναι στο κέντρο της B_{n+1}. Αρα το κέντρο παράγεται από την Δ^2.

□

2.3 Dehornoy Handle Reduction

Θα ξεκινήσουμε με κάποιους βασικούς ορισμούς προκειμένου να παρουσιάσουμε το κεντρικό αποτέλεσμα της συγκεκριμένης παραγράφου

Ορισμός 2.15. Έστω w μια λέξη πλεξίδας. Θα συμβολίζουμε με $\overline{w}$ την αντίστοιχη πλεξίδα που αναπαρίσταται από την w. Δύο λέξεις w, w' που αναπαριστούν την ίδια πλεξίδα θα καλούνται **ισοδύναμες** και θα γράφουμε $w \equiv w'$.

Ορισμός 2.16.

- Θα λέμε ότι μια λέξη w έχει **μήκος** l αν γράφεται ως αλληλουχία l γραμμάτων.
- Για $1 \leqslant p \leqslant q \leqslant l$ η λέξη που προκύπτει από την w αν διαγράψουμε όλα τα γράμματα πριν από τη θέση p και μετά τη θέση q θα καλείται (p, q) **υπολέξη της** w.
- Μια $(1, q)$ υπολέξη της w θα καλείται **πρόθεμα** της w.

2.3.1 Το κεντρικό αποτέλεσμα

Ορισμός 2.17. Έστω w μία μη-κενή λέξη. Θα λέμε ότι το σ_m είναι το **κύριο γράμμα** (main letter) της w αν το $\sigma_m^{\pm 1}$ εμφανίζεται στην w αλλά κανένα άλλο γράμμα $\sigma_i^{\pm 1}$ με $i > m$ δεν εμφανίζεται. Θα λέμε ότι η w είναι **σ-θετική** (αντ. **σ-αρνητική**) αν το κύριο γράμμα σ_m της w εμφανίζεται μόνο θετικά (αντ. αρνητικά). Δηλ. το σ_m εμφανίζεται αλλά όχι το σ_m^{-1}.

Στόχος μας είναι να αποδείξουμε το ακόλουθο θεώρημα:

Θεώρημα 2.6. *Κάθε λέξη πλεξίδας είναι ισοδύναμη με μία λέξη w η οποία είναι είτε η κενή, είτε σ-θετική είτε σ-αρνητική*

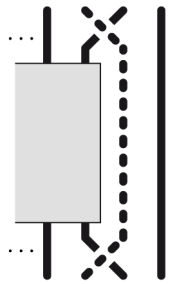
Η απόδειξη του παραπάνω θεωρήματος είναι μακροσκελής και βασίζεται στον ακόλουθο ορισμό, καθώς και σε μια σειρά από ισοδύναμες προτάσεις και λήμματα. Στο τέλος αυτής της παραγράφου θα δούμε πως το συγκεκριμένο θεώρημα συνδέεται άμεσα με την ύπαρξη μιας ολικής διάταξης στην B_n.

Ορισμός 2.18.

- Θα λέμε ότι μια λέξη πλεξίδας v είναι μια **σ_i-λαβή** προσήμου + (αντ. -) αν η v είναι της μορφής $\sigma_i u \sigma_i^{-1}$ (αντ. $\sigma_i^{-1} u \sigma_i$) με την u να μην περιέχει κανένα γράμμα $\sigma_j^{\pm 1}$ με $j \geqslant i$. Βλ. Σχ. 2.3.
- Θα λέμε ότι η v είναι μια **καλή σ_i-λαβή** αν επιπλέον τουλάχιστον ένα από τα γράμματα $\sigma_{i-1}, \sigma_{i-1}^{-1}$ δεν εμφανίζεται. Δηλ. αν η v δεν περιέχει καμία σ_{i-1}-λαβή.

Με βάση τον παραπάνω ορισμό θα διατυπώσουμε μια πρόταση ισοδύναμη του Θεωρήματος 2.6:

Πρόταση 2.2. *Κάθε λέξη πλεξίδας w με κύριο γράμμα το σ_m είναι ισοδύναμη με μιά λέξη w' που δεν περιέχει σ_m-λαβή.*



Σχήμα 2.3: Μια σ_i^{-1}-λαβή

Πράγματι, είναι φανερό από τον ορισμό της σ_i-λαβής ότι αν μία λέξη δεν περιέχει μια σ_m-λαβή τότε το κύριο της γράμμα σ_m θα εμφανίζεται είτε μόνο θετικά είτε μόνο αρνητικά είτε δεν θα έχει κύριο γράμμα και κατ' επέκταση θα είναι η κενή λέξη.

Κάθε λέξη που περιέχει μία λαβή, περιέχει και μία καλή λαβή. Ο ισχυρισμός αυτός αποδεικνύεται στη συνέχεια με τη βοήθεια του επόμενου ορισμού και του ακόλουθου λήμματος.

Ορισμός 2.19. Έστω μια λέξη w. Θα λέμε ότι η v είναι η **πρώτη λαβή** στην w αν η v είναι λαβή και υπάρχουν p, q τέτοια ώστε η v είναι μια (p, q)υπολέξη της w και **δεν** υπάρχουν p', q' με $q' < q$ τέτοια ώστε η (p', q')υπολέξη της w να είναι καλή λαβή.

Η πρώτη λαβή σε μια λέξη w είναι αυτή που ολοκληρώνεται πρώτη όταν κανείς ξεκινήσει να διαβάζει την w από τα αριστερά.

Λήμμα 2.5. *Έστω w μια λέξη πλεξίδας που περιέχει τουλάχιστον μια λαβή. Τότε η πρώτη λαβή της w είναι καλή λαβή.*

Απόδειξη. Έστω q το ελάχιστο μήκος τέτοιο ώστε το πρόθεμα w' μήκους q να περιέχει μια λαβή. Από υπόθεση, υπάρχει ένα p τέτοιο ώστε η (p, q)υπολέξη της w να είναι λαβή, έστω $\sigma_i^e u \sigma_i^{-e}$ με $e = \pm 1$. Από κατασκευής, είναι η πρώτη λαβή της w. Ισχυριζόμαστε ότι αυτή η λαβή (πρώτη) είναι καλή λαβή. Πράγματι, έστω ότι αυτό δεν ισχύει. Τότε θα υπήρχαν $p', q' < q$ τέτοια ώστε η (p', q')υπολέξη της w να είναι μία σ_{i-1}-λαβή, το οποίο σημαίνει ότι το πρόθεμα μήκους q' της w περιέχει μία λαβή. Άτοπο λόγω αρχικής επιλογής του q.

□

Η επόμενη πρόταση είναι ισοδύναμη με την Πρόταση 2.2 και συνεπώς ισοδύναμη με το Θεώρημα 2.6.

Πρόταση 2.3. *Κάθε λέξη πλεξίδας είναι ισοδύναμη με μια λέξη που δεν περιέχει καλή λαβή.*

Πράγματι, από τα μέχρι τώρα, παρατηρούμε ότι αν μία λέξη δεν περιέχει καλή λαβή τότε δεν περιέχει και πρώτη λαβή συνεπώς δεν περιέχει καμία λαβή. Αυτή είναι η τρίτη ισοδύναμη πρόταση που διατυπώνουμε προκειμένου να οδηγηθούμε στο επιθυμητό αποτέλεσμα. Μετά την ανάλυση της παρακάτω μεθόδου θα οδηγηθούμε σε μία τέταρτη ισοδύναμη πρόταση, της οποίας η απόδειξη θα μας δώσει το ζητούμενο.

2.3.2 Handle Reduction

Η μέθοδος handle reduction παρουσιάστηκε πρώτη φορά στο άρθρο του P. Dehornoy "A Fast Method for Comparing Braids" [11]. Η μέθοδος αυτή έχει ποικίλες ισοδύναμες μορφές. Εδώ θα ασχοληθούμε με αυτή που αναπτύσσεται στο [12]. Στόχος μας είναι να απαλλαγούμε από τις καλές λαβές. Θα το επιτύχουμε αυτό μέσα από μία επαναληπτική διαδικασία που την ονομάζουμε αναγωγή λαβών - **handle reduction**, η οποία ξεκινάει αντικαθιστώντας την πρωτη λαβή και επαναλαμβάνεται μέχρι να μην έχει μείνει καμία λαβή.

Ορισμός 2.20. (i) Έστω ότι η v είναι μια καλή σ_i-λαβή, $v = \sigma_i^e u \sigma_i^{-e}$. Η **αναγωγή** (reduct) της v ορίζεται ως η λέξη που λαμβάνουμε από την $\boldsymbol{u}$ αντικαθιστώντας κάθε γράμμα σ_{i-1} με $\sigma_{i-1}^{-e}\sigma_i\sigma_{i-1}^{e}$ και κάθε γράμμα σ_{i-1}^{-1} με $\sigma_{i-1}^{-e}\sigma_i^{-1}\sigma_{i-1}^{e}$. Βλ. Σχήμα 2.4

(ii) Έστω w μια λέξη που περιέχει τουλάχιστον μια λαβή. Θα συμβολίζουμε με $\boldsymbol{red(w)}$ τη λέξη που προκύπτει από την w αν αντικαταστήσουμε την πρώτη λαβή της w με την ανάγωγή της.

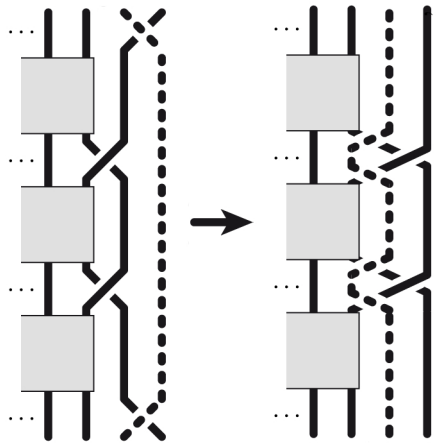
(iii) Θα γράφουμε $\boldsymbol{red^k(w)}$ για $\underbrace{red(red(...red(w))...)}_{\text{k φορές}}$ δηλαδή την λέξη που προκύπτει αν επαναλάβουμε την διαδικασία handle reduction k φορές. Κάθε λέξη της μορφής $red^k(w)$ θα λέμε ότι προκύπτει από την w μέσω της μεθόδου ***first handle reduction***.[2]

Παρατήρηση 2.2. Κάθε λέξη της μορφής $\sigma_i\sigma_i^{-1}$ και $\sigma_i^{-1}\sigma_i$ είναι μία καλή λαβή και η αναγωγή της είναι η κενή λέξη. Συνεπώς μπορούμε να πούμε ότι η handle reduction επεκτείνει την free group reduction.

Λήμμα 2.6. *Κάθε καλή λαβή είναι ισοδύναμη με την αναγωγή της.*

Απόδειξη. Στο επόμενο σχήμα είναι σχεδόν φανερό γιατί ισχύει το παραπάνω. Ωστόσο μια πιό αυστηρή απόδειξη, θα δώσουμε στο Λήμμα 2.10, όπου ο αναγνώστης θα μπορέσει να διαπιστώσει και αλγεβρικά τον παραπάνω ισχυρισμό. □

[2] Για λόγους συντομίας στη συνέχεια του κειμένου θα καλούμε τη μέθοδο handle reduction, παρ'ολα αυτά ο Dehornoy έχει διατυπώσει ισοδύναμες μεθόδους που δεν ξεκινούν με την πρώτη λαβή. Ο ενδιαφερόμενος αναγνώστης μπορεί να βρεί περισσότερα στο [13].



Σχήμα 2.4: handle reduction

Το Θεώρημα 2.6 προκύπτει από την σύγκλιση (τερματισμό) της μεθόδου first handle reduction όπως διατυπώνεται στην παρακάτω πρόταση, η οποία είναι και η τελευταία ισοδύναμη που διατυπώνουμε προκειμένου να αποδείξουμε το Θεώρημα:

Πρόταση 2.4. *Για κάθε λέξη w υπάρχει k τέτοιο ώστε η $red^k(w)$ να μην περιέχει καμμία λαβή.*

Στην συνέχεια θα αποδείξουμε την παραπάνω πρόταση βασιζόμενοι σε τρία λήμματα και σε μερικούς χρήσιμους ορισμούς.

Παρατηρούμε ότι για κάθε n η ταυτοτική απεικόνιση στο $\{\sigma_1, \dots, \sigma_{n-1}\}$ επάγει μία εμφύτευση της B_n στην B_{n+1}, τέτοια ώστε οι ομάδες B_n να διαρθρώνουν φυσιολογικά ένα επαγωγικό σύστημα ομάδων. Το ευθύ όριό τους συμβολίζεται με $\boldsymbol{B_\infty}$. Η B_∞ είναι η ομάδα που παράγεται από το άπειρο σύνολο $\{\sigma_1, \sigma_2, \dots\}$ και διατηρεί τις σχέσεις πλεξίδων.

Παράδειγμα 2.1. Θα δώσουμε ένα παράδειγμα της μεθόδου handle redu-

ction σε μία πλεξίδα της B_4 καθώς και το αντίστοιχο σχήμα (βλ. Σχήμα 2.5):

$$\begin{aligned}
w &= \underline{\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3^{-1}}\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\\
red(w) &= \sigma_2^{-1}\sigma_3\underline{\sigma_2\sigma_1\sigma_2^{-1}}\sigma_3\sigma_2\sigma_2^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\\
red^2(w) &= \sigma_2^{-1}\sigma_3\sigma_1^{-1}\sigma_2\sigma_1\sigma_3\underline{\sigma_2\sigma_2^{-1}}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\\
red^3(w) &= \sigma_2^{-1}\sigma_3\sigma_1^{-1}\sigma_2\sigma_1\underline{\sigma_3\sigma_3^{-1}}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\\
red^4(w) &= \sigma_2^{-1}\sigma_3\sigma_1^{-1}\underline{\sigma_2\sigma_1\sigma_2^{-1}}\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\\
red^5(w) &= \sigma_2^{-1}\sigma_3\sigma_1^{-1}\sigma_1^{-1}\sigma_2\underline{\sigma_1\sigma_1^{-1}}\sigma_2^{-1}\sigma_3^{-1}\\
red^6(w) &= \sigma_2^{-1}\sigma_3\sigma_1^{-1}\sigma_1^{-1}\underline{\sigma_2\sigma_2^{-1}}\sigma_3^{-1}\\
red^7(w) &= \sigma_2^{-1}\underline{\sigma_3\sigma_1^{-1}\sigma_1\sigma_3^{-1}}\\
red^8(w) &= \sigma_2^{-1}\sigma_1^{-1}\sigma_1^{-1}
\end{aligned}$$

Παρατηρούμε ότι τελικά έχουμε μία σ_2-αρνητική λέξη.

2.3.3 Το κεντρικό Λήμμα Α

Ορισμός 2.21. Έστω $X \subseteq B_\infty$ και $a \in X$. Θα λέμε ότι μια λέξη πλεξίδας w **προέρχεται από την a στο X**, αν για κάθε πρόθεμα u της w η πλεξίδα $a\bar{u} \in X$

Παρατηρούμε ότι ακόμα και αν το X είναι πεπερασμένο, λέξεις τυχαίου μήκους μπορεί να προέρχονται από το X. Για παράδειγμα αν $X = \{\epsilon, \sigma_1\}$, τότε $\forall k \in \mathbb{Z}$ η λέξη $(\sigma_1\sigma_1^{-1})^k$ προέρχεται από το X.

Ορισμός 2.22.

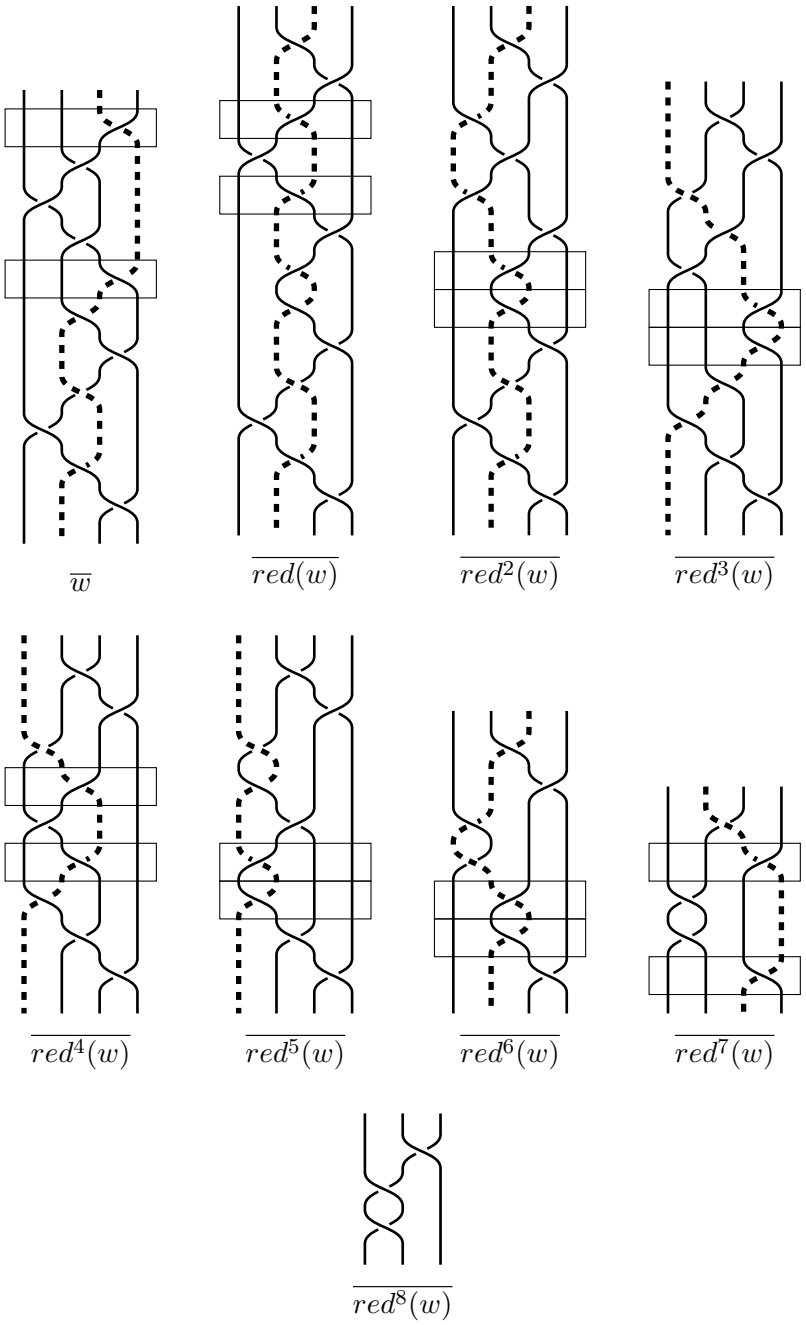
- Αν a, b πλεξίδες, θα λέμε ότι η a είναι **αριστερός διαιρέτης** της b και θα συμβολίζουμε με $\boldsymbol{a \preccurlyeq b}$ αν για κάποια $x \in B_\infty^+$ ισχύει $b = ax$.
- Για $b \in B_\infty^+$ θα συμβολίζουμε με $\boldsymbol{Div(b)}$ το σύνολο όλων των αριστερών διαιρετών της b στην B_∞^+

$$Div(b) = \{a \in B_\infty^+ : 1 \preccurlyeq a \preccurlyeq b\}$$

Λήμμα 2.7 (Κεντρικό Λήμμα Α). *Για κάθε λέξη πλεξίδας w υπάρχουν δύο θετικές πλεξίδες a, b τέτοιες ώστε κάθε λέξη της μορφής $red^k(w)$ να προέρχεται από την a στο $Div(b)$. Ισοδύναμα: $\exists x \in B_\infty^+ : b = a\bar{u}x, \forall$ πρόθεμα u της $red^k(w)$.*

Η απόδειξη του Λήμματος 2.7 βασίζεται στα δύο παρακάτω βοηθητικά λήμματα.

Λήμμα 2.8. *Για κάθε λέξη w, υπάρχουν δύο θετικές πλεξίδες a, b τέτοιες ώστε η w να προέρχεται από την a στο $Div(b)$.*



Σχήμα 2.5: Παράδειγμα της μεθόδου handle reduction

Απόδειξη. Έστω ότι η w έχει μήκος l και κεντρικό γράμμα το σ_m. Για $p \leqslant l$ έστω w_p το πρόθεμα μήκους p της w. Ο Garside έχει δείξει ότι $\forall p$, υπάρχουν ακέραιοι $d_p, e_p \geqslant 0$ τέτοιοι ώστε $1 \preccurlyeq \Delta_{n+1}^{d_p}\overline{w_p} \preccurlyeq \Delta_{n+1}^{d_p+e_p}$. Έστω $d := max\{d_1, \ldots, d_p\}, e := max\{e_1, \ldots, e_p\}$. Τότε για κάθε p έχουμε: $1 \preccurlyeq \Delta_{n+1}^{d}\overline{w_p} \preccurlyeq \Delta_{n+1}^{d+e}$ το οποίο για $a = \Delta_{n+1}^{d}$ και $b = \Delta_{n+1}^{d+e}$ συνεπάγεται ότι η w προέρχεται από την a στο $Div(b)$. □

Λήμμα 2.9. *Έστω ότι η w προέρχεται από την a στο $Div(b)$. Τότε εάν η $red(w)$ υπάρχει, προέρχεται και αυτή από την a στο $Div(b)$.*

Η απόδειξη του Λήμματος 2.9 συνίσταται στην ανάλυση της μεθόδου handle reduction σε πιο απλούς μετασχηματισμούς, που επι της ουσίας αποτελούν τις σχέσεις πλεξίδων και στο να δείξουμε ότι το σύνολο των λέξεων που προέρχονται από την a στο $Div(b)$ είναι κλειστό μέσω αυτών των μετασχηματισμών. Ο ορισμός των μετασχηματισμών αυτών μαζί με τα ακόλουθα δύο λήμματα ολοκληρώνει την απόδειξη του Λήμματος 2.7

Ορισμός 2.23. Έστω w, w' λέξεις. Θα λέμε ότι η w' προκύπτει από την w μέσω του μετασχηματισμού τύπου 1, 2, 3 ή 4 αν η w' προκύπτει από την w αντικαθιστώντας κάποια από τις παρακάτω υπολέξεις με την αντίστοιχή της.

- **τύπος 1**: $\sigma_i\sigma_j \mapsto \sigma_j\sigma_i$ με $|i-j| \geqslant 2$.
- **τύπος 2**: $\sigma_i^{-1}\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma_i^{-1}$ με $|i-j| \geqslant 2$.
- **τύπος 3**: $\sigma_i^{-1}\sigma_j \mapsto \sigma_j\sigma i^{-1}$ με $|i-j| \geqslant 2$.
  ή $\sigma_i^{-1}\sigma_j \mapsto \sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1}$ με $|i-j| = 1$.
  ή $\sigma_i^{-1}\sigma_i \mapsto \epsilon$.
- **τύπος 4**: $\sigma_i\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma i$ με $|i-j| \geqslant 2$.
  ή $\sigma_i\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i$ με $|i-j| = 1$.
  ή $\sigma_i\sigma_i^{-1} \mapsto \epsilon$.

Λήμμα 2.10. *Από κάθε λέξη w, τέτοια ώστε να υπάρχει η $red(w)$ μπορεί να μεταβεί κανείς από την w στην $red(w)$ μέσω μιας πεπερασμένης ακολουθίας των μετασχηματισμών 1-4.*

Απόδειξη. Αρκεί να δείξουμε ότι αν η v είναι μια καλή λαβή και η v' η ανάγωγή της, μπορεί να μεταβεί κανείς από την v στην v' μέσα από μία πεπερασμένη ακολουθία των μετασχηματισμών τύπου 1-4. Εξ' ορισμού υπάρχουν εκθέτες $d, e = \pm 1$, τέτοιοι ώστε η v να είναι της μορφής:

$$v = \sigma_i^e u_0 \underline{\sigma_{i-1}^d} u_1 \underline{\sigma_{i-1}^d} \ldots u_{r-1} \underline{\sigma_{i-1}^d} u_r \sigma_i^{-e}$$

όπου οι λέξεις $u_0 \ldots u_r$ περιέχουν μόνο γράμματα της μορφής σ_j με $i - j \geqslant 2$ και τότε από handle reduction έχουμε:

$$v' = u_0 \underline{\sigma_{i-1}^{-e}\sigma_i^d\sigma_{i-1}^e} u_1 \underline{\sigma_{i-1}^{-e}\sigma_i^d\sigma_{i-1}^e} \ldots u_{r-1} \underline{\sigma_{i-1}^{-e}\sigma_i^d\sigma_{i-1}^e} u_r$$

Υποθέτουμε αρχικά ότι $d = 1$ και $e = -1$ και οι λέξεις v, v' γίνονται:

$$v = \sigma_i^{-1} u_0 \sigma_{i-1} u_1 \dots u_{r-1} \sigma_{i-1} u_r \sigma_i$$

$$v' = u_0 \sigma_{i-1} \sigma_i \sigma_{i-1}^{-1} u_1 \dots u_{r-1} \sigma_{i-1} \sigma_i \sigma_{i-1}^{-1} u_r$$

Η ιδέα είναι να χρησιμοποιήσουμε τους μετασχηματισμούς 2 και 3 προκειμένου να μεταφέρουμε το αρχικό γράμμα σ_i^{-1} της v στο τέλος.

- Αρχικά το σ_i^{-1} περνάει την u_0 χρησιμοποιώντας τον μετασχηματισμό 3 (i) για τα θετικά γράμματα και τον μετασχηματισμό 2 για τα αρνητικά. Έτσι έχουμε:
$$u_0 \underline{\sigma_i^{-1}} \sigma_{i-1} u_1 \dots u_{r-1} \sigma_{i-1} \sigma_i$$
- Με χρήση του μετασχηματισμού 3 (ii) έχουμε:
$$u_0 \sigma_{i-1} \sigma_i \sigma_{i-1}^{-1} \underline{\sigma_i^{-1}} u_1 \dots u_{r-1} \sigma_{i-1} u_r \sigma_i$$
- Επαναλαμβάνοντας την ίδια διαδικασία r φορές έχουμε:
$$u_0 \sigma_{i-1} \sigma_i \sigma_{i-1}^{-1} u_1 \dots u_{r-1} \sigma_{i-1} \sigma_i \sigma_{i-1}^{-1} u_r \underline{\sigma_i^{-1}} \sigma_i$$
- Εφαρμόζοντας τώρα για τελευταία φορά τον μετασχηματισμό 3 (iii) παίρνουμε την λέξη v'.

Για τις υπόλοιπες περιπτώσεις των d, e τα επιχειρήματα είναι παρόμοια και αποδεικνύεται εύκολα ότι με χρήση μόνο των προαναφερθέντων μετασχηματισμών φτάνουμε στην ζητούμενη λέξη □

Λήμμα 2.11. *Έστω ότι η λέξη w προέρχεται από την a στο $Div(b)$ και η w' προκύπτει από την w μέσω των μετασχηματισμών 1-4. Τότε και η w' προέρχεται από την a στο $Div(b)$.*

Απόδειξη. Έστω λέξη w η οποία προέρχεται από την a στο $Div(b)$. Θα εξετάσουμε την περίπτωση η w' να προέρχεται από τον μετασχηματισμό 1, για τους υπόλοιπους μετασχηματισμούς η απόδειξη είναι παρόμοια και ακολουθούνται τα ίδια επιχειρήματα. Έστω ότι η w' προκύπτει από την w μέσω του μετασχηματισμού 1, δηλ. $\exists\, w_1$, w_2 λέξεις τέτοιες ώστε:

$$w = w_1 \sigma_i \sigma_j w_2 \text{ και } w' = w_1 \sigma_j \sigma_i w_2$$

Θα δείξουμε ότι για κάθε πρόθεμα u της w' η $a\bar{u} \in Div(b)$.
Από κατασκευή κάθε πρόθεμα της w' είναι και πρόθεμα της w εκτός της $u_1 = w_1 \sigma_j$. Αρκεί να δείξουμε ότι $1 \preccurlyeq a\overline{u_1} \preccurlyeq b$. Έστω $c = a\overline{w_1}$ και $d = a\overline{w_1}\sigma_i\sigma_j$. Λόγω κατασκευής έχουμε: $c \preccurlyeq a\overline{u_1} \preccurlyeq d$. Πράγματι:

$$a\overline{w_1} \preccurlyeq a\overline{w_1\sigma_j} \preccurlyeq a\overline{w_1\sigma_j\sigma_i}$$

$$a\overline{w_1} \preccurlyeq a\overline{w_1\sigma_j} \preccurlyeq a\overline{w_1\sigma_i\sigma_j} \text{ (από σχέσεις πλεξίδων)}$$

Είναι προφανές ότι $1 \preccurlyeq c$. Θα δείξουμε ότι $d \preccurlyeq b$. Επειδή η w πρόερχεται από την a στο $Div(b)$ έχουμε ότι $\forall$ πρόθεμα u της $w : a\bar{u} \preccurlyeq b$. Επίσης έχουμε ότι $d = \overline{w_1}\sigma_i\sigma_j$. Θέτουμε $u_2 = w_1\sigma_i\sigma_j$, τότε το u_2 είναι πρόθεμα της w και άρα $a\bar{u_2} \preccurlyeq b$, που συνεπάγεται ότι $d \preccurlyeq b$. Παραλείπουμε την απόδειξη για τους άλλους τρείς μετασχηματισμούς καθώς είναι παρόμοια. □

Απόδειξη του Λήμματος Α (2.7). Έστω w λέξη. Τότε από Λήμμα 2.8 υπάρχουν δύο θετικές πλεξίδες a, b τέτοιες ώστε η w να προέρχεται από την a στο $Div(b)$. Επίσης, από Λήμμα 2.11, αν η w προέρχεται από την a στο $Div(b)$ και η w' προκύπτει από την w μέσω των μετασχηματισμών 1-4 τότε και η w' προέρχεται από την a στο $Div(b)$. Τέλος, από το Λήμμα 2.10 έχουμε ότι για κάθε λέξη w, η $red(w)$ όταν υπάρχει μπορεί να προκύψει μέσω των μετασχηματισμών 1-4. Άρα η $red(w)$ προέρχεται από την a στο $Div(b)$. Επαγωγικά: αν η $red^n(w) = w_n$ προέρχεται από την a στο $Div(b)$ τότε και η $red^{n+1}(w) = red(w_n)$ προέρχεται από την a στο $Div(b)$ και το ζητούμενο έχει αποδειχθεί. □

2.3.4 Το κεντρικό Λήμμα Β

Το λήμμα που ακολουθεί μας επιτρέπει να μετατρέψουμε την γεωμετρική κλειστότητα του Λήμματος 2.7 σε ένα αποτέλεσμα τερματισμού της μεθόδου handle reduction. Δηλαδή θα δείξουμε ότι όλες οι λέξεις που προκύπτουν από την handle reduction παραμένουν "drawn in" σε κάποιο πεπερασμένο υποσύνολο του μονοειδούς B_∞.

Λήμμα 2.12 (Κεντρικό Λήμμα Β). *Μία σ-θετική λέξη δεν είναι ισοδύναμη με την κενή.*

Εδώ θα πρέπει να σημειώσουμε ότι στην συγκεκριμένη παράγραφο θα θεωρήσουμε ως κύριο γράμμα αυτό με τον ελάχιστο δείκτη και όχι αυτό με τον μέγιστο όπως προηγουμένως. Αυτη η αλλαγή δεν θα επηρεάσει το τελικό μας αποτέλεσμα αλλά μας είναι χρήσιμη προκειμένου να ακολουθήσουμε την απόδειξη του Dehornoy όπως αυτή περιγράφεται στο πέμπτο κεφάλαιο του [14].

Πόρισμα 2.3. *Έστω a, b θετικές πλεξίδες και w μια σ-θετική λέξη που προέρχεται από την a στο $Div(b)$. Τότε ο αριθμός των εμφανίσεων του κύριου γράμματος της w είναι το πολύ ίσος με την πληθικότητα του $Div(b)$.*

Απόδειξη. Έστω ότι το σ_m εμφανίζεται r φορές στην w και έστω $\sigma_{m_1}, \ldots, \sigma_{m_r}$ οι r εμφανίσεις του σ_m. Έστω επίσης $u_1, \ldots, u_r$ τα προθέματα της w τέτοια

ώστε κάθε u_j τελειώνει ακριβώς πριν το j-οστό σ_m στην w.

$$w = \underbrace{\underbrace{\underbrace{v_1}_{u_1}\,\sigma_{m_1} v_2\,\sigma_{m_2} v_3\,\sigma_{m_3}}_{u_2}}_{u_3}$$

Από υπόθεση όλες οι πλεξίδες $a\bar{u}$ ανήκουν στο $Div(b)$. Προφανώς αν $j < j'$ συνεπάγεται ότι $a\overline{u_j} \neq a\overline{u_{j'}}$. Πράγματι από κατασκευή έχουμε $u_{j'} = u_j v$, όπου η v περιέχει τουλάχιστον ένα σ_m και κανένα σ_m^{-1} έτσι από Λήμμα Β έχουμε $\bar{v} \neq 1$. Έτσι οι πλεξίδες $a\overline{u_1}, a\overline{u_2}, \ldots, a\overline{u_r}$ είναι ανά δύο διαφορετικά στοιχεία του $Div(b)$ και άρα $r \leqslant card(Div(b))$. □

Η απόδειξη του Λήμματος Β που θα προσπαθήσουμε να περιγράψουμε παρακάτω βασίζεται σε αυτήν που ο ίδιος ο P. Dehornoy παρουσιάζει στο [14]. Η ίδια η απόδειξη είναι εξαιρετικά συνοπτική αλλά βασίζεται σε μια σειρά από λήμματα και ορισμούς. Η γενική ιδέα είναι να αποδείξουμε ότι αν μια λέξη πλεξίδας w περιέχει τουλάχιστον ένα γράμμα σ_1 και κανένα σ_1^{-1}, τότε ο αντίστοιχος αυτομορφισμός που θα ορίσουμε παρακάτω δεν είναι ο ταυτοτικός και άρα η λέξη w δεν μπορεί να αναπαριστά την μοναδιαία πλεξίδα.

Για $1 \leqslant n < \infty$ θα συμβολίζουμε με $\boldsymbol{F_n}$ την ελεύθερη ομάδα τάξης n με γεννήτορες τα $\{x_1, \ldots, x_n\}$ και με $\boldsymbol{F_\infty}$ την ελεύθερη ομάδα με γεννήτορες τα $\{x_i, 1 \leqslant i < \infty\}$.

Ορισμός 2.24. Για $i < n$, θα συμβολίζουμε με $\hat{\boldsymbol{\sigma_i}}$ τον αυτομορφισμό της F_n που ορίζεται ώς:

$$\hat{\sigma}_i(x_k) = \begin{cases} x_i x_{i+1} x_i^{-1} & \text{για } k = i \\ x_i & \text{για } k = i+1 \\ x_k & \text{για } k \neq i, i+1 \end{cases} \tag{2.7}$$

Λήμμα 2.13. *Για $1 \leqslant n < \infty$ η απεικόνιση $\sigma_i \mapsto \hat{\sigma}_i$ επεκτείνεται σε έναν ομομορφισμό ϕ, της B_n στην $Aut(F_n)$.*

Απόδειξη. Το παραπάνω λήμμα είναι αρκετά γνωστό στην βιβλιογραφία. Αρκεί να δείξει κανείς ότι τα $\hat{\sigma}_i$ ικανοποιούν τις σχέσεις πλεξίδων, δηλαδή:

$$\hat{\sigma}_i\hat{\sigma}_j(x_k) = \hat{\sigma}_j\hat{\sigma}_i(x_k), \text{ για } |i-j| \geqslant 2 \text{ και } \forall\, k$$
$$\hat{\sigma}_i\hat{\sigma}_j\hat{\sigma}_i(x_k) = \hat{\sigma}_j\hat{\sigma}_i\hat{\sigma}_j(x_k), \text{ για } |i-j| = 1 \text{ και } \forall\, k$$

τα οποία είναι απλά θέμα υπολογισμών. □

Για κάθε πλεξίδα β, θα συμβολίζουμε με $\hat{\boldsymbol{\beta}}$ τον αντίστοιχο αυτομορφισμό, ενώ για κάθε λέξη πλεξίδας w, θα συμβολίζουμε με $\hat{\boldsymbol{w}}$ τον αυτομορφισμό που

αντιστοιχεί στην πλεξίδα που αναπαρίσταται από την w.

Για κάθε n, η ταυτοτική απεικόνιση στο σύνολο των γεννητόρων σ_i επάγει μια εμφύτευση της B_n στην B_{n+1} τέτοια ώστε να μπορούμε να θεωρήσουμε κάθε n-πλεξίδα ως μια ειδική περίπτωση $(n+1)$-πλεξίδας. Με τον ίδιο τρόπο θεωρούμε και την εμφύτευση της $Aut(F_n)$ στην $Aut(F_{n+1})$ και έτσι δεν χρειάζεται από εδώ και στο εξής να προσδιορίσουμε κάποιο n, θα δουλέψουμε με τις B_∞ και F_∞.

Στην συνέχεια θα μελετήσουμε τις εικόνες των σ-θετικών λέξεων και θα δείξουμε ότι αν η β έχει τουλάχιστον μία σ-θετική λέξη w που την αναπαριστά, τότε ο αυτομορφισμός $\hat{\beta}$ έχει κάποιες συγκεκριμένες ιδιότητες που μπορούν να βρεθούν στις λέξεις $\hat{\beta}(x_i)$.

Ορισμός 2.25. Θα λέμε ότι μια λέξη u είναι **ανηγμένη** αν δεν περιέχει καμία υπολέξη της μορφής $x_i x_i^{-1}$ ή $x_i^{-1} x_i$ και θα συμβολίζουμε με $\boldsymbol{r(u)}$ τη μοναδική ανηγμένη λέξη που προκύπτει από την u έπειτα από διαδοχικές διαγραφές των υπολέξεων της μορφής $x_i x_i^{-1}$ και $x_i^{-1} x_i$.

Από εδώ και στο εξής θα ταυτίσουμε το σύνολο F_∞ με το σύνολο όλων των ανηγμένων λέξεων των $x_1^{\pm 1}, x_2^{\pm 1}, \ldots$.

Ορισμός 2.26. Έστω x ένα τυχαίο γράμμα x_i ή x_i^{-1}, θα συμβολίζουμε με $\boldsymbol{S(x)}$ το υποσύνολο της F_∞ που αποτελείται από όλες τις ελεύθερα ανηγμένες λέξεις που τελειώνουν με το γράμμα x.

Θα εξετάσουμε την εικόνα του συνόλου $S(x_1^{-1})$ μέσω του αυτομορφισμού $\widehat{\sigma_i}^{\pm 1}$.

Ορισμός 2.27. Θα συμβολίζουμε με $\boldsymbol{sh} : F_\infty \mapsto F_\infty$ τον ενδομορφισμό που απεικονίζει $x_k^{\pm 1}$ στο $x_{k+1}^{\pm 1}$ για κάθε k. Έστω $f \in Aut(F_\infty)$ θα συμβολίζουμε με $\boldsymbol{sh(f)}$ τον αυτομορφισμό της F_∞ που ορίζεται ως εξής:

$$sh(f)(x_1) = x_1$$
$$sh(f)(x_{k+1}) = sh(f(x_k))$$

Λήμμα 2.14. *Κάθε αυτομορφισμός $sh(f)$ απεικονίζει το $S(x_1^{-1})$ στον εαυτό του*

Απόδειξη. Έστω λέξη $w = ux_1^{-1} \in S(x_1^{-1})$. Προφανώς έχουμε ότι $u \notin S(x_1)$ γιατί διαφορετικά θα είχαμε $w = u' x_1 x_1^{-1} = u$ και άρα η w δεν θα ανήκε στο $S(x_1^{-1})$ γιατί δεν θα ήταν ανηγμένη.
Από κατασκευής και λόγω υπόθεσης έχουμε:

$$sh(f)(ux_1^{-1}) = r(sh(f)(u) \cdot x_1^{-1})$$

Πράγματι:

$$\begin{aligned} sh(f)(ux_1^{-1}) &= sh(f)(u) \cdot sh(f)(x_1^{-1}) \\ &= sh(f)(u) \cdot x_1^{-1} \\ &= r(sh(f)(u) \cdot x_1^{-1}), \text{ γιατί αλλιώς } u \in S(x_1) \end{aligned}$$

Έστω ότι $sh(f)(ux_1^{-1}) = sh(f)(u)x_1^{-1} \notin S(x_1^{-1})$.
Τότε το τελικό γράμμα x_1^{-1} στην $sh(f)(u)x_1^{-1}$ φεύγει από κάποιο γράμμα x_1 στην $sh(f)(u)$, το οποίο θα προέρχεται από κάποιο x_1 στην u. Άρα υπάρχει μιά ανάλυση της u ως εξής: $u = u_1x_1u_2$ με $sh(f)(u_2) = \varepsilon \xrightarrow{sh(f) \in Aut(F_\infty)} u_2 = \varepsilon$ και άρα $u \in S(x_1)$. Άτοπο. □

Λήμμα 2.15. *Ο αυτομορφισμός $\widehat{\sigma_i}$ απεικονίζει τα σύνολα $S(x_i)$ και $S(x_i^{-1})$ στο $S(x_i^{-1})$.*

Απόδειξη. Έστω μία λέξη $w = ux_i^e \in S(x_i) \cup S(x_i^{-1})$ με $e = \pm 1$ και $u \notin S(x_i^{-e})$. Τότε από τις σχέσεις 2.7 έχουμε: $\widehat{\sigma_i}(ux_i^e) = r(\widehat{\sigma_i}(u)x_ix_{i+1}^ex_i^{-1})$. Έστω ότι $\widehat{\sigma_i}(ux_i^e) \notin S(x_i^{-1})$.
Αυτό σημαίνει ότι το τελευταίο γράμμα x_i^{-1} στο $\widehat{\sigma_i}(ux_i^e)$ διαγράφεται από κάποιο $x_i \in \widehat{\sigma_i}(u)$, το οποίο θα προέρχεται είτε από κάποιο x_{i+1} ή από κάποιο $x_i^{e'}$ στην u.

- Έστω ότι το x_i προέρχεται από κάποιο x_{i+1} στην u, τότε: $u = u_1x_{i+1}u_2$ όπου η u_2 είναι ανηγμένη λέξη και έχουμε:

  $$\widehat{\sigma_i}(ux_i^e) = r(\widehat{\sigma_i}(u_1)x_i\underline{\widehat{\sigma_i}(u_2)x_ix_{i+1}^e}x_i^{-1})$$

  Τότε από υπόθεση θα πρέπει: $r(\widehat{\sigma_i}(u_2)x_ix_{i+1}^e) = \varepsilon \implies$

  $$\begin{aligned} \widehat{\sigma_i}(u_2) &= x_{i+1}^{-e}x_i^{-1} \\ &= \widehat{\sigma_i}(x_{i+1}^{-1}x_i^{-e}). \end{aligned}$$

  Δηλαδή, $u_2 = x_{i+1}^{-1}x_i^{-e}$ το όποίο συνεπάγεται ότι $u \in S(x_i^{-e})$ το οποίο είναι άτοπο από υπόθεση.

- Έστω τώρα ότι το γράμμα x_i προέρχεται από κάποιο $x_i^{e'}$ στην u. Όμοια με προηγουμένως: $u = u_1x_i^{e'}u_2$ με $e' = \pm 1$. Έτσι έχουμε:

  $$\widehat{\sigma_i}(ux_i^e) = r(\widehat{\sigma_i}(u_1)x_i\underline{x_{i+1}^{e'}x_i^{-1}\widehat{\sigma_i}(u_2)x_ix_{i+1}^e}x_i^{-1})$$

  και λόγω υπόθεσης θα πρέπει: $r(x_{i+1}^{e'}x_i^{-1}\widehat{\sigma_i}(u_2)x_ix_{i+1}^e) = \varepsilon \implies$

  $$\begin{aligned} r(\widehat{\sigma_i}(u_2)) &= x_ix_{i+1}^{-e-e'}x_i^{-1} \\ &= \widehat{\sigma_i}(x_i^{-e-e'}) \end{aligned}$$

Άρα $u_2 = x_i^{-e-e'}$. Εξετάζουμε τις τέσσερις διαφορετικές περιπτώσεις για τις διάφορες τιμές των e, e':
Για $e = e' = 1$ έχουμε $u_2 = x_i^{-2}$ και άρα $u = u_1 x_i x_i^{-2} = u_1 x_i^{-e} \in S(x_i^{-e})$ άτοπο.
Για $e = 1$, $e' = 1$ και $e = -1$, $e' = 1$ έχουμε $u_2 = \varepsilon$ και άρα $u = u_1 x_i^{e'} = u_1 x_i^{-e} \in S(x_i^{-e})$ πάλι άτοπο. Και τέλος για $e = e' = -1$ έχουμε $u_2 = x_i^2$ και άρα $u = u_1 x_i^{-e}$ και πάλι άτοπο.

Άρα $\widehat{\sigma_i}(ux_i^e) = \widehat{\sigma_i}(w) \in S(x_i^{-1})$ για κάθε $w \in S(x_i) \cup S(x_i^{-1})$. □

Προκειμένου να ολοκληρώσουμε την απόδειξη του Λήμματος Β θα παραθέσουμε σε αυτό το σημείο μία βοηθητική πρόταση χωρίς την απόδειξή της, η οποία μπορεί να βρεθεί στο [14].

Πρόταση 2.5. *Κάθε πλεξίδα στην B_n μπορεί να αναπαρασταθεί από μία λέξη η οποία είναι είτα σ_1-θετική, είτε σ_1-αρνητική είτε σ_1-ελεύθερη (δηλαδή δεν περιέχει κανένα σ_1).*

Η επόμενη πρόταση έπεται άμεσα από το προηγούμενο λήμμα και την προηγούμενη πρόταση:

Πρόταση 2.6. *Έστω ότι στην πλεξίδα β αντιστοιχεί τουλάχιστον μια σ_1-θετική λέξη που την αναπαριστά, τότε η λέξη $\widehat{\beta}(x_1)$ τελειώνει με το γράμμα x_1^{-1}.*

Απόδειξη. Η υπόθεσή μας βασίζεται στο γεγονός ότι στον αυτομορφισμό $\widehat{\beta}$ αντιστοιχεί μια ανάλυση της μορφής:

$$\widehat{\beta} = sh(f_0) \circ \widehat{\sigma_1} \circ sh(f_1) \circ \widehat{\sigma_1} \circ \cdots \circ \widehat{\sigma_1} \circ sh(f_p)$$

Εξ' ορισμού έχουμε $sh(f_p)(x_1) = x_1 \in S(x_1)\ \forall p$ και $\widehat{\sigma_i}(x_1) = x_1 x_2 x_1^{-1} \in S(x_1^{-1})$.
Από λήμμα 2.15 έχουμε ότι ο αυτομορφισμός $\hat{\sigma_1}$ θα ανοίκει στο $S(x_1^{-1})$ ενώ από λήμμα 2.14 έχουμε ότι $sh(f_{p-1}) \in S(x_1^{-1})$ για κάθε $p \geqslant 1$.
Άρα έχουμε $\widehat{\beta}(x_1) \in S(x_1^{-1})$. □

Σε αυτό το σημείο μπορούμε πλέον να ολοκληρώσουμε την απόδειξη του Λήμματος Β, το οποίο σε συνδυασμό με το Λήμμα Α καθώς και το επόμενο Λήμμα θα μας οδηγήσουν στο ζητούμενο.

Απόδειξη Λήμματος Β (2.12). Έστω μια πλεξίδα β στην οποία αντιστοιχεί μια σ_1-θετική λέξη, τότε ο αυτομορφισμός $\widehat{\beta}$ δεν απεικονίζει το x_1 στο x_1 και άρα δεν είναι ο ταυτοτικός. Άρα η β δεν είναι τετριμμένη και αντίστοιχα δεν είναι τετριμμένη η λέξη που την αναπαριστά. □

2.3.5 Το κεντρικό Λήμμα C

Το τελευταίο Λήμμα που θα παρουσιάσουμε θα μας βοηθήσει να ολοκληρώσουμε την απόδειξη της Πρότασης 2.4 και κατά συνέπεια του Θεωρήματος 2.6. Το παρακάτω Λήμμα είναι ένα αποτέλεσμα μονοτονίας που μας λέει ότι κατά τη διαδικασία της μεθόδου handle reduction, κάποια παράμετρος είτε συνεχώς μειώνεται είτε συνεχώς αυξάνεται. Παρ' όλο που η διατύπωση του Λήμματος μπορεί να φανεί ξένη ως προς τον αρχικο μας στόχο, κατά την ενσωμάτωση του στην ζητούμενη απόδειξη θα φανεί η χρησιμότητά του.

Ορισμός 2.28. Έστω w μία λέξη με κύριο γράμμα το σ_i.

(i) Θα συμβολίζουμε με $\boldsymbol{h(w)}$ τον αριθμό των σ_i-λαβών στην w.
Αν επιπλέον $h(w) \geqslant 1$:

(ii) Θα συμβολίζουμε με $\boldsymbol{e(w)}$ το πρόσημο της πρώτης σ_i-λαβής στην w.

(iii) Θα συμβολίζουμε με $\boldsymbol{\pi(w)}$ το πρόθεμα της w που τελειώνει με το πρώτο γράμμα της πρώτης σ_i-λαβής της w.

Λήμμα 2.16 (Λήμμα C). *Έστω w μία λέξη που προέρχεται από την a στο $Div(b)$, η οποία περιέχει τουλάχιστον μία λαβή, με κεντρικό γράμμα το σ_m και η πρώτη λαβή της w είναι μια σ_i-λαβή. Έστω επιπλέον ότι η w' προκύπτει από την w με την μέθοδο της handle reduction για την πρώτη λαβή της w. Τότε έχουμε τρείς πιθανές περιπτώσεις:*

1. $h(w') = h(w) = 0$ *(η w δεν περιέχει σ_m-λαβές).*
2. $h(w') < h(w)$ *(η πρώτη λαβή της w είναι μια σ_m-λαβή)*
3. $h(w') = h(w) \geqslant 1$ *(η πρώτη λαβή της w δεν είναι μια σ_m-λαβή αλλά περιέχει σ_m-λαβές)*

   Επιπλέον για την περίπτωση 3, έχουμε $e(w') = e(w)$ και υπάρχει λέξη $\gamma(w)$ που ικανοποιεί τα παρακάτω:

   (α') *Η $\gamma(w)$ προέρχεται από την $a\overline{\pi(w)}$ στο $Div(b)$.*
   (β') *Έχουμε $\pi(w') \equiv \pi(w)\gamma(w)$.*
   (γ') *Αν $i < m$, τότε $\gamma(w) = \varepsilon$.*
   (δ') *Αν $i = m$, τότε η $\gamma(w)$ περιέχει ένα γράμμα $\sigma_i^{-e(w)}$ και δεν περιέχει γράμμα $\sigma_i^{e(w)}$.*

Η απόδειξη του Λήμματος είναι τεχνική και αρκετά εκτενής και θα προτιμήσουμε να μην την παρουσιάσουμε εδώ. Ο ενδιαφερόμενος αναγνώστης μπορεί να τη βρεί στο [12].

2.3.6 Η απόδειξη του Θεωρήματος 2.6

Πλέον μπορούμε να αποδείξουμε την Πρόταση 2.4 και κατά συνέπεια το Θεώρημα 2.6.

Απόδειξη Πρότασης 2.4. Υπενθυμίζουμε την πρόταση, την οποία θα αποδείξουμε με επαγωγή στο $m \geqslant 1$:

Για κάθε λέξη w με κεντρικό γράμμα[3] *το σ_m, υπάρχει k τέτοιο ώστε η $red^k(w)$ να μην περιέχει καμία λαβή.(Συνεπώς η $red^{k+1}(w)$ δεν υπάρχει.)*

- Για $m = 1$ τα μόνα πιθανά γράμματα στην w είναι τα σ_1, σ_1^{-1} συνεπώς η μέθοδος handle reduction, είναι επί της ουσίας η αναγωγή των ελεύθερων ομάδων, δηλαδή η αντικατάσταση των $\sigma_1\sigma_1^{-1}$ και $\sigma_1^{-1}\sigma_1$ με την κενή λέξη ε. Το ζητούμενο αποτέλεσμα είναι προφανές με $k \leqslant \frac{l(w)}{2}$. Όπου $l(w)$ το μήκος της λέξης w.

- Έστω $m \geqslant 2$ και έστω με εις άτοπο ότι η w είναι μία λέξη με κεντρικό γράμμα το σ_m τέτοια ώστε η $red^k(w)$ υπάρχει για κάθε k. Για λόγους συντομίας θα συμβολίζουμε με w_k την $red^k(w)$.
  Απο το Λήμμα C, οι αριθμοί $h(w_k)$ φτιάχνουν μια φθίνουσα, τελικά σταθερή ακολουθία. Δηλαδή $\exists\, n \in \mathbb{N}$ τέτοιο ώστε $\forall\, k \geqslant n, h(w_k) = h$.
  Από υπόθεση η w_{k+1} προκύπτει από την w_k διαγράφοντας την πρώτη λαβή της w_k η οποία είναι είτε μια σ_m-λαβή είτε μια σ_i-λαβή για κάποιο $i < m$. Έστω K το σύνολο όλων των k για τα οποία η πρώτη λαβή της w είναι μια σ_m-λαβή.
  - Αρχικά ισχυριζόμαστε ότι το K είναι άπειρο. Πράγματι έστω k ένας οποιοσδήποτε μη αρνητικός ακέραιος. Τότε έχουμε:

$$w_k = v_0\sigma_m^e v_1\sigma_m^e v_2 \dots v_{r-1}\sigma_m^e v_r v$$

  όπου το v είτε ξεκινάει με $\sigma_m^{-e} \Rightarrow h > 0$ είτε είναι η κενή λέξη $\Rightarrow h = 0$. Από κατασκευή, το κεντρικό γράμμα κάθε λέξης v_j είναι κάποιο $\sigma_{m'}$ με $m' < m$. Έτσι από επαγωγική υπόθεση έχουμε ότι για κάθε j έναν ακέραιο k_j τέτοιον ώστε η $red^{k_j}(v_j)$ να μην περιέχει καμία λαβή. Έστω τώρα $k' = k + k_0 + \dots + k_{r-1} + k_r$. Τότε από κατασκευής θα έχουμε:

$$w_{k'} = red^{k_0}(v_0)\sigma_m^e red^{k_1}(v_1)\sigma_m^e \dots red^{k_{r-1}}(v_{r-1})red^{k_r}(v_r)v$$

  Αν η v είναι η κενή λέξη, τότε η $w_{k'}$ δεν θα περιέχει λαβή, το οποίο αντιτίθεται στην αρχική μας υπόθεση ότι η ακολουθία $(w_k)_{k\geqslant 0}$ είναι άπειρη. Άρα η v ξεκινάει με σ_m^{-e} και η πρώτη λαβή της $w_{k'}$ είναι μια σ_m λαβή. Συνεπώς βρήκαμε ένα k' με $k' \geqslant k$ και άρα το K είναι άπειρο.

[3] Να σημειώσουμε σε αυτό το σημείο ότι επιστρέφουμε στον αρχικό μας ορισμό του κεντρικού γράμματος, αυτού δηλαδή με το μέγιστο δείκτη

- Από την άλλη μεριά ισχυριζόμαστε οτι το K είναι πεπερασμένο. Πράγματι, έστω a, b θετικές braids, τέτοιες ώστε η w, καθώς και όλες οι w_k, λόγω λήμματος Α να προέρχονται από την a στο $Div(b)$. Εφαρμόζουμε το Λήμμα C στην w_k και λόγω υπόθεσης είμαστε πάντα στην περίπτωση 3. Έστω e η κοινή τιμή όλων των $e(w_k)$ για κάθε k, και έστω γ η άπειρη λέξη $\gamma(w_0)\gamma(w_1)\ldots$. Από κατασκευή, η λέξη γ προέρχεται από την $a\overline{\pi(w)}$ στο $Div(b)$, δεν περιέχει γράμμα σ_m^e και περιέχει ακριβώς ένα γράμμα σ_m^{-e} για κάθε $k \in K$. Από το Πόρισμα 2.3 του Λήμματος Β έχουμε ότι ο αριθμός τέτοιων γραμμάτων και άρα η πληθικότητα του K είναι το πολύ ίση με την πληθυκότητα του $Div(b)$. Συνεπώς το σύνολο K είναι πεπερασμένο.

Τελικά έχουμε ότι η υπόθεση της ύπαρξης μιας λέξης w με κεντρικό γράμμα το σ_m τέτοια ώστε η $red^k(w)$ να υπάρχει για κάθε k είναι αντιφατική και οδηγεί σε άτοπο.

□

Η απόδειξη της παραπάνω πρότασης οδηγεί άμεσα και στην απόδειξη του Θεωρήματος 2.6 μέσω των αντίστοιχων ισοδύαμων προτάσεων που διατυπώθηκαν κατά τη διάρκεια του κεφαλαίου. Παρατηρούμε ότι αν για κάθε λέξη w, με κεντρικό γράμμα κάποιο σ_m υπάρχει ένα k τέτοιο ώστε η $red^k(w)$ να μην περιέχει κάποια λαβή, τότε προφανώς και δεν θα περιέχει κάποια σ_m-λαβή και κατ' επέκταση θα είναι είτε σ-θετική, είτε σ-αρνητική είτε η κενή.

Το ενδιαφέρον αυτής της πρότασης δεν εξαντλείται στην επίλυση του word problem, αλλά όπως θα δούμε στην συνέχεια, χρησιμεύει στο να ορίσουμε μια (ολική) διάταξη στην Ομάδα Πλεξίδων.

Πρόταση 2.7. *Για δύο οποιεσδήποτε πλεξίδες β, β' θα λέμε ότι $\beta < \beta'$ αν και μόνο αν η λέξη που αναπαριστά την $\beta^{-1}\beta'$ είναι σ-θετική. Η σχέση "$<$" που ορίσαμε είναι μια γραμμική(ολική) διάταξη στην B_∞.*

Η παραπάνω πρόταση διατυπώνεται ως πόρισμα στο [11] το οποίο είναι και το πρώτο άρθρο του Dehornoy που παρουσιάζεται η μέθοδος handle reduction. Παρακάτω θα δείξουμε ότι η σχέση που μόλις ορίσαμε αποτελεί πράγματι μια ολική διάταξη στην B_n.

Ορίζουμε ως **ολική διάταξη** σε ένα σύνολο $\mathbf{\Omega}$ μια σχέση $<$ που ικανοποιεί τα παρακάτω:

(i) Για κάθε $x \in \Omega \ \rightarrow \ x \not< x$.

(ii) Αν $x < y$ και $y < z$ τότε $x < z$.

(iii) Για κάθε x, $x' \in \Omega$ έχουμε είτε $x < x'$ είτε $x' < x$ είτε $x = x'$.

Απόδειξη. Η σχέση $<$ που ορίσαμε ικανοποιεί τις ιδιότητες της ολικής διάταξης.

(i) Έστω β μια πλεξίδα της B_n και έστω ότι ισχύει: $\beta < \beta$ τότε $\beta^{-1}\beta = 1$ είναι σ-θετική, άτοπο γιατί από Λήμμα Β μιά σ-θετική λέξη δεν είναι η κενή. Άρα $\beta \not< \beta$.

(ii) Έστω τώρα β_1, β_2, β_3 πλεξίδες της B_n τέτοιες ώστε να ισχύει: $\beta_1 < \beta_2$ και $\beta_2 < \beta_3$ ισοδύναμα θα έχουμε ότι οι λέξεις που αναπαριστούν τις πλεξίδες $\beta_1^{-1}\beta_2$ και $\beta_2^{-1}\beta_3$ είναι σ-θετικές. Τότε, προφανώς, έχουμε ότι η λέξη που αναπαριστά την $\beta_1^{-1}\beta_3 = \beta_1^{-1}\beta_2\beta_2^{-1}\beta_3$ είναι σ-θετική και άρα $\beta_1 < \beta_3$.

(iii) Από την Πρόταση 4.4 έχουμε ότι το γινόμενο δύο οποιονδήποτε πλεξίδων β, β' μπορεί να αναπαρασταθεί από μία λέξη που είναι είτε σ_1-θετική, είτε σ_1- αρνητική, είτε σ_1-ελεύθερη. Άρα μπορούμε πάντα να πούμε αν ισχύει $\beta < \beta'$.

□

Να συμπληρώσουμε εδώ ότι στο [13] ο Dehornoy ονομάζει την παραπάνω διάταξη **σίγμα - διάταξη** και την χωρίζει σε:

- $<$ αν το κύριο γράμμα είναι αυτό με το μικρότερο δείκτη
- $<^{\Phi}$ αν το κύριο γράμμα είναι αυτό με τον μέγιστο δείκτη.

2.4 Birman - Ko - Lee Canonical form

Παρόμοια με τους γεννήτορες του Artin οι Birman, Ko και Lee στο [8] εισήγαγαν νέους γεννήτορες για τις ομάδες των πλεξίδων όπου και σε αυτούς ένα ζεύγος κλωστών διασταυρώνεται ακριβώς μία φορά. Η διαφορά με τους γεννήτορες αυτούς είναι ότι η διασταύρωση γίνεται μεταξύ δύο τυχαίων κλωστών και όχι δύο γειτονικών. Στην παρούσα παράγραφο δεν θα εξετάσουμε διεξοδικά την κανονική μορφή και κατ' επέκταση την λύση του word problem που προτείνουν οι Birman - Ko - Lee, αλλά θα αναφερθούμε συνοπτικά στους καινούργιους γεννήτορες και θα παρουσιάσουμε την καινούργια κανονική μορφή που εισήγαγαν, η οποία βασίζεται και βρίσκεται σε πλήρη αναλογία με αυτή του Garside.

Στη συνέχεια θα ορίσουμε την εναλλακτική παράσταση των Birman-Ko-Lee (στο εξής BKL) με βάση τους κλασσικούς γεννήτορες του Artin.

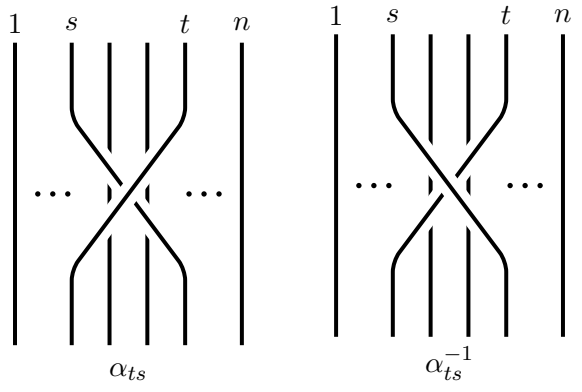
Ορισμός 2.29. Έστω η ομάδα B_n και οι κλωστές της t, s με $1 \leqslant s < t \leqslant n$, ορίζουμε τον γεννήτορα α_{ts} της B_n ως εξής:

$$\alpha_{ts} = (\sigma_{t-1}\sigma_{t-2}\dots\sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1}\dots\sigma_{t-2}^{-1}\sigma_{t-1}^{-1})$$

στο εξής θα αναφερόμαστε στους παραπάνω γεννήτορες ως **BKL-γεννήτορες**.

Παρατηρούμε εδώ ότι αν η κλασσική παράσταση του Artin για την B_n περιέχει $n-1$ γεννήτορες, η παράσταση BKL περιέχει $\frac{(n-1)(n-2)}{2}$ γεννήτορες.

Αν θα θέλαμε να ορίσουμε γεωμετρικά τους παραπάνω γεννήτορες, θα λέγαμε ότι η κλωστή που ξεκινάει από το σημείο t καταλήγει στο s και αντίστοιχα αυτή που ξεκινάει από το σημείο s καταλήγει στο t, θεωρώντας, όμοια με προηγούμενα, ότι η θετική πλέξη είναι αυτή που η δεξιότερη κλωστή περνά πάνω από την αριστερή.

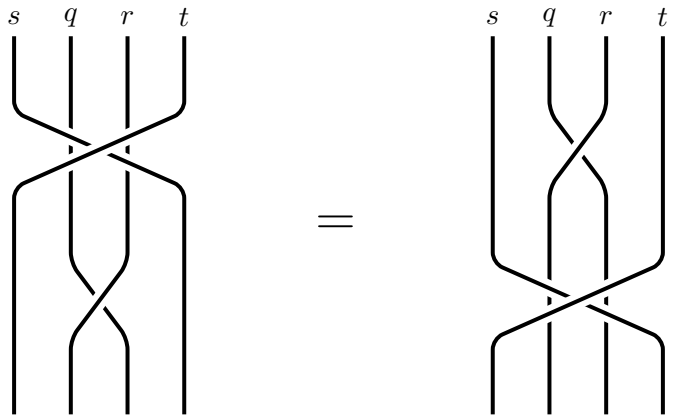


α_{ts} α_{ts}^{-1}

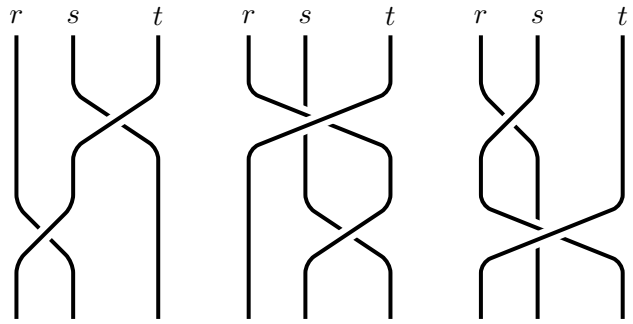
Σχήμα 2.6: Ο BKL-γεννήτορας και ο αντίστροφός του.

Οι γεννήτορες που μόλις ορίσαμε ικανοποιούν τις ακόλουθες σχέσεις:

1. $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ αν $(t-r)(t-q)(s-r)(s-q) > 0$.
2. $\alpha_{ts}\alpha_{sr} = \alpha_{tr}\alpha_{ts} = \alpha_{sr}\alpha_{tr}$ για $1 \leqslant r < s < t \leqslant n$.



Σχήμα 2.7: Η σχέση $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ για $1 \leqslant s < q < r \leqslant t$.



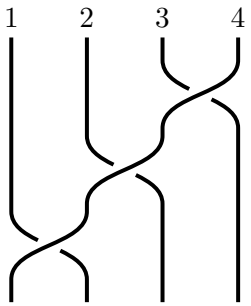
Σχήμα 2.8: Η σχέση $\alpha_{ts}\alpha_{sr} = \alpha_{tr}\alpha_{ts} = \alpha_{sr}\alpha_{tr}$ για $1 \leqslant r < s < t \leqslant n$.

Με βάση τους καινούργιους γεννήτορες και ακολουθώντας πλήρως την λογική του Garside, οι Birman-Ko-Lee ορίσαν μιά καινούργια κανονική μορφή για τα στοιχεία της ομάδας των πλεξίδων.

Ορισμός 2.30. Θα ορίσουμε ως **BKL-θεμελιώδη λέξη** στην ομάδα πλεξίδων B_n, με γεννήτορες τους BKL-γεννήτορες, την λέξη που ορίζεται ώς:

$$\delta_n = \alpha_{n,n-1}\alpha_{n-1,n-2}\cdots\alpha_{2,1} = \sigma_{n-1}\sigma_{n-2}\cdots\sigma_1$$

και θα την συμβολίζουμε με $\boldsymbol{\delta_n}$



Σχήμα 2.9: Η δ_4 BKL-θεμελιώδης λέξη της B_4.

Παρατηρούμε ότι για την νέα θεμελιώδη λέξη που ορίσαμε ισχύει:

$$\Delta_n^2 = \delta_n^n$$

Δηλαδή το κέντρο της B_n είναι, με χρήση των γεννητόρων BKL, δ_n^n.

Η δ_n έχει παρόμοιες ιδιότητες με αυτές της Δ_n:

1. Για οποιοδήποτε γεννήτορα α_{ts} έχουμε:

$$\delta_n = \alpha_{ts} A = B \alpha_{ts}$$

όπου A, B θετικές πλεξίδες[4] εκφρασμένες στους BKL-γεννήτορες.

2. Για οποιοδήποτε γεννήτορα α_{ts} ισχύει:

$$\alpha_{ts} \delta_n = \delta_n \alpha_{t+1,s+1}$$

Σε αυτό το σημείο θα διατυπωσουμε ένα βασικό θεώρημα των Birman-Ko-Lee, οι οποίοι ακολουθώντας τα βήματα του Garside, παρουσιάζουν στο [8] μια κανονική μορφή για την ομάδα B_n με χρήση των καινούργιων γεννητόρων.

Θεώρημα 2.7. *Κάθε στοιχείο στην B_n που αναπαρίσταται από μία λέξη w μπορεί να γραφεί μοναδικά στην μορφή:*

$$w = \delta_n^j A_1 A_2 \dots A_k$$

όπου το $A = A_1 A_2 \dots A_k$ είναι θετικό, το j είναι μέγιστο και το k ελάχιστο για κάθε τέτοια αναπαράσταση. Επίσης, τα A_i είναι θετικές πλεξίδες που προσδιορίζονται μοναδικά μέσω των μεταθέσεων που τις αντιστοιχούν.

Η απόδειξη του θεωρήματος παραλείπεται καθώς είναι εκτενής και παρουσιάζει πολλές ομοιότητες με αυτή του Garside, σε αναλογία με τους καινούργιους γεννήτορες. Μπορεί να βρεθεί στο [8].

[4] Όταν λέμε θετικές πλεξίδες εννοούμε αυτές που γράφονται με χρήση μόνο θετικών BKL-γεννητόρων.

ΚΕΦΑΛΑΙΟ 3

Εφαρμογές στην Κρυπτογραφία

Σε αυτό το κεφάλαιο δεν φιλοδοξούμε να παρουσιάσουμε τις τελευταίες εξελίξεις γύρω από τις πλεξίδες και τις εφαρμογές τους στην κρυπτογραφία. Θα αναφέρουμε συνοπτικά τα δύο κυριότερα πρωτόκολλα που εισήγαγαν το θέμα καθώς και τους λόγους για τους οποίους επιλέχθηκε η συγκεκριμένη ομάδα ως πλατφόρμα για την δημιουργία κρυπτογραφιών πρωτοκόλλων. Να πούμε μονάχα πως οι βελτιωμένες λύσεις του προβλήματος της συζυγίας που έχουν παρουσιαστεί τα τελευταία χρόνια πάγωσαν για λίγο το ενδιαφέρον για τις κρυπτογραφικές πτυχές των πλεξίδων.

3.1 Εισαγωγή στην Κρυπτογραφία

3.1.1 Γενικά

Αν θελήσουμε να δώσουμε έναν γενικό ορισμό για την κρυπτογραφία θα μπορούσαμε να πούμε πως είναι η επιστήμη που ασχολείται με τη μελέτη, την ανάπτυξη και την χρήση τεχνικών με στόχο την ασφαλή επικοινωνία. Θα πρέπει να διευκρινήσουμε πως όταν λέμε ασφαλή επικοινωνία, εννοούμε ότι το μήνυμα το οποίο θέλουμε να μεταφερθεί σε ένα ή και περισσότερα άτομα, θα διαβαστεί αποκλειστικά από αυτά και οποιοσδήποτε τρίτος θελήσει να το διαβάσει ή και να το αλλοιώσει, δεν θα μπορέσει.

Ιστορικά, η κρυπτογραφία ανάγεται στα αρχαία χρόνια και χρησιμοποιείται σαν μέθοδος ασφαλούς επικοινωνίας μέχρι και σήμερα. Τότε η κρυπτογράφηση βασιζόταν κυρίως σε γλωσσικούς μετασχηματισμους. Δηλαδή στην αντικατάσταση γραμμάτων με άλλα γράμματα ή και αριθμούς. Η πρώτη γνωστή κρυπτογραφική συσκευή θεωρείται η ¨Σπαρτατική Σκυτάλη¨, η οποία ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης. Μια πλήρης, μη τεχνική καταγραφή της ιστορίας της κρυπτογραφίας μπορεί να βρεί κανείς στο βιβλίο του Kahn, *The Codebreakers*, που όμως σταματά γύρω στο 1970.

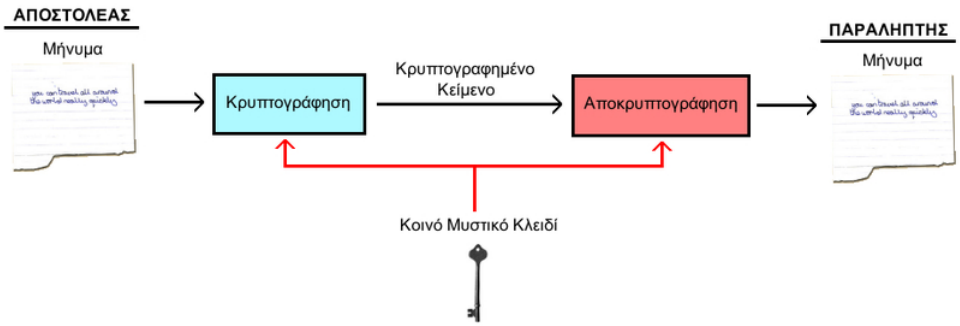
Η εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών και των επικοινωνιακών συστημάτων κατα τη δεκαετία του ΄60, έδωσε μια νέα ώθηση στην μελέτη της επιστήμης της κρυπτογραφίας. Θα μπορούσαμε να πούμε ότι η πιό εντυπωσιακή εξέλιξη στην ιστορία της, έγινε το 1976 όταν οι Diffie - Hellman δημοσίευσαν το άρθρο *New Directions in Cryptogrphy*[15]. Σε αυτό το άρθρο εισήγαγαν την επαναστατική ιδέα της κρυπτογράφισης δημοσίου κλειδιου και πρότειναν μια καινούργια μέθοδο ανταλαγής κλειδιού η ασφάλεια της οποίας βασίζεται σε ένα δύσκολο μαθηματικό πρόβλημα, αυτό του διακριτού λογαρίθμου. Αν και οι συγγραφείς του άρθρου δεν πρότειναν κάποια πρακτική υλοποίηση της κρυπτογράφησης δημοσίου κλειδιού, η ιδέα που παρουσίασαν ήταν ξεκάθαρη και κίνησε το ενδιαφέρον πολλών μελετητών. Δύο χρόνια αργότερα οι Rivest, Shamir και Adleman στο [31], ανακάλυψαν την πρώτη πρακτική μέθοδο κρυπτογράφησης δημοσίου κλειδιού που βασίζεται σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της παραγοντοποίησης μεγάλων ακεράιων.

Θα δώσουμε κάποιους χρήσιμους ορισμούς για την συνέχεια.

Ορισμός 3.1. Κρυπτογράφηση ονομάζουμε την διαδικασία μετσαχηματισμού ενός μηνύματος με χρήση κάποιου αλγορίθμου, που θα τον ονομάζουμε **κρυπτογραφικό αλγόριθμο** ώστε να αποκρύπτεται η αρχική του μορφή. Η αντίστροφη διαδικασία που ακολουθούμε προκειμένου να επαναφέρουμε το

μετασχηματισμένο μήνυμα στην αρχική του μορφή, ονομάζεται **αποκρυπτογράφηση**. Το μήνυμα προς αποστολή ονομάζεται **αρχικό κείμενο** ενώ το μετασχημεατισμένο μήνυμα **κρυπτογραφημένο κείμενο**. Ως **κλειδί κρυπτογράφησης** ορίζουμε την πληροφορία εκείνη που χρησιμοποιεί ο κρυπτογραφικός αλγόριθμος και καθορίζει τον μετασχηματισμό του αρχικού κειμένου σε κρυπτοκείμενο.

Μέχρι και το 1976 η κρυπτογράφηση γινόταν σε γενικές γραμμές με έναν συγκεκριμένο τρόπο, που ονομάστηκε **Κρυπτογραφία Συμμετρικού Κλειδιού**. Η διαδικασία αυτής της κρυπτογράφησης βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη



Σχήμα 3.1: Κρυπτογράφηση Συμμετρικού Κλειδιού

3.1.2 Κρυπτογραφία Δημοσίου Κλειδιού

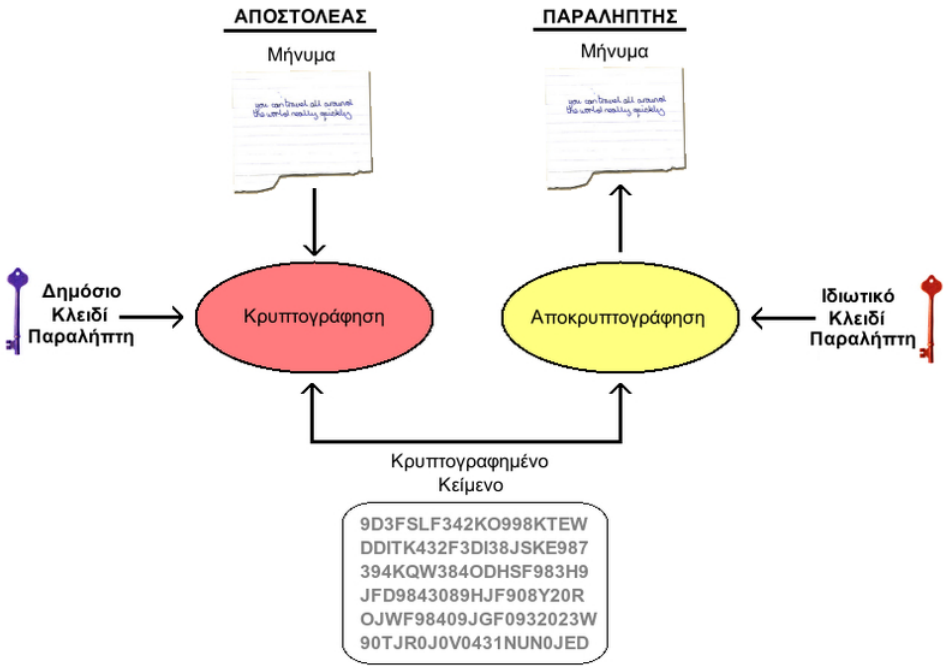
Η κρυπτογράφηση **δημοσίου κλειδιού (Public Key Cryptography)** ή **ασύμμετρου κλειδιού (Asymmetric Cryptography)** παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται **ιδιωτικό κλειδί (private key)** και το άλλο **δημόσιο κλειδί (public key)**. Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός

ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα· Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης.



Σχήμα 3.2: Κρυπτογράφηση Δημοσίου Κλειδιού

3.1.3 Μία ταχυδρομική αναλογία

Για να κατανοήσουμε καλύτερα τις διαφορές μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης, μπορούμε να φανταστούμε δύο ανθρώπους, την Alice και τον Bob που θέλουνε να ανταλλάξουνε κρυφά μηνύματα μέσω του ταχυδρομείου.

Με ένα σύστημα συμμετρικού κλειδιού, η Alice πρώτα βάζει το μυστικό μήνυμα που θέλει να στείλει σε ένα κουτί, το οποίο κλειδώνει με μία κλειδαριά για την οποία έχει το κλειδί. Στη συνέχεια το στέλνει στον Bob μέσω ταχυδρομείου. Όταν ο Bob λάβει το μήνυμα, χρησιμοποιεί ένα κλειδί πανομοιότυπο με αυτό της Alice (το οποίο έχει αποκτήσει προηγουμένως, ίσως σε πρόσωπο με πρόσωπο συνάντηση με την Alice) για να ξεκλειδώσει και να διαβάσει το μήνυμα. Στη συνέχεια ο Bob μπορεί να χρησιμοποιήσει το ίδιο λουκέτο για να στείλει την κρυφή του απάντηση στην Alice.

Σε ένα σύστημα ασύμμετρου κλειδιού, η Alice και ο Bob έχουν ξεχωριστές κλειδαριές. Πρώτα, η Alice ζητάει από τον Bob να της στείλει το ξεκλείδωτο λουκέτο του μέσω απλού ταχυδρομείου, ενώ το κλειδί για το λουκέτο αυτό το κρατάει ο Bob για τον εαυτό του. Όταν η Alice το λάβει, το χρησιμοποιεί για να κλειδώσει ένα κουτί το οποίο περιέχει το μήνυμά της και στέλνει το κλειδωμένο κουτί στον Bob. Όταν αυτός το λάβει, είναι ο μόνος που έχει το κλειδί για το λουκέτο, και άρα ο μόνος που μπορεί να το διαβάσει. Για να απαντήσει στην Alice, θα πρέπει αντίστοιχα και αυτός να πάρει ένα ανοιχτό λουκέτο από την Alice.

Το κρίσιμο πλεονέκτημα που μας προσφέρει η ασυμμετρική κρυπτογραφία είναι ότι η Alice και ο Bob δεν χρειάζεται να ανταλλάξουν κλειδιά. Αυτό αποτρέπει κάποιον τρίτο (ίσως, στο παράδειγμά μας, κάποιον διεφθαρμένο ταχυδρομικό υπάλληλο) από το να υποκλέψει το κλειδί καθώς αυτό μεταφέρεται, κάτι το οποίο θα επέτρεπε σε αυτόν τον τρίτο να κατασκοπεύει όλα τα μελλοντικά μηνύματα μεταξύ του Bob και της Alice. Οπότε, στο σύστημα δημοσίου κλειδιού, η Alice και ο Bob δε χρειάζεται να εμπιστεύονται ιδιαίτερα το ταχυδρομείο (και γενικά τον οποιοδήποτε δίαυλο επικοινωνίας).

3.2 Οι ομάδες των πλεξίδων ως υπόβαθρο για κρυπτογραφικά πρωτόκολλα

Προκειμένου να επιλέξουμε μία ομάδα, ως πλατφόρμα - υπόβαθρο για τν κατασκευή ενός κρυπτογραφικού πρωτοκόλλου πρέπει να πληρεί κάποιες προϋποθέσεις τις οποίες θα εκθέσουμε συνοπτικά παρακάτω:

1. Αρχικά απαιτούμε η ομάδα G να είναι επαρκώς «γνωστή», δηλαδή μελετημένη.

2. Επίσης, θέλουμε το word problem να έχει λύση και μάλιστα γρήγορη, μέσω κάποιου ντετερμινιστικού αλγορίθμου. Ακόμα, η ομάδα θα πρέπει να έχει μία εύκολα υπολογίσιμη κανονική μορφή για τα στοιχεία της.

3. Θα πρέπει να υπάρχει μία μέθοδος συγκάληψης των στοιχείων της G, τέτοια ώστε να είναι εδύνατο να υπολογίσει κανείς τα x και y αν του δοθεί η τιμή του xy. Η ύπαρξη μιας κανονικής μορφής μας επιτρέπει να έχουμε μία τέτοια μέθοδο.

4. Θα πρέπει ο αριθμός των στοιχείων μήκους n να αυξάνει σε εκθετικό χρόνο σε σχέση με το n.

Οι ομάδες των πλεξίδων φαίνεται πως ικανοποιούν όλες τις παραπάνω ιδιότητες. Η ιστορία λέει πως όταν οι συγγραφείς του [2] επινόησαν το κρυπτογραφικό τους πρωτόκολλο, απευθήνθηκαν στην Joan Birman προκειμένου να τους υποδείξει μία μη-αβελιανή ομάδα, η Birman τους πρότεινε, όχι τυχαία για εκείνη την περίοδο, την Ομάδα των Πλεξίδων. Πράγματι οι ομάδες αυτές ικανοποιούν τις παραπάνω ιδιότητες και για κάποια χρόνια ο ενθουσιασμός για την ομάδα αυτή ως πλατφόρμα για πρωτόκολλα υπήρξε μεγάλος. Κάποιες βελτιωμένες λύσεις του προβλήματος της συζηγίας έκαμψαν τον τελευταίο καιρό αυτόν τον ενθουσιασμό. Η ύπαρξη όμως άλυτων ακόμα προβλημάτων στην Ομάδα των Πλεξίδων αφήνει ανοιχτά ενδέχομενα ως προς την εφαρμογή τους στην Κρυπτογραφία.

3.3 Το πρωτόκολλο ανταλλαγής κλειδιών των I. Anshel, M. Anshel, D. Goldfeld

3.3.1 The algebraic key establishment protocol

Η γενική μορφή του αλγεβρικού πρωτοκόλλου θεμελίωσης κλειδιού είναι η εξής:

Έστω μια πεντάδα $(\boldsymbol{U}, \boldsymbol{V}, \beta, \gamma_1, \gamma_2)$, όπου οι $\boldsymbol{U}$, $\boldsymbol{V}$ είναι (εφικτά) υπολογίσιμα μονοειδή[1] και

$$\beta : \boldsymbol{U} \times \boldsymbol{U} \longrightarrow \boldsymbol{V}, \quad \gamma_i : \boldsymbol{U} \times \boldsymbol{V} \longrightarrow \boldsymbol{V} \ (i = 1, 2)$$

υπολογίσιμες συναρτήσεις που ικανοποιούν τις παρακάτω ιδιότητες:

(i) Για κάθε $x, y_1, y_2 \in \boldsymbol{U}$,

$$\beta(x, y_1 \cdot y_2) = \beta(x, y_1) \cdot \beta(x, y_2).$$

(ii) Για κάθε $x,\ y \in \boldsymbol{U}$,

$$\gamma_1(x, \beta(x, y)) = \gamma_2(y, \beta(x, y)).$$

(iii) Έστω $y_1, y_2, \ldots, y_k \in \boldsymbol{U}$ και $\beta(x, y_1), \beta(x, y_2), \ldots, \beta(x, y_k)$ δημόσια για κάποιο κρυφό στοιχείο $x \in \boldsymbol{U}$. Τότε, γενικά, δεν είναι εφικτό να προσδιορίσει κανείς το στοιχείο x.

Στην Alice ανατίθεται δημόσια ένα υπο-μονοειδές[2] $S_A \subseteq \boldsymbol{U}$ και αντίστοιχα στον Bob ανατίθεται δημόσια ένα υπο-μονοειδές $T_B \subseteq \boldsymbol{U}$. Έστω ότι το S_A παράγεται από τα στοιχεία $\{s_1, s_2, \ldots, s_m\}$ και το T_B απο τα στοιχεία $\{t_1, t_2, \ldots, t_n\}$.

Το πρωτόκολλο έχει ως εξής:

- Η Alice επιλέγει ένα κρυφό στοιχείο $a \in S_A$ και στέλνει τα στοιχεία:

$$\beta(a, t_i) \quad i = 1, \ldots, n$$

- Όμοια ο Bob επιλέγει ένα κρυφό $b \in T_B$ και στέλνει τα στοιχεία:

$$\beta(b, s_i) \quad i = 1, \ldots, m$$

[1] Να σημειώσουμε σε αυτό το σημείο ότι **μονοειδές** είναι ένα σύνολο S εφοδιασμένο με μία διμελή πράξη $*$ τέτοια ώστε να ικανοποιούνται οι ιδιότητες (i)και (ii) αλλά όχι η (iii) του ορισμού της Ομάδας (1.1)

[2] Ο ορισμός του υπο-μονοειδούς σε σχέση με το μονοειδές βρίσκεται σε πλήρη αντιστοιχία με αυτόν της υποομάδας σε σχέση με την ομάδα.

Από την ιδιότητα (iii) εξασφαλίζεται ότι, παρ' όλη την αποστολή των $\beta(a, t_i)$ και $\beta(b, s_i)$ μέσω ενός δημόσιου καναλιού, τα στοιχεία a, b παραμένουν κρυφά.

- Η Alice μέσω της ιδιότητας (i) μπορεί και υπολογίζει το στοιχείο

  $$\beta(b, a)$$

  και το στοιχείο

  $$\gamma_1(a, \beta(b, a))$$

- Αντίστοιχα ο Bob υπολογίζει τα στοιχεία

  $$\beta(a, b) \quad \text{και} \quad \gamma_2(a, \beta(a, b))$$

- Τέλος από την ιδιότητα (ii) βλέπουμε ότι

  $$\kappa = \gamma_1(a, \beta(b, a)) = \gamma_2(a, \beta(a, b))$$

  Το οποίο μπορεί να χρησιμοποιηθεί ως το κοινό κλειδί.

3.3.2 Εφαρμογή του πρωτοκόλλου σε ομάδες

Το παρακάτω αποτελεί ειδική περίπτωση του πρωτοκόλλου που μόλις περιγράψαμε. Εδώ έχουμε $\boldsymbol{U} = \boldsymbol{V} = \boldsymbol{G}$, όπου η $\boldsymbol{G}$ είναι μία ομάδα. Όπως και προηγουμένως,η Alice και ο Bob επιλέγουν και δημοσιοποιούν δύο πεπερασμένα παραγόμενες υποομάδες S_A και T_B αντίστοιχα.

$$S_A = \langle s_1, s_2, \ldots, s_m \rangle, \qquad T_B = \langle t_1, t_2, \ldots, t_n \rangle$$

Εδώ η συνάρτηση $\beta : \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}$ επιλέγουμε να είναι η συζυγία

$$\beta(x, y) = x^{-1}yx$$

και οι συναρτήσεις $\gamma_1,\ \gamma_2 : \boldsymbol{G} \times \boldsymbol{G} \to \boldsymbol{G}$ να είναι οι ακόλουθες:

$$\gamma_1(x, y) = x^{-1}y \ \text{ και } \ \gamma_2(x, y) = y^{-1}x$$

Οπως προηγουμένως,η Alice και ο Bob επιλέγουν δύο κρυφά στοιχεία $a \in S_A$ και $b \in T_B$ αντίστοιχα.

- Η Alice ξεκινάει το πρωτόκολλο υπολογίζοντας, ξαναγράφοντας και στέλνοντας τα στοιχεία $\beta(a, t_i)$ για $i = 1, \ldots, n \quad \Rightarrow$

  $$a^{-1}t_1a,\ a^{-1}t_2a,\ \ldots,\ a^{-1}t_na$$

- Όμοια ο Bob υπολογίζει, ξαναγράφει και στέλνει τα στοιχεία:

$$b^{-1}s_1b,\ b^{-1}s_2b,\ \ldots,\ b^{-1}s_nb$$

Εδώ πρέπει να πούμε ότι κάποιος εχθρικός παρατηρητής που παρακολουθεί το δημόσιο κανάλι προκειμένου να προσδιορίσει τα a, b πρέπει να μπορέσει να λύσει τα συστήματα συζυγών εξισώσεων. Γι' αυτό το λόγο όταν η Alice και ο Bob ξαναγάφουν τα στοιχεία $\beta(a, t_i)$ και $\beta(b, s_i)$, φροντίζουν ώστε η μορφή τους να είναι τέτοια, που να μην μπορεί κάποιος να αναγνωρίσει τα a και b απο τα στοιχεία που στέλνονται μέσω του δημόσιου καναλιού.

Υπενθυμίζουμε ότι ο συζυγής του γινομένου δύο στοιχείων είναι ίσος με το γινόμενο των συζυγών αυτών των στοιχείων, από την ιδιότητα (i).
Έτσι η Alice υπολογίζει:

$$\beta(b, a) = b^{-1}ab.$$

Και ο Bob:

$$\beta(a, b) = a^{-1}ba.$$

Τέλος, υπολογίζοντας η Alice το

$$\kappa = \gamma_1(a, \beta(b, a)) = a^{-1}b^{-1}ab$$

και ο Bob το

$$\kappa = \gamma_2(b, \beta(b, a)) = a^{-1}b^{-1}ab.$$

Σε αυτό το σημείο κάθε χρήστης έχει στην κατοχή του το κοινό, μυστικό κλειδί κ, γραμμένο συνήθως σε διαφορετική μορφή ο καθένας. Η ύπαρξη όμως ενός υπολογικστικά γρήγορου αλγορίθμου ώστε να μπορούμε να μετατρέπουμε κάθε λέξη στην κανονική της μορφή, η οποία επιπλέον είναι και μοναδική, επιτρέπει στους χρήστες να τον εφαρμόσουν και τέλος να έχει ο καθένας ένα κοινό, πανομοιότυπα γραμμένο, κλειδί.

3.4 Το πρωτόκολλο των Ko, Lee, Cheon, Han, Kang και Park

Το πρωτόκολλο αυτό παρουσιάστηκε από τους K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang και C. Park στο [24] λίγο μετά απο αυτό των Anshel, Anshel & Goldfeld.

Θα ξεκινήσουμε με κάποιους χρήσιμους ορισμούς και με την περιγραφή του κρυπτοσυστήματος δημοσίου κλειδιού του El-Gamal[17], το οποίο μοιάζει αρκετά με το κρυπτοσύστημα που θα παρουσιάσουμε στην συνέχεια.

Ορισμός 3.2. Μία συνάρτηση $f : X \to Y$ λέγεται **μονόδρομη συνάρτηση** (one-way function), αν είναι ¨εύκολο¨ να υπολογίσουμε τις τιμές $f(x)$ για κάθε $x \in X$ αλλά υπολογιστικά ¨δύσκολο¨ να βρεθεί η αντίστροφή της. Δηλαδή να υπολογίσουμε οποιοδήποτε x αν μας δοθεί μονάχα το $f(x)$.

Ορισμός 3.3. Μία μονόδρομή συνάρτηση θα ονομάζεται **trapdoor**-μονόδρομη συνάρτηση αν, δεδομένου ότι μας δίνεται μια συγκεκριμένη πληροφορία, γνωστή και ως trapdoor πληροφορία, καθίσταται εύκολο να υπολογιστεί η αντίστροφη της.

Ορισμός 3.4. Έστω G μια πολλαπλασιαστική ομάδα. Δοθέντα τα στοιχεία g, g^x, g^y της ομάδας, να υπολογιστεί το g^{xy}. Το πρόβλημα που μόλις διατυπώσαμε είναι γνωστό ως **Diffie-Hellman Problem**.

Να παρατηρήσουμε εδώ πως προκειμένου να υπολογίσει κανείς το g^{xy} πρέπει να μπορεί να βρεί τα x, y από τις τιμές των g^x και g^y το οποίο είναι γενικά δύσκολο.

Στη συνέχεια θα περιγράψουμε το κρυπτοσύστημα του El-Gamal.

EL-GAMAL ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

1. **Δημιουργία κλειδιού**
   - Η Alice επιλέγει μια κυκλική ομάδα G τάξης q
   - Η Alice επιλέγει τυχαία ένα $x \in \{1, \ldots, q-1\}$.
   - Η Alice υπολογίζει $h = g^x$.
   - Η Alice δημοσιοποιεί το (h, G, q, g) ως το δημόσιο κλειδί της και κρατά το x ως το ιδιωτικό.
2. **Κρυπτογράφηση** Έστω m το μήνυμα που θέλει να στείλει ο Bob στην Aliceμε χρήση του δημοσίου κλειδιού της, (h, G, q, g).
   - Ο Bob επιλέγει τυχαία ένα $y \in \{1, \ldots, q-1\}$ και υπολογίζει: $c_1 = h^y$.

- Επίσης ο Bob υπολογίζει το κοινό κλειδί $s = h^y$.
- Ο Bob μετατρέπει το μήνυμα m σε $m' \in G$.
- Ο Bob υπολογίζει $c_2 = m's = m'h^y$.
- Τέλος ο Bob στέλνει το κρυπτογραφημένο μήνυμα (c_1, c_2).

$$\Rightarrow (c_1, c_2) = (g^y, m'h^y) = (g^y, m'g^{xy})$$

Να σημειώσουμε ότι μπορεί κανείς εύκολα να υπολογίσει το h^y αν γνωρίζει το m' και έτσι το y αλλάζει κάθε φορά και γι' αυτό ονομάζεται **εφήμερο κλειδί**.

3. **Αποκρυπτογράφηση**

   - Η Alice υπολογίζει το κοινό κλειδί $s = c_1^x$
   - Η Alice υπολογίζει $m' = c_2 s^{-1}$.

   $$\Rightarrow m' = c_2 s^{-1} = m'h^y s^{-1} = m'(g^x)^y (g^{xy})^{-1} = m'$$

   - Τέλος μετατρέπει το $m' \in G$ σε m.

3.4.1 Ιδιότητες του πρωτοκόλλου

1. Το σχήμα ανταλλαγής κλειδιού βασίζεται σε μιά παραλλαγή του conjugacy problem η οποία μοιάζει με το πρόβλημα των Diffie-Hellman και το κρυπτοσύστημα κατασκευάζεται από αυτό το σχήμα συνεπώς συμπεριφέρεται παρόμοια με αυτό του El-Gamal.

2. Το κρυπτοσύστημα δημοσίου κλειδιού που παρουσιάζεται στην συνέχεια δεν είναι ντετερμινιστικό, δηλαδή το κρυπτοκείμενο εξαρτάται και από το απλό κείμενο και από την πλεξίδα που επιλέχθηκε τυχαία κάθε φορά.

3. Η επέκταση του αρχικού μηνύματος είναι το πολύ 4 προς 1.

4. Υπάρχουν δύο παράμετροι p, n στο κρυπτοσύστημα τέτοιοι ώστε το μήκος του μηνύματος να γίνεται $pnlogn$. Η κρυπτογράφηση και η αποκρυπτογράφηση γίνονται σε χρόνο $O(p^2 nlogn)$.

3.4.2 Η μονόδρομη συνάρτηση

Οι δημιουργοί του πρωτοκόλλου προτείνουν μια μονόδρομη συνάρτηση η οποία βασίζεται στην δυσκολία επίλυσης του Generalized Conjugacy Search Problem. Επίσης προτείνεται μιά συμφωνία για το κλειδί και ένα Κρυπτοσύστημα Δημοσίου Κλειδιού με χρήση της συγκεκριμένης συνάρτησης. Δεν προτείνεται κάποιο σχήμα ψηφιακής υπογραφής.

Να σημειώσουμε σε αυτό το σημείο ότι κατά την εκτέλεση των πρωτοκόλλων όλες οι πλεξίδες θεωρούμε ότι υπολογίζονται σε κάποια *κανονική μορφή* και έτσι είναι δύσκολο αν είναι γνωστή κάποια πλεξίδα $ab \in B_n$ να υπολογιστούν τα a, b.

Έστω δύο υποομάδες LB_l και RB_r της B_{l+r}, όπου:

$$LB_l = \langle \sigma_1, \ldots, \sigma_{l-1} \mid \text{σχέσεις πλεξίδων} \rangle$$

$$RB_r = \langle \sigma_{l+1}, \ldots, \sigma_{r+l} \mid \text{σχέσεις πλεξίδων} \rangle$$

Η LB_l είναι η υποομάδα της B_{l+r} που αποτελείται από τις πλεξίδες που δημιουργούνται από τις l πρώτες κλωστές ενώ η RB_r αποτελείται από τις πλεξίδες που δημιουργούνται από τις υπόλοιπες r κλωστές.

Επίσης, για κάθε $a \in LB_l$ και για κάθε $b \in RB_r$ ισχύει ότι $\boldsymbol{ab = ba}$, το οποίο προκύπτει άμεσα από τις σχέσεις πλεξίδων και από το γεγονός όλα τα στοιχεία της LB_l αντιμετατίθενται με τα στοιχεία της RB_r. Ορίζουμε την μονόδρομη συνάρτηση:

$$f : LB_l \times B_{l+r} \to B_{l+r} \times B_{l+r}, \text{ με}$$
$$f(a, x) = (axa^{-1}, x)$$

Η οποία είναι πράγματι μονόδρομη διότι δοθέντος ενός ζεύγους (a, x) είναι απλός ο υπολογισμός του axa^{-1} αλλά όλες οι γνωστές επιθέσεις[3] για τον υπολογισμό του a μέσω του (axa^{-1}, x), είναι εκθετικού χρόνου. Συγκεκριμένα η μονόδρομη συνάρτηση που μόλις ορίσαμε βασίζεται στο "Generalized Conjugacy Search Problem"

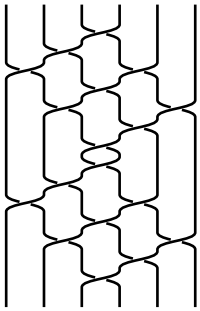
Η ασφάλεια του σχήματος συμφωνίας κλειδιού (key agreement scheme) καθώς και του Κρυπτοσυστήματος Δημοσίου κλειδιού βασίζονται στο παρακάτω πρόβλημα:

- **[Βασικό Πρόβλημα]** Έστω x, y_1, y_2 στοιχεία στην B_{l+r} τέτοια ώστε $y_1 = axa^{-1}$ και $y_2 = bxb^{-1}$ για κάποια κρυφά στοιχεία $a \in LB_l$ και $b \in RB_r$. Να υπολογιστεί το $by_1b^{-1} = (ay_2a^{-1} = abxa^{-1}b^{-1})$.

Δεν γνωρίζουμε αν το πρόβλημα που μόλις διατυπώσαμε συνεπάγεται το "Generalized Conjugacy Search Problem", αν και το τελευταίο συνεπάγεται το πρώτο.

Ο ρόλος του x είναι αντίστοιχος με αυτόν του g στο Πρόβλημα των Diffie-Hellman, όπου καλούμαστε να υπολογίσουμε τα g^x, g^y από το g^{xy}. Προκειμένου να ¨δυσκολέψουμε¨ το βασικό μας πρόβλημα , απαιτούμε το x να

[3] Γνωστές μέχρι τη στιγμή που γραφόταν το συγκεκριμένο άρθρο (2000)



Σχήμα 3.3: Μια πλεξίδα της μορφής x_1x_2z

είναι επαρκώς πολύπλοκο, αποφεύγοντας τις πλεξίδες της μορφής x_1x_2z οπου $x_1 \in LB_l$, $x_2 \in RB_r$ και $z \in B_{l+r}$ ώστε η z να αντιμετατίθεται και με την LB_l και με την RB_r.
Έστω λοιπόν ότι το x μπορούσε να αναλυθεί στην μορφή: x_1x_2z τότε θα είχαμε

$$by_1b^{-1} = baxa^{-1}b^{-1} = bax_1x_2za^{-1}b^{-1} = ax_1a^{-1}bx_2b^{-1}z = y_1y_2z$$

Άρα θα μπορούσαμε να υπολογίσουμε το by_1b^{-1} χωρίς να χρειάζεται να ξέρουμε τα a, b γιατί θα είχαμε

$$y_1 = axa^{-1} = (axa^{-1})x_2z \quad \text{και} \quad y_2 = bxb^{-1} = x_1(bx_2b^{-1})z$$

3.4.3 Η Συμφωνία Κλειδιού

1. **Προπρασκευαστικό Βήμα:** Επιλέγεται ένα κατάλληλο ζευγάρι ακεραίων (l, r) και μιά επαρκώς πολύπλοκη $(l + r)$-πλεξίδα, $x \in B_{l+r}$ και δημοσιεύονται.

2. **Η συμφωνία του κοινού κλειδιού:**

   (i) Η Αλίκη επιλέγει μια τυχαία, κρυφή πλεξίδα $a \in LB_l$ και στέλνει στον Bob: $y_1 = axa^{-1}$

   (ii) Αντίστοιχα ο Bob επιλέξει μια τυχαία, κρυφή πλεξίδα $b \in RB_r$ και στέλνει στην Αλίκη το στοιχείο $y_2 = bxb^{-1}$.

   (iii) Η Αλίκη λαμβάνει το y_2 και υπολογίζει το κοινό κλειδί $\kappa = ay_2a^{-1}$.

   (iv) Ο Bob λαμβάνει το y_1 και υπολογίζει και αυτό το κοινό κλειδί $\kappa = by_1b^{-1}$.

Επειδή γνωρίζουμε ότι $ab = ba$ για $a \in LB_l$ και $b \in RB_r$, έχουμε:

$$ay_2a^{-1} = a(bxb^{-1})a^{-1} = b(axa^{-1})b^{-1} = by_1b^{-1} = \kappa$$

και άρα έχουμε ένα κοινό κλειδί, που λόγω του ότι οι πλεξίδες γράφονται από τον κάθε χρήστη σε μία κοινή κανονική μορφή, τα κλειδιά είναι πανοοιότυπα.

3.4.4 Κρυπτογράφιση Δημοσίου Κλειδιού

Με χρήση του συστήματος συμφωνίας κλειδιού που μόλις περιγράψαμε, κατασκευάζουμε ένα καινούργιο Κρυπτοσύστημα Δημοσίου Κλειδιού.

Θα χρειαστούμε δύο ορισμούς:

Ορισμός 3.5. Συνάρτηση κατακερματισμού (hash function) ονομάζεται μια οποιαδήποτε συνάρτηση απεικονίζει δεδομένα αυθαίρετου μεγέθους σε δεδομένα καθορισμένου (μικρότερου) μεγέθους.

Ορισμός 3.6. Έστω $x_1, x_2 \in \{0,1\}^k$ η πράξη $\oplus$ μεταξύ των δύο στοιχείων, δίνει αποτέλεσμα ένα $x \in \{0,1\}^k$ όπου η συντεταγμένη i του x είναι 1 αν και μόνο αν τα ψηφία των x_1 και x_2 στην θέση i είναι διαφορετικά, αλλιώς είναι 0. Η πράξη $\oplus$ είναι αντιμεταθετική και προσεταιριστική. Επίσης, ισχύει: $x \oplus 0 = 0 \oplus x = x$ και $x \oplus x = 0$.

Παράδειγμα 3.1. $10011 \oplus 01010 = 11001$.

Το Κρυπτοσύστημα όπως παρουσιάζεται στο [24].

Έστω μια συνάρτηση κατακερματισμού

$$H : B_{l+r} \to \{0,1\}^k$$

1. **Η δημιουργία του κλειδιού**
   (α') Η Αλίκη επιλέγει μία επαρκώς πολύπλοκη $(l+r)$-πλεξίδα $x \in B_{l+r}$.
   (β') Επίσης, επιλέγει και μία πλεξίδα $a \in LB_l$.
   (γ') Το δημόσιο κλειδί είναι το (x, y), όπου $y = axa^{-1}$. Το ιδιωτικό κλειδί είναι η πλεξίδα a.

2. **Η κρυπτογράφιση**
   Έστω ένα μήνυμα $m \in \{0,1\}^k$ και έστω και το δημόσιο κλειδί (x, y)
   (α') Ο Bob επιλέγει μια τυχαία πλεξίδα $b \in RB_r$
   (β') Το κρυπτοκείμενο είναι το ζευγάρι (c, d), όπου $c = bxb^{-1}$ και $d = H(byb^{-1}) \oplus m$.

3. **Η αποκρυπτογράφιση**
   Έστω, τέλος, ένα κρυπτοκείμενο (c, d) και ένα ιδιωτικό κλειδί a, αποκρυπτογραφούμε υπολογίζοντας: $m = H(aca^{-1}) \oplus d$.

Επειδή οι πλεξίδες a και b αντιμετατίθενται, έχουμε:

$$ava^{-1} = abxb^{-1}a^{-1} = baxa^{-1}b^{-1} = byb^{-1}$$

έτσι

$$H(aca^{-1}) \oplus d = H(byb^{-1}) \oplus H(byb^{-1}) \oplus m = m$$

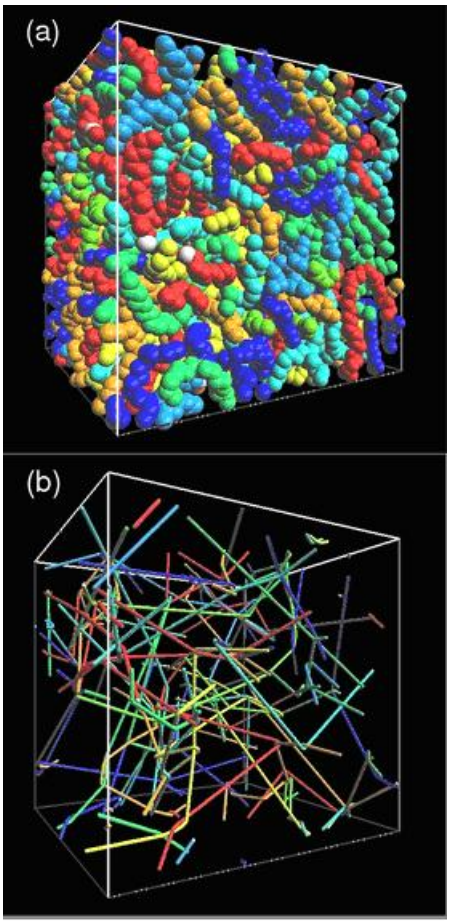
έτσι, η αποκρυπτογράφιση αποκαλύπτει το αρχικό μήνυμα m.

ΠΑΡΑΡΤΗΜΑ Α΄

Εφαρμογή των πλεξίδων στην μελέτη της διαπλοκής των πολυμερών

Οι πολυμερικές αλυσίδες είναι μακριά εύκαμπτα μόρια που δεν μπορούν να διαπεράσουν το ένα το άλλο [32]. Για αυτόν τον λόγο, σε ένα τήγμα πολυμερούς που αποτελείται από πολλές πολυμερικές αλυσίδες, αυτές επιβάλλουν τοπολογικά εμπόδια η μία στην άλλη. Αυτά τα τοπολογικά εμπόδια, αποκαλούνται **διαπλοκές** και επηρρεάζουν την διαμόρφωση και την κίνηση των αλυσίδων μέσα σε ένα τήγμα πολυμερούς.

Ο Edwards [32] έδειξε ότι η κίνηση των πολυμερικών αλυσίδων σε ένα τήγμα μπορεί να μελετηθεί χρησιμοποιώντας το **μοντέλο σωλήνα**. Πιο συγκεκριμένα, θεώρησε ότι τα τοπολογικά εμπόδια που επιβάλλουν οι γειτονικές αλυσίδες σε μία συγκεκριμένη αλυσίδα περιορίζουν την κίνησή της σε μία σωληνοειδή περιοχή. Έτσι, η κίνηση της αλυσίδας σε μικρή κλίμακα είναι περιορισμένη στην τάξη μεγέθους της διαμέτρου του σωλήνα, και η κίνηση σε μεγάλη κλίμακα γίνεται έρποντας κατά μήκους του άξονα του σωλήνα της. Ο κεντρικός άξονας αυτού του σωλήνα λέγεται **πρωταρχικό μονοπάτι** (primitive path). Οι Χ. Τζουμανέκας και Δ. Θεοδώρου στο [33], ακολουθώντας την οπτική του Edwards, εισήγαγαν τον αλγόριθμο CReTA για την αναγωγή μίας ατομιστικής προσομοίωσης πολυμερούς, παραγόμενης από υπολογιστή σε ένα (δίκτυο διαπλοκής) πρωταρχικών μονοπατιών (Εικ. Α΄.1). Με αυτόν τον αλγόριθμο, το πρωταρχικό μονοπάτι προσεγγίζεται από το μικρότερο μονοπάτι που κατασκευάζεται κρατώντας τα άκρα της αλυσίδας σταθερά ενώ κανείς συνεχώς σφίγγει τις αλυσίδες (ελαττώνοντας το μήκος κάθε αλυσίδας), χωρίς να επιτρέπει στις αλυσίδες να διαπερνούν η μία την άλλη. Εφαρμόζοντας αυτήν τη κατασκευή για όλες τις αλυσίδες καταλήγουμε σε μία αδροποιημένη (coarse grained) εικόνα του πολυμερικού τήγματος η οποία διατηρεί και αποκαλύπτει τα τοπολογικά χαρακτηριστικά του.



Σχήμα Α΄.1: (α) Αντιπροσωπευτικό ατομιστικό δείγμα PE (πολυαιθυλενίου) και (β) το αντίστοιχο παραγόμενο δίκτυο

Προκειμένου να μελετήσει κανείς τα τοπολογικά χαρακτηριστικά του πολυμερούς, αν οι πολυμερικές αλυσίδες είναι κλειστές, τότε μπορεί να εφαρμόσει τις γνωστές μεθόδους από την Θεωρία Κόμβων. Αυτό γίνεται με την χρήση τοπολογικών αναλλοίωτων, όπως για παράδειγμα, ο αριθμός περιέλιξης, το πολυώνυμο Jones, κλπ.

Οι κόμβοι και οι κρίκοι σχετίζονται άμεσα με τις πλεξίδες, εφόσον ενώνοντας τα αντίστοιχα άκρα μίας πλεξίδας με απλά τόξα παίρνουμε έναν κόμβο ή έναν κρίκο. Θα είχε μεγάλο ενδιαφέρον να χρησιμοποιήσουμε πλεξίδες για την μελέτη της διαπλοκής των πολυμερών, καθώς θα μπορούσαν να μας δώσουν πολύ περισσότερη πληροφορία από τα μέτρα που χρησιμοποιούνται συνήθως. Το πρώτο βήμα σε μία τέτοια μελέτη είναι να αντιστοιχίσουμε μία πλεξίδα σε μία διαμόρφωση ενός δείγματος πολυμερούς, όπως δίνεται μετά την εφαρμογή του αλγορίθμου CReTA, και στη συνέχεια να αναγνωρίσουμε

μία λέξη που αντιστοιχεί σε αυτήν την πλεξίδα. Έστω ότι για ένα πολυμερές μας έχουν δοθεί ν λέξεις (που αντιστοιχούν σε ν διαφορετικές διαμορφώσεις), π.χ. $\nu = 10$. Φέρνοντας την κάθε λέξη στην κανονική της μορφή μπορεί κανείς συγκρίνοντάς τες, κάνοντας χρήση κάποιου γνωστού αλγορίθμου επίλυσης του word problem να ανιχνεύσει τα (αλγεβρικά) κοινά χαρακτηριστικά σε αυτές τις λέξεις, τα οποία θα σχετίζονται με τις φυσικές ιδιότητες του συγκεκριμένου πολυμερούς. Στη συνέχεια, κάνοντας το ίδιο για ένα διαφορετικό πολυμερές, μπορεί κανείς να συγκρίνει τις λέξεις των δύο διαφορετικών πολυμερών και να βρεί αλγεβρικές διαφορές οι οποίες θα αντανακλούν στις φυσικές ιδιότητες αυτών των πολυμερών.

Βιβλιογραφία

[1] P. Anandam, *Introduction to Braid Group Cryptography*, March 2006

[2] I. Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public-key cryptography,* Math. Research Letters **6** (1999), 287-291

[3] E. Artin, *Theorie der Zöpfe,* Hamburg Abh. **4** (1925), 47-72

[4] E. Artin, *Theory of Braids,* Ann. Math. **48** (1947), 101-126

[5] Stephan Bigelow, *Braid Groups are Linear*. J. Amer. Math. Soc. **14** (2001), 471-486

[6] J. S. Birman, *Braids, Links and Mapping Class Groups*, Annals of Math. Studies **82**, Princeton Univ. Press (1975).

[7] J. S. Birman and T. E. Brendle, *Braids a survey,* (2005) online: http://arxiv.org/abs/math/0409205v2

[8] J.S. Birman, K. Ko and S. Lee, *A new approach to the word problem in braid groups*, Adv. Math. **139** (1998), 322-353.

[9] W.L. Chow, *On the algebraical braid group,* Ann. Math. **49** (1948), 654-658

[10] Max Dehn, *Papers on Group Theory and Topology*, Springer, (1987).

[11] P. Dehornoy, *A fast method for comparing braids*, Adv. Math. **125** (1997), 200-235.

[12] P. Dehornoy, *Convergence of handle reduction of braids*, preprint (online: http://www.math.unicaen.fr/ dehornoy/Surveys/Dhn.pdf).

[13] P. Dehornoy with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs Vol. **148**, Amer. Math. Soc., (2008).

[14] P.Dehornoy, I. Dynnikov, D. Rolfsen and B. Wiest, *Why are braids orderable?*, Panoramas & Synthéses, Vol. **14**, Soc. Math. France (2002).

[15] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. on Inf. Theory **22** (1976), 644-654.

[16] Doi M. and Edwards S. F., *The Theory of Polymer Dynamics*, Clarendon Press, Oxford, (1986).

[17] T. El-Gamal, *A publiv-key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **IT-31** (4) (1985), 469-472.

[18] M. Epple, *Orbits of Asteroids, a Braid and the First Link Invariant*, The Mathematics Intelligencer, **20**, no. 1 (1998), 45-52.

[19] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Peterson and W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992)

[20] J.B. Fraleigh, *Εισαγωγή στην Άλγεβρα*, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 2007.

[21] David Garber, *Braid Group Cryptography,* in Braids: Introductory Lectures on Braids, Configurations and Their Applications (2009) http://arxiv.org.abs/0711.3941.

[22] F. A. Garside, *The braid group and other groups,* Quart. J. Math Oxford **20-78** (1969), 235-254.

[23] C. Kassel V. Turaev, *Braid Groups*, Vol. 247, Graduate Texts in Mathematics, Springer, New York, 2008.

[24] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang and C. Park, *New public-key cryptosystem using braid groups*; Crypto 2000; Springer Lect. Notes in Comp. Sci. **1880** (2000), 166-184.

[25] Daan Krammer, *Braid Groups are Linear*, Annals of Math., Vol. **151** (2002), 131-156.

[26] Karl Mahburg, *An overview of Braid Group Cryptography*, preprint (online:http://www.math.wisc.edu/ boston/mahlburg.pdf)

[27] A. Menézes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc. (1997).

[28] K. Murasugi, B.I. Kurpita *A Study of Braids,* Mathematics and Its Applications, Kluweer Avademy Publishers (1999)

[29] O. Ore, *Linear Equations in Non-Commutative Fields,* Ann. Math. **32**(3) (1931), pp.463-477.

[30] V.V. Prasolov, A.B. Sossinsky, *Knots, Links, Braids and 3-Manifolds,* Translations of Mathematical Monographs vol. 154, Amer. Math. Soc., (1997).

[31] R.L. Rivest, A. Shamir and L. Andleman, *On Difital Signatures and Public Key Cryptosystems,* Commun. Ass. Comp. Mach. **21** (1978), 120-126.

[32] Rubinstein M. and Colby R. *Polymer Physics*, Oxford University Press, (2003).

[33] Tzoumanekas C. and Theodorou D. N., *Macromolecules*,**39**,4592 (2006).

Ευρετήριο