Οι Ομάδες των Πλεξίδων και Εφαρμογές τους στην Κρυπτογραφία και τα Πολυμερή

Μαντοπούλου Παλούκα Δανάη

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών
ΕΜΠ

Επιβλέπουσα Καθηγήτρια: Λαμπροπούλου Σοφία

Ιούλιος, 2013

Περιεχόμενα

- Η Ομάδα των Πλεξίδων

Περιεχόμενα

- Η Ομάδα των Πλεξίδων
- Η κανονική μορφή του Garside

Περιεχόμενα

- Η Ομάδα των Πλεξίδων
- Η κανονική μορφή του Garside
- Η μέθοδος handle reduction του Dehornoy

Περιεχόμενα

- Η Ομάδα των Πλεξίδων
- Η κανονική μορφή του Garside
- Η μέθοδος handle reduction του Dehornoy
- Εφαρμογές στην Κρυπτογραφία

Περιεχόμενα

- Η Ομάδα των Πλεξίδων
- Η κανονική μορφή του Garside
- Η μέθοδος handle reduction του Dehornoy
- Εφαρμογές στην Κρυπτογραφία
- Εφαρμογή στα Πολυμερή

Η Ομάδα των Πλεξίδων

- Η πρώτη καταγεγραμμένη μαθηματική μορφή συναντάται στα γραπτά του Gauss

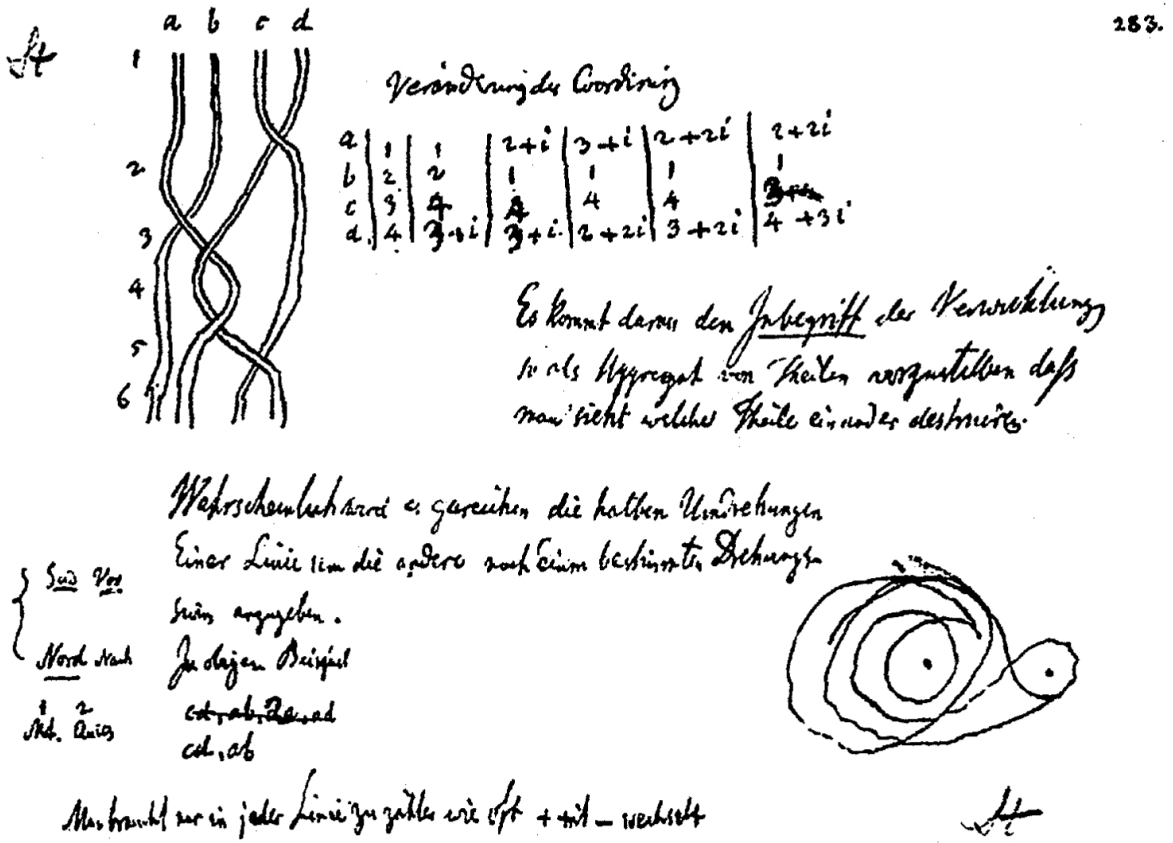
Η Ομάδα των Πλεξίδων

- Η πρώτη καταγεγραμμένη μαθηματική μορφή συναντάται στα γραπτά του Gauss
- Ο πρώτος αυστηρός μαθηματικός τους ορισμός έγινε από τον Artin στο άρθρο του *Theorie der Zöpfe*.

Η Ομάδα των Πλεξίδων

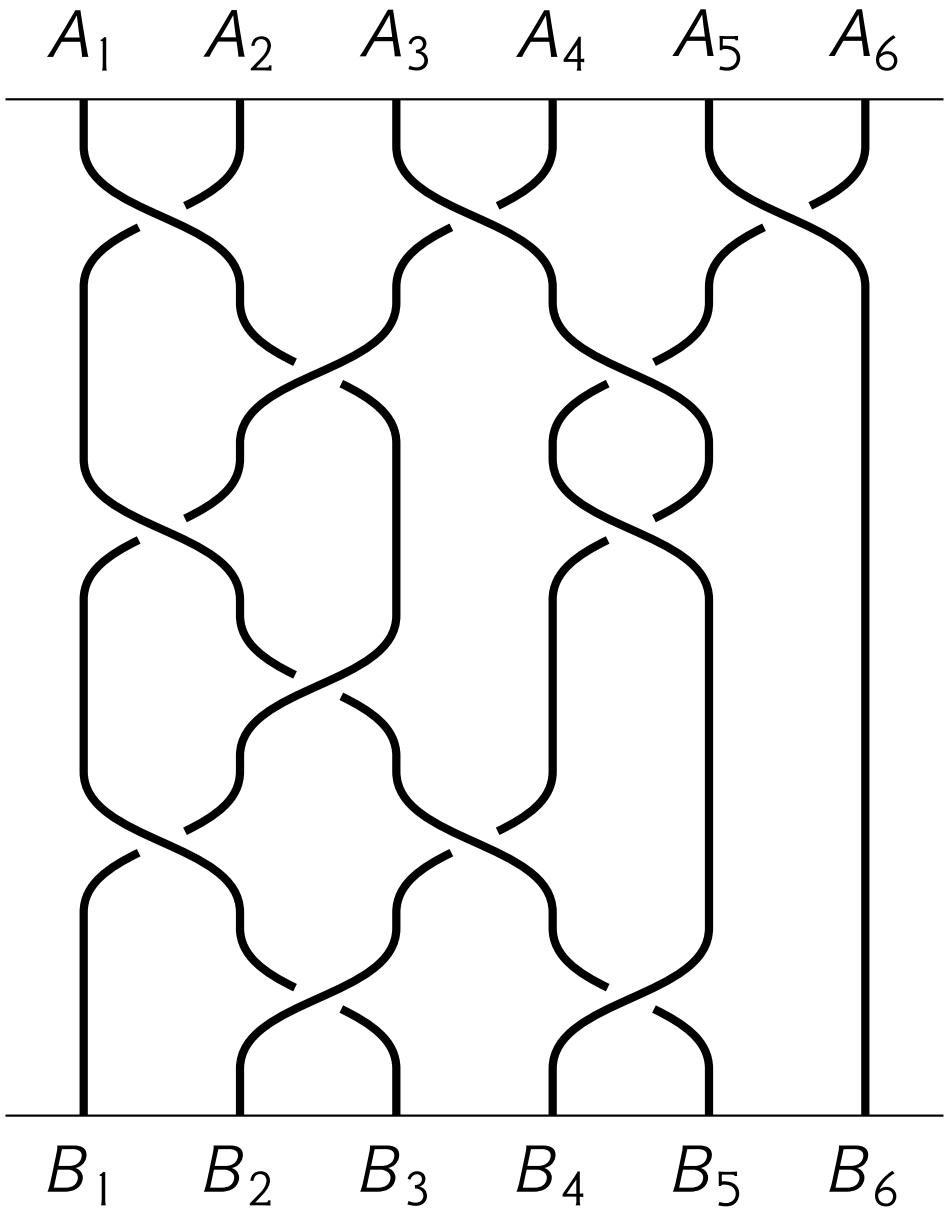
- Η πρώτη καταγεγραμμένη μαθηματική μορφή συναντάται στα γραπτά του Gauss
- Ο πρώτος αυστηρός μαθηματικός τους ορισμός έγινε από τον Artin στο άρθρο του *Theorie der Zöpfe*.
- Έκτοτε μελετώνται εκτενώς από τοπολόγους και αλγεβριστές

Η Ομάδα των Πλεξίδων



Από το σημειωματάριο του Gauss

Η Ομάδα των Πλεξίδων



Η Ομάδα των Πλεξίδων

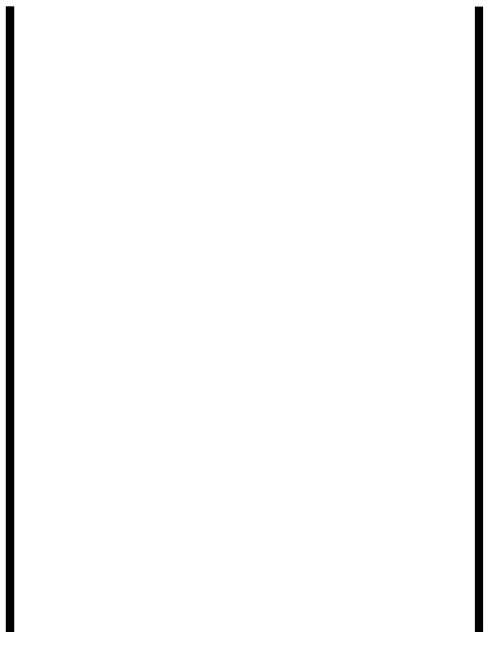
Ορισμός

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

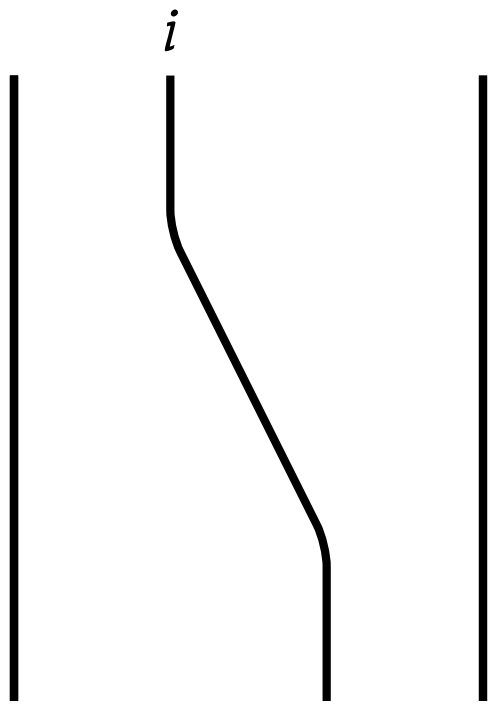
$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{c} \sigma_i\sigma_j = \sigma_j\sigma_i \quad \gamma\iota\alpha \;\; |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \quad \gamma\iota\alpha \;\; |i-j| = 1 \end{array} \right\rangle \quad (1)$$

Η Ομάδα των Πλειάδων

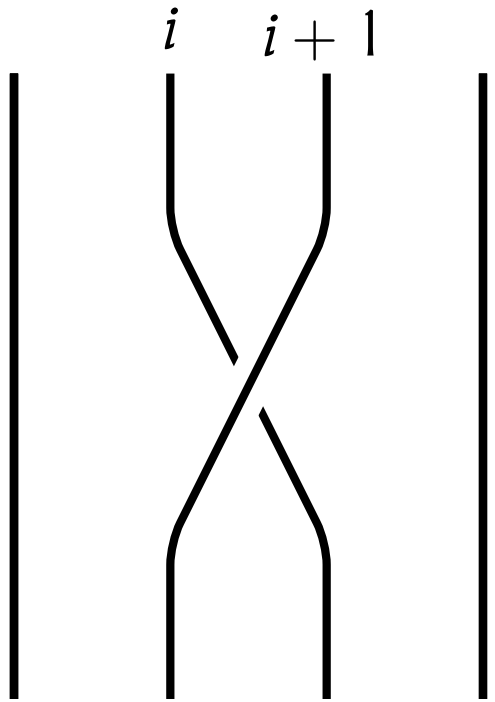
Η Ομάδα των Πλειάδων



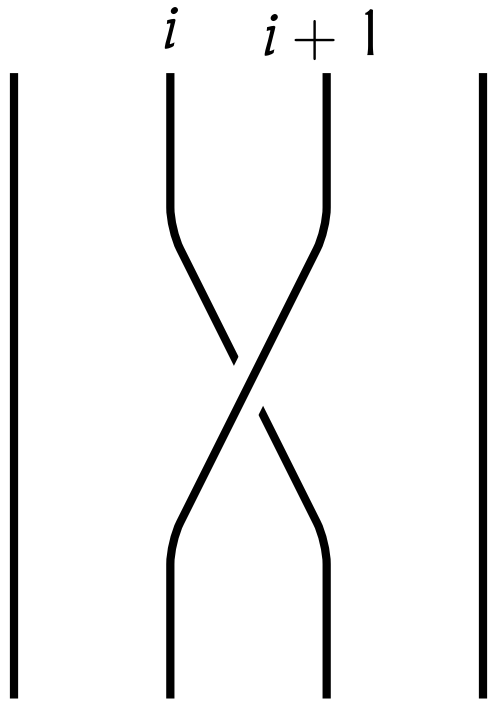
Η Ομάδα των Πλεξίδων



Η Ομάδα των Πλεξίδων



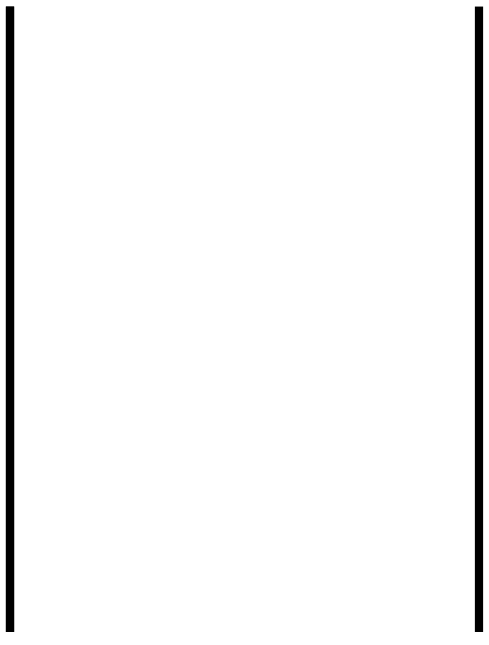
Η Ομάδα των Πλεξίδων



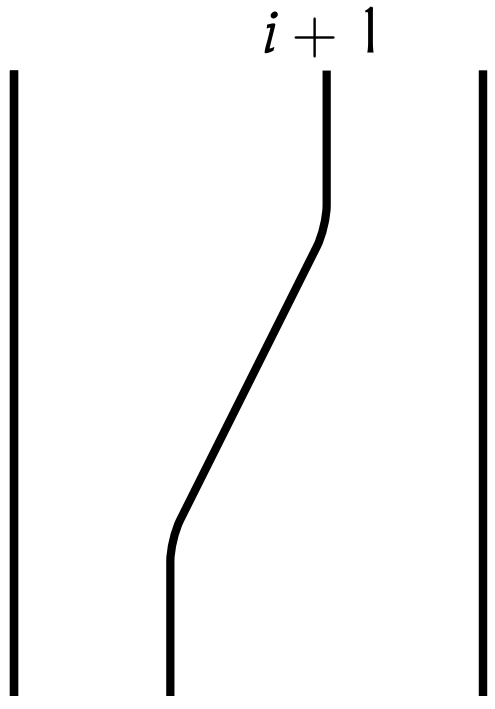
Ο γεννήτορας σ_i

Η Ομάδα των Πλειάδων

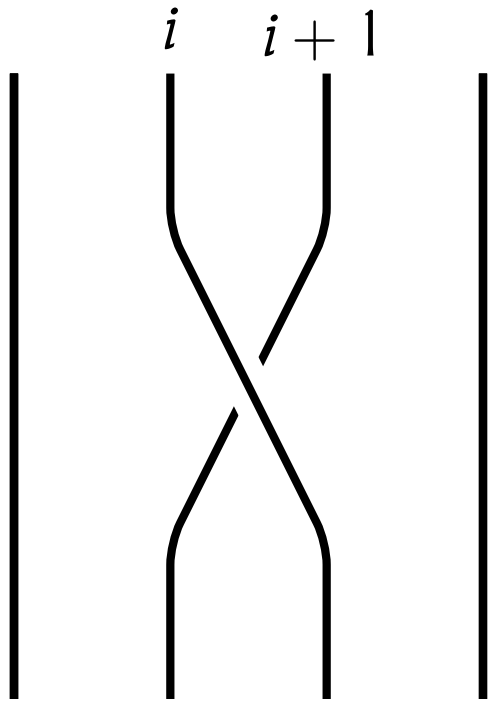
Η Ομάδα των Πλειάδων



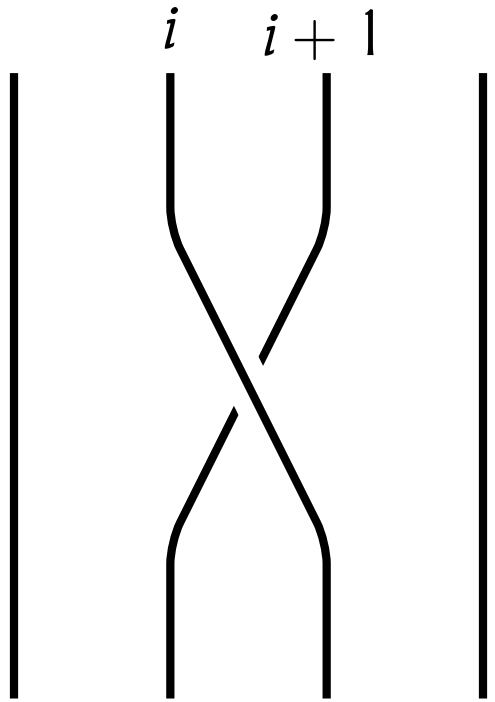
Η Ομάδα των Πλεξίδων



Η Ομάδα των Πλεξίδων

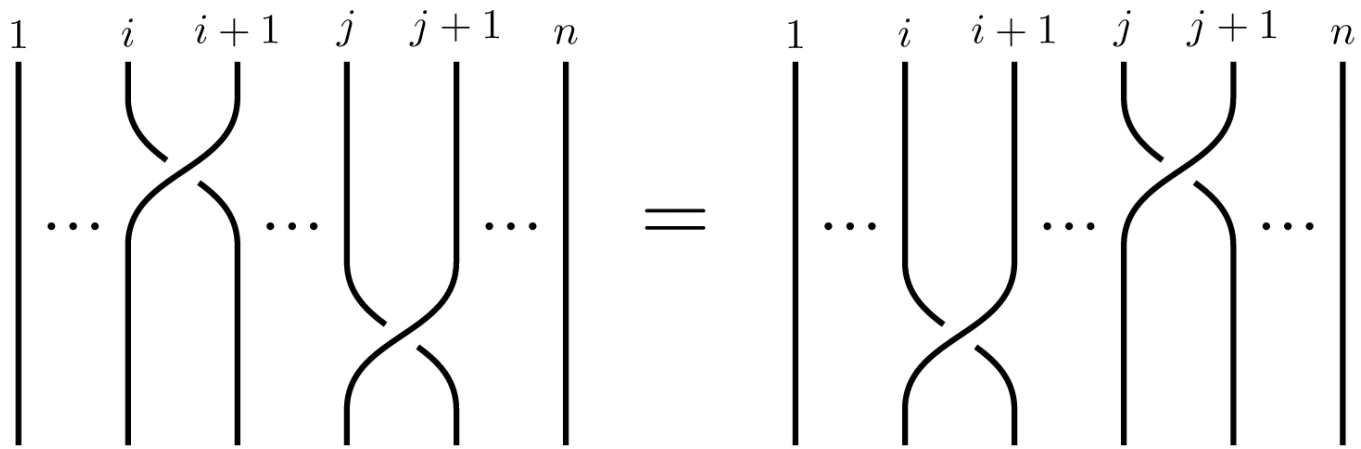


Η Ομάδα των Πλεξίδων



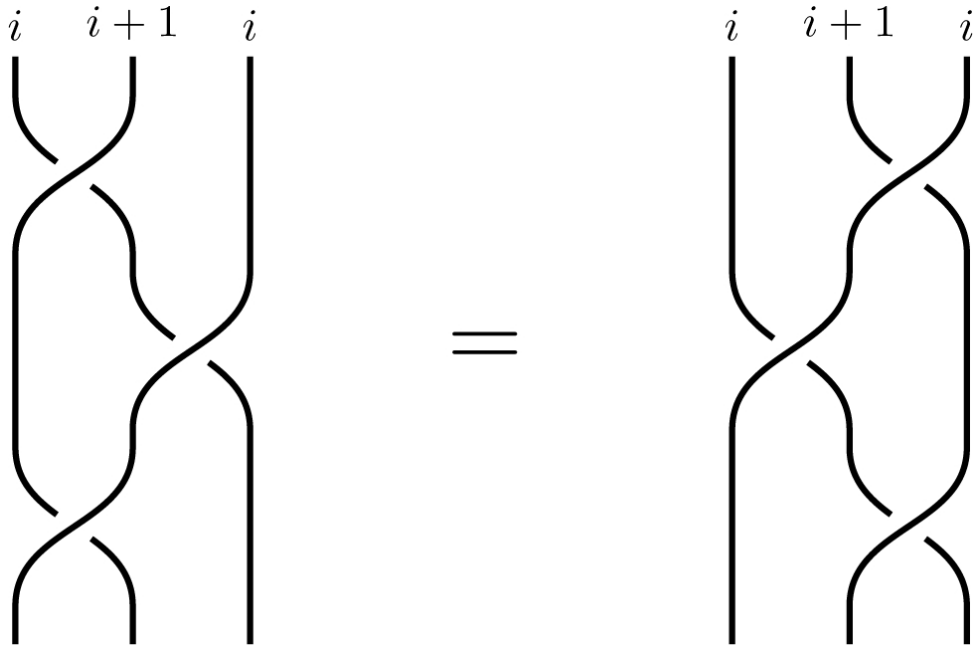
και ο γεννήτορας σ_i^{-1}

Η Ομάδα των Πλεξίδων



Η πρώτη σχέση πλεξίδων $\sigma_i\sigma_j = \sigma_j\sigma_i$ για $|i-j| \geqslant 2$.

Η Ομάδα των Πλεξίδων



Η δεύτερη σχέση πλεξίδων $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ για $|i-j| = 1$.

Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

1. **Προβλήματα Απόφασης** (Decision Problems)

Word Problem

Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

1. **Προβλήματα Απόφασης** (Decision Problems)

2. **Προβλήματα Εύρεσης**(Search Problems)

Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

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)

Αλγοριθμικά Προβλήματα της Θεωρίας Ομάδων

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

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:

ΠΡΟΒΛΗΜΑΤΑ ΣΥΖΥΓΙΑΣ:

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

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

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 $\beta_2 = \beta'' \beta_1 \beta''^{-1}$.

Κανονικές Μορφές

Ορισμός

Κανονική μορφή μιάς ομάδας G, με ένα σύνολο γεννητόρων S, είναι μια επιλογή μιας *συγκεκριμένης λέξης* για κάθε στοιχείο $g \in G$.

Κανονικές Μορφές

Ορισμός

Κανονική μορφή μιάς ομάδας G, με ένα σύνολο γεννητόρων S, είναι μια επιλογή μιας *συγκεκριμένης λέξης* για κάθε στοιχείο $g \in G$.

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

Κανονικές Μορφές

Ορισμός

Κανονική μορφή μιάς ομάδας G, με ένα σύνολο γεννητόρων S, είναι μια επιλογή μιας *συγκεκριμένης λέξης* για κάθε στοιχείο $g \in G$.

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.

Word Problem

Word Problem (1)

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

Word Problem

Word Problem (1)

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

ΙΣΟΔΥΝΑΜΑ:

Word Problem

Word Problem (1)

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

ΙΣΟΔΥΝΑΜΑ:

Word Problem (2)

Έστω g_1, g_2 στοιχεία στην G. Βρείτε αν ισχύει: $g_1 = g_2$.

Word Problem

Word Problem (1)

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

ΙΣΟΔΥΝΑΜΑ:

Word Problem (2)

Έστω g_1, g_2 στοιχεία στην G. Βρείτε αν ισχύει: $g_1 = g_2$.

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

Κανονική Μορφή Garside

Θεώρημα (Garside-1969)

Στην ομάδα B_{n+1}, κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

Κανονική Μορφή Garside

Θεώρημα (Garside-1969)

Στην ομάδα B_{n+1}, κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

όπου:

- Δ η ***θεμελιώδης λέξη***

Κανονική Μορφή Garside

Θεώρημα (Garside-1969)

Στην ομάδα B_{n+1}, κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

όπου:

- Δ η ***θεμελιώδης λέξη***
- $m \in \mathbb{Z}$

Κανονική Μορφή Garside

Θεώρημα (Garside-1969)

Στην ομάδα B_{n+1}, κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

όπου:

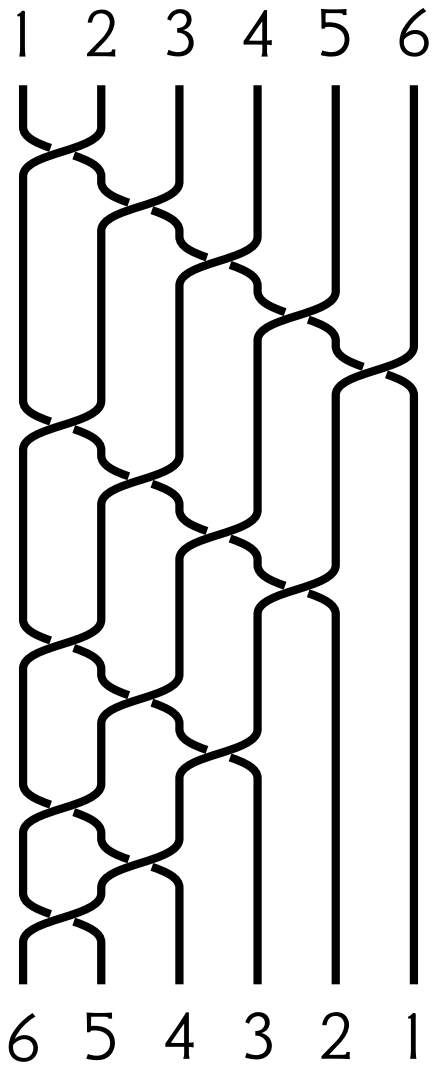
- Δ η ***θεμελιώδης λέξη***
- $m \in \mathbb{Z}$
- $\bar{A}$ ***θετική λέξη***, μοναδικά εκφρασμένη.

Χρήσιμοι Ορισμοί-Η Θεμελιώδης Λέξη

Ορισμός

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.

Χρήσιμοι Ορισμοί-Η Θεμελιώδης Λέξη



$$\Delta_5 = (\sigma_1\sigma_2\sigma_3\sigma_4\sigma_5)(\sigma_1\sigma_2\sigma_3\sigma_4)(\sigma_1\sigma_2\sigma_3)(\sigma_1\sigma_2)\sigma_1$$

Θετική Λέξη

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

Χρήσιμοι Ορισμοί

Θετική Λέξη

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

$D(W)$

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

Ορισμός

Έστω W μια λέξη μήκους l στην B_{n+1} και έστω ότι το $D(W)$ αποτελείται από m λέξεις:

$$W_1 \equiv \sigma_i\sigma_j\sigma_k\ldots,\ W_2 \equiv \sigma_p\sigma_q\sigma_r\ldots,\ldots,\ W_m \equiv \sigma_x\sigma_y\sigma_z\ldots$$

Τότε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των λέξεων:
$W_1, W_2, \ldots, W_m$ και των αριθμών:

$$P_1 \equiv ijk\ldots,\ P_2 \equiv pqr\ldots,\ldots,\ P_m \equiv xyz\ldots.$$

Οι αριθμοί $P_i, i \in \{1,\ldots,m\}$ είναι διακεκριμένοι μεταξύ τους. Έστω P_r ο μικρότερος εξ' αυτών, τότε η αντίστοιχη λέξη W_r θα καλείται **βάση** του $D(W)$.

Χρήσιμοι Ορισμοί

Ορισμός

Έστω A, B, W θετικές λέξεις. Αν για κάποια $W_i \in D(W)$ ισχύει

$$W_i = A\Delta B$$

θα λέμε ότι η Δ είναι **παράγοντας** της W, διαφορετικά θα λέμέ ότι η W είναι **πρώτη** ως προς την Δ.

Συμβολισμός

Αν B είναι πρώτη ως προς την Δ και B είναι βάση του $D(B)$ θα την συμβολίζουμε με $\overline{\boldsymbol{B}}$.

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$,

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$, όπου:
  $W \equiv W_1(x_1)^{-1} W_2(x_2)^{-1} \dots W_s(x_s)^{-1} W_{s+1}$

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$, όπου:
  $W \equiv W_1(x_1)^{-1}W_2(x_2)^{-1}\ldots W_s(x_s)^{-1}W_{s+1}$
- $\forall \sigma_r$ γεννήτορα, $\exists X_r \in B_{n+1}$:

$$\sigma_r X_r = \Delta \Rightarrow (\sigma_r)^{-1} = X_r \Delta^{-1}$$

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$, όπου:
  $W \equiv W_1(x_1)^{-1}W_2(x_2)^{-1}\ldots W_s(x_s)^{-1}W_{s+1}$
- $\forall \sigma_r$ γεννήτορα, $\exists X_r \in B_{n+1}$:

$$\sigma_r X_r = \Delta \Rightarrow (\sigma_r)^{-1} = X_r \Delta^{-1}$$

- $W = W_1 X_1 \Delta^{-1} W_2 X_2 \Delta^{-1} \ldots W_s X_s \Delta^{-1} W_{s+1}$

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$, όπου:
  $W \equiv W_1(x_1)^{-1}W_2(x_2)^{-1}\ldots W_s(x_s)^{-1}W_{s+1}$
- $\forall \sigma_r$ γεννήτορα, $\exists X_r \in B_{n+1}$:

$$\sigma_r X_r = \Delta \Rightarrow (\sigma_r)^{-1} = X_r \Delta^{-1}$$

- $W = W_1 X_1 \Delta^{-1} W_2 X_2 \Delta^{-1} \ldots W_s X_s \Delta^{-1} W_{s+1}$
- Επίσης $\forall \sigma_i$ έχουμε:

$$\sigma_i \Delta^{2m+1} = \Delta^{2m+1} \sigma_{n+1-i}$$

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Έστω $W \in B_{n+1}$, όπου:
  $W \equiv W_1(x_1)^{-1}W_2(x_2)^{-1}\ldots W_s(x_s)^{-1}W_{s+1}$
- $\forall \sigma_r$ γεννήτορα, $\exists X_r \in B_{n+1}$:

$$\sigma_r X_r = \Delta \Rightarrow (\sigma_r)^{-1} = X_r \Delta^{-1}$$

- $W = W_1 X_1 \Delta^{-1} W_2 X_2 \Delta^{-1} \ldots W_s X_s \Delta^{-1} W_{s+1}$
- Επίσης $\forall \sigma_i$ έχουμε:

$$\sigma_i \Delta^{2m+1} = \Delta^{2m+1} \sigma_{n+1-i}$$

- $W = \Delta^{-s} P$, όπου P μια θετική λέξη

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Αν P πρώτη ως προς Δ τότε $W = \Delta^{-s}\overline{P}$

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Αν P πρώτη ως προς Δ τότε $W = \Delta^{-s}\overline{P}$
- Αν όχι γράφουμε $P = \Delta^{t}\overline{A}$, με t μέγιστο για όλες τις $P_i \in D(P)$.

Κανονική Μορφή Garside - Σκιαγράφηση Απόδειξης

- Αν P πρώτη ως προς Δ τότε $W = \Delta^{-s}\overline{P}$
- Αν όχι γράφουμε $P = \Delta^t \overline{A}$, με t μέγιστο για όλες τις $P_i \in D(P)$.
-

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

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

- Ειναι μοναδική η γραφή.

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

- Ειναι μοναδική η γραφή.
- Αποτελεί λύση του word problem

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

- Ειναι μοναδική η γραφή.
- Αποτελεί λύση του word problem
- Όλες οι βελτιωμένες λύσεις ακολουθούν τη λογική του Garside (πλην του Dehornoy)

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

- Ειναι μοναδική η γραφή.
- Αποτελεί λύση του word problem
- Όλες οι βελτιωμένες λύσεις ακολουθούν τη λογική του Garside (πλην του Dehornoy)
- Η Δ^2 παράγει το κέντρο της B_n.

Κανονική Μορφή Garside

Θεώρημα (Garside, 1969)

Στην B_{n+1} κάθε λέξη W μπορεί να εκφρασθεί μοναδικά στην μορφή $\Delta^m \bar{A}$

- Ειναι μοναδική η γραφή.
- Αποτελεί λύση του word problem
- Όλες οι βελτιωμένες λύσεις ακολουθούν τη λογική του Garside (πλην του Dehornoy)
- Η Δ^2 παράγει το κέντρο της B_n.
- Έλυσε το conjugacy problem.

Η μέθοδος Handle Reduction του Dehornoy

- Πρώτο άρθρο "A Fast Method for Comparing Braids", (1997)

Η μέθοδος Handle Reduction του Dehornoy

- Πρώτο άρθρο "A Fast Method for Comparing Braids", (1997)
- Λύνει το word problem

Η μέθοδος Handle Reduction του Dehornoy

- Πρώτο άρθρο "A Fast Method for Comparing Braids", (1997)
- Λύνει το word problem
- Αποδεικνύει την ύπαρξη μιας γραμμικής διάταξης στην Ομάδα των Πλεξίδων

Η μέθοδος Handle Reduction του Dehornoy

- Πρώτο άρθρο "A Fast Method for Comparing Braids", (1997)
- Λύνει το word problem
- Αποδεικνύει την ύπαρξη μιας γραμμικής διάταξης στην Ομάδα των Πλεξίδων
- Δεν δίνει λύση στο conjugacy problem

Η μέθοδος Handle Reduction του Dehornoy

Ορισμός

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.

Ορισμός

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}.

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα, 1997

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα, 1997

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

- Λύνει το word problem

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα, 1997

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

- Λύνει το word problem
- Επάγει μια ολική διάταξη στην B_n

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα, 1997

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

- Λύνει το word problem
- Επάγει μια ολική διάταξη στην B_n

Η Διάταξη στην B_n

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

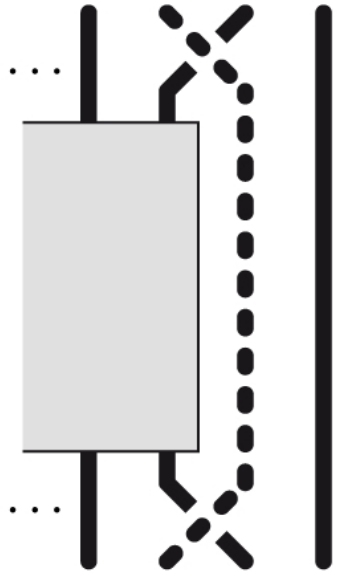
Η μέθοδος Handle Reduction του Dehornoy

- 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 $j \geqslant i$.

Η μέθοδος Handle Reduction του Dehornoy

- 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 $j \geqslant i$.
- 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.

Η μέθοδος Handle Reduction του Dehornoy



Μια σ_i-λαβή προσήμου $-$

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

$1^{η}$ Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

- *Κάθε λέξη που περιέχει μία λαβή, περιέχει και μία καλή λαβή*

Η μέθοδος Handle Reduction του Dehornoy

- *Κάθε λέξη που περιέχει μία λαβή, περιέχει και μία καλή λαβή*
- Η **πρώτη λαβή** σε μια λέξη w είναι αυτή που ολοκληρώνεται πρώτη όταν κανείς ξεκινήσει να διαβάζει την w από τα αριστερά

Η μέθοδος Handle Reduction του Dehornoy

- *Κάθε λέξη που περιέχει μία λαβή, περιέχει και μία καλή λαβή*
- Η **πρώτη λαβή** σε μια λέξη w είναι αυτή που ολοκληρώνεται πρώτη όταν κανείς ξεκινήσει να διαβάζει την w από τα αριστερά
- Έστω w μια λέξη πλεξίδας που περιέχει τουλάχιστον μια λαβή. Τότε η πρώτη λαβή της w είναι καλή λαβή

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

1η Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

$1^{η}$ Ισοδύναμη πρόταση

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

$2^{η}$ Ισοδύναμη πρόταση

Κάθε λέξη πλεξίδας είναι ισοδύναμη με μια λέξη που δεν περιέχει καλή λαβή

Η μέθοδος Handle Reduction του Dehornoy

Η κεντρική ιδέα της μεθόδου

- **free group reduction** (αναγωγή ελεύθερων ομάδων): Η αντικατάσταση των $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i$ με την κενή λέξη

Η μέθοδος Handle Reduction του Dehornoy

Η κεντρική ιδέα της μεθόδου

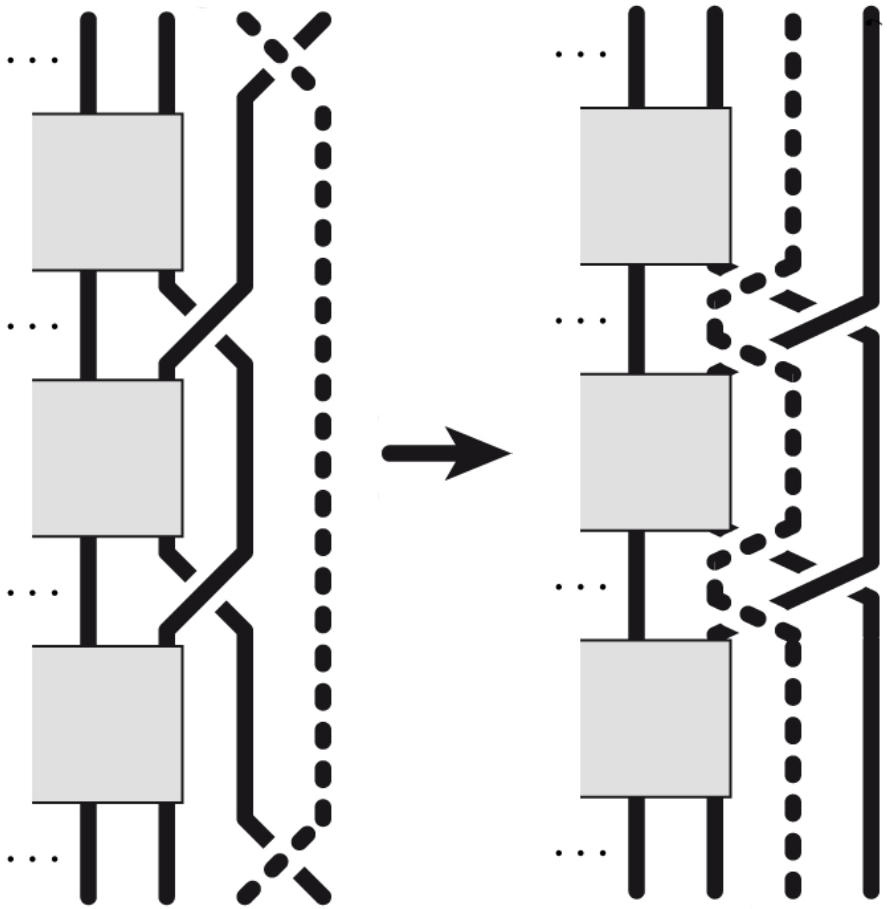
- **free group reduction** (αναγωγή ελεύθερων ομάδων): Η αντικατάσταση των $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i$ με την κενή λέξη
- Μπορούμε να επεκτείνουμε την αναγωγή των ελεύθερων ομάδων;

Η μέθοδος Handle Reduction του Dehornoy

Handle Reduction

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 $\sigma_{i-1}^{-e}\sigma_i^{-1}\sigma_{i-1}^{e}$, όπου $e = \pm 1$

Η μέθοδος Handle Reduction του Dehornoy



handle reduction

Η μέθοδος Handle Reduction του Dehornoy

- 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.

Η μέθοδος Handle Reduction του Dehornoy

- 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.
- Θα γράφουμε $\boldsymbol{red^k(w)}$ για $\underbrace{red(red(\ldots red(w))\ldots)}_{\text{k φορές}}$

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

$1^{η}$ Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

$1^{η}$ Ισοδύναμη πρόταση

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

$2^{η}$ Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

Το Βασικό Θεώρημα

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

$1^η$ Ισοδύναμη πρόταση

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

$2^η$ Ισοδύναμη πρόταση

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

$3^η$ Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

$3^{η}$ Ισοδύναμη πρόταση

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

Η μέθοδος Handle Reduction του Dehornoy

$3^{η}$ Ισοδύναμη πρόταση

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

- 3 Κεντρικά Λήμματα

Η μέθοδος Handle Reduction του Dehornoy

$3^{η}$ Ισοδύναμη πρόταση

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

- 3 Κεντρικά Λήμματα
- Πολλές βοηθητικές προτάσεις

Η μέθοδος Handle Reduction του Dehornoy

$3^{η}$ Ισοδύναμη πρόταση

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

- 3 Κεντρικά Λήμματα
- Πολλές βοηθητικές προτάσεις
- Πολλούς και τεχνικούς ορισμούς

Η παράσταση των Birman, Ko και Lee

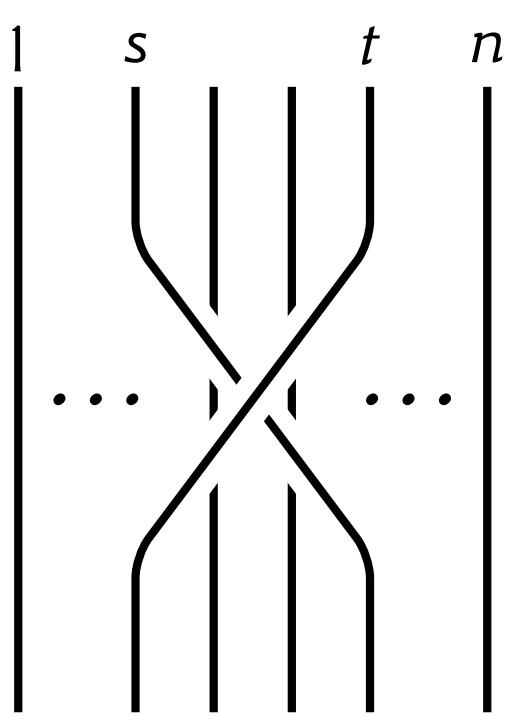
Ορισμός

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:

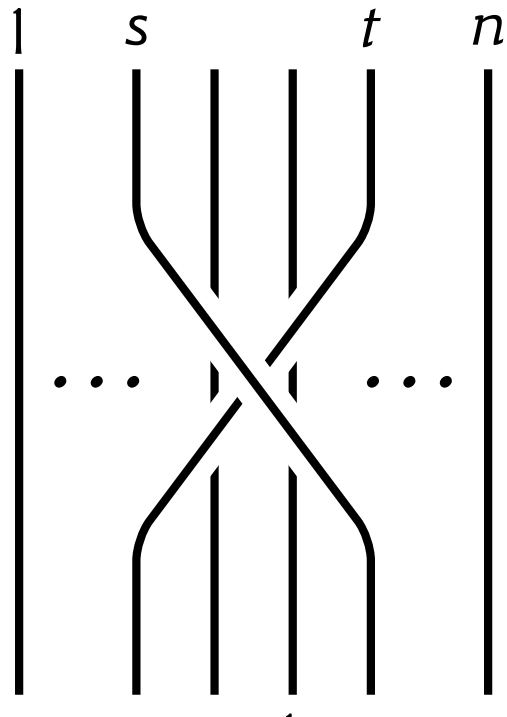
$$\alpha_{ts} = (\sigma_{t-1}\sigma_{t-2}\dots\sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1}\dots\sigma_{t-2}^{-1}\sigma_{t-1}^{-1})$$

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

Η παράσταση των Birman, Ko και Lee



α_{ts}



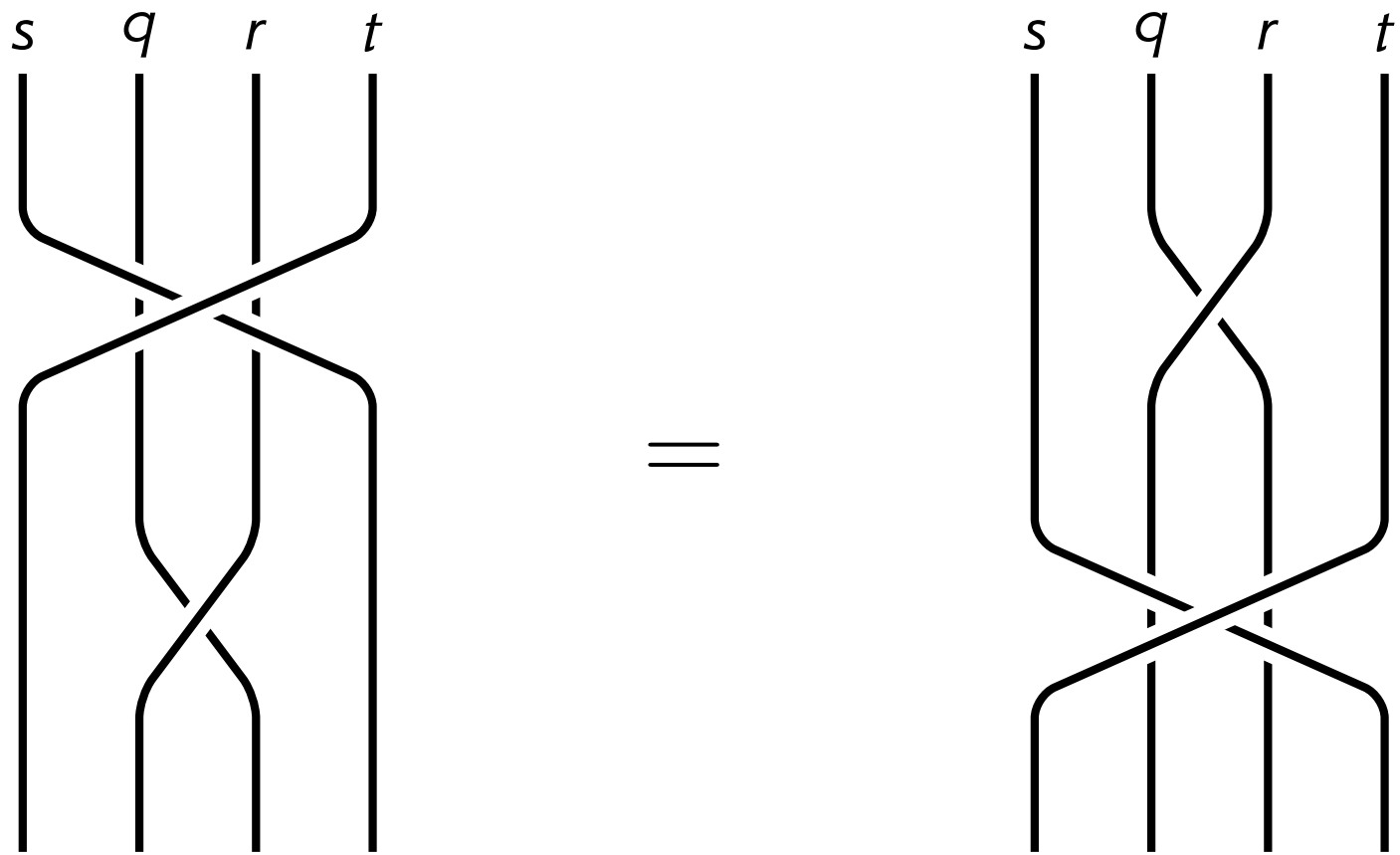
α_{ts}^{-1}

Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ αν $(t-r)(t-q)(s-r)(s-q) > 0$.

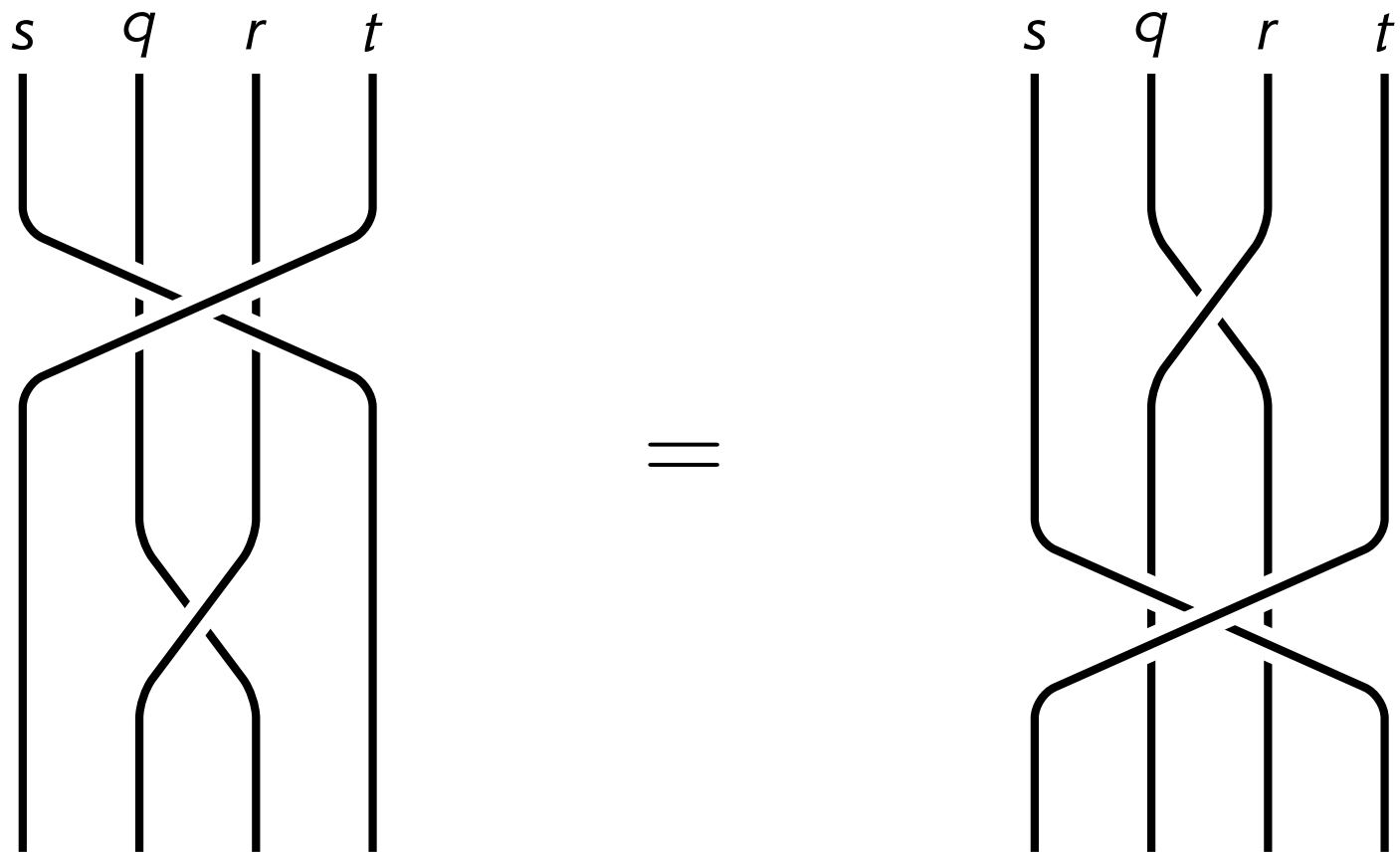
Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ αν $(t-r)(t-q)(s-r)(s-q) > 0$.



Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ αν $(t-r)(t-q)(s-r)(s-q) > 0$.



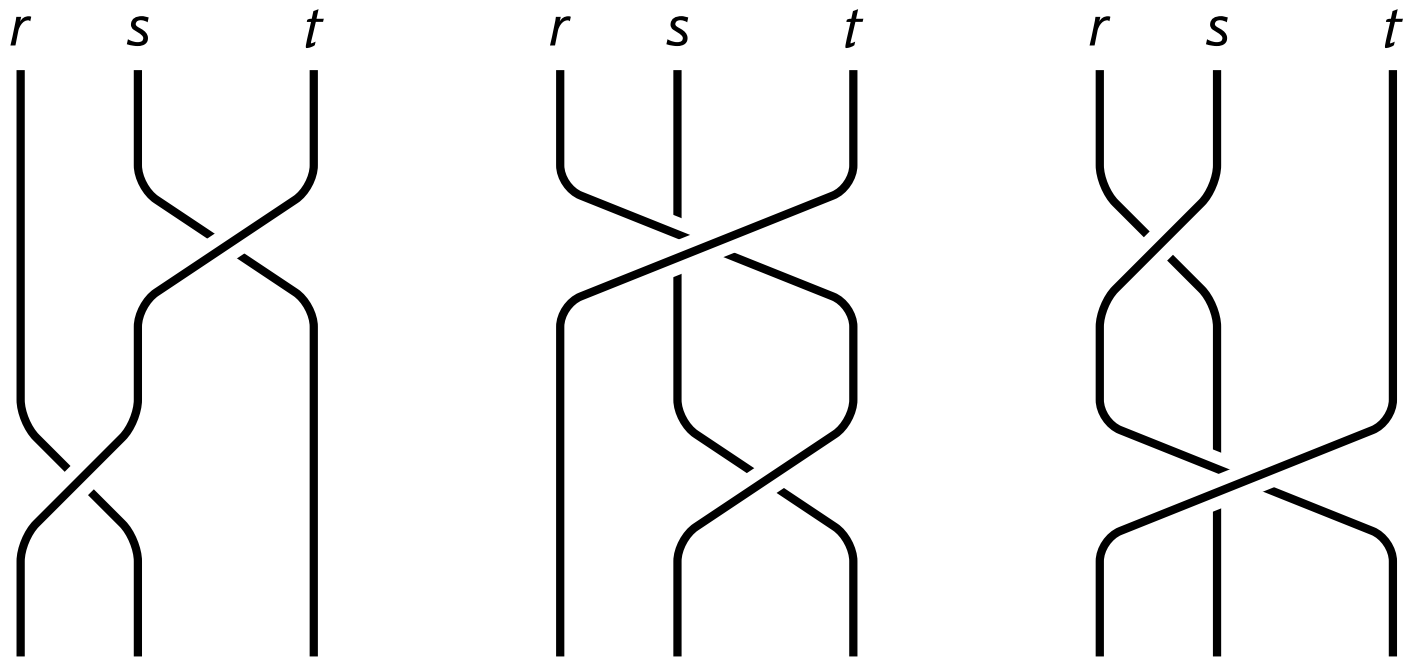
Η σχέση $\alpha_{ts}\alpha_{rq} = \alpha_{rq}\alpha_{ts}$ για $1 \leqslant s < q < r \leqslant t$.

Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{sr} = \alpha_{tr}\alpha_{ts} = \alpha_{sr}\alpha_{tr}$ για $1 \leqslant r < s < t \leqslant n$.

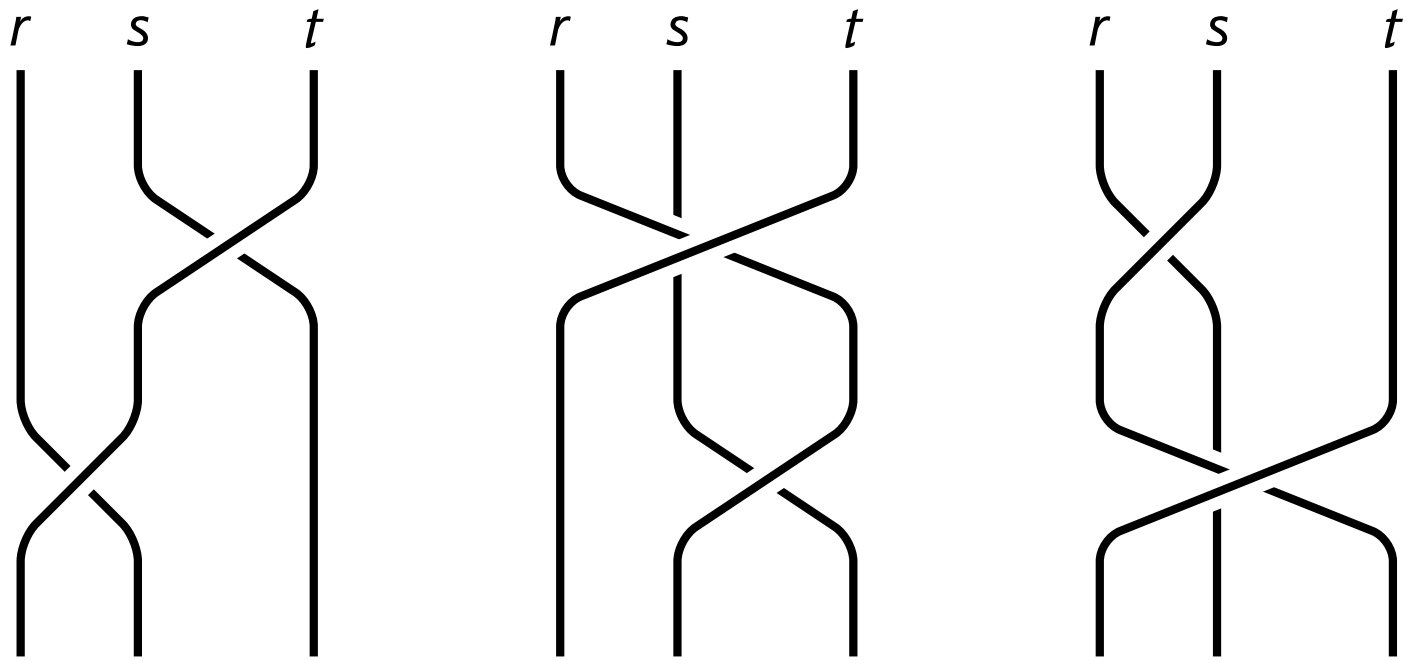
Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{sr} = \alpha_{tr}\alpha_{ts} = \alpha_{sr}\alpha_{tr}$ για $1 \leqslant r < s < t \leqslant n$.



Η παράσταση των Birman, Ko και Lee

- $\alpha_{ts}\alpha_{sr} = \alpha_{tr}\alpha_{ts} = \alpha_{sr}\alpha_{tr}$ για $1 \leqslant r < s < t \leqslant n$.



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

Η παράσταση των Birman, Ko και Lee

Ορισμός

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 $\boldsymbol{\delta_n}$

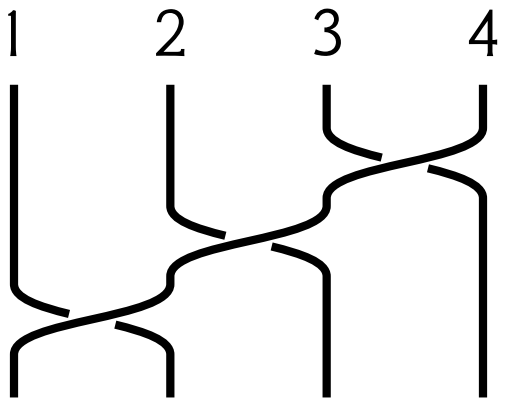
Η παράσταση των Birman, Ko και Lee

Ορισμός

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 $\boldsymbol{\delta_n}$



Η παράσταση των Birman, Ko και Lee

ΙΔΙΟΤΗΤΕΣ ΤΗΣ δ_n

Η παράσταση των Birman, Ko και Lee

ΙΔΙΟΤΗΤΕΣ ΤΗΣ δ_n

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

Η παράσταση των Birman, Ko και Lee

ΙΔΙΟΤΗΤΕΣ ΤΗΣ δ_n

1. $\Delta_n^2 = \delta_n^n$
2. $\delta_n = \alpha_{ts} A = B \alpha_{ts} \quad$ για κάθε $\alpha_{ts} \in B_n$

Η παράσταση των Birman, Ko και Lee

ΙΔΙΟΤΗΤΕΣ ΤΗΣ δ_n

1. $\Delta_n^2 = \delta_n^n$
2. $\delta_n = \alpha_{ts} A = B \alpha_{ts} \quad$ για κάθε $\alpha_{ts} \in B_n$
3. $\alpha_{ts} \delta_n = \delta_n \alpha_{t+1,s+1} \quad$ για κάθε $\alpha_{ts} \in B_n$

Η παράσταση των Birman, Ko και Lee

Θεώρημα

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.

Εφαρμογές στην Κρυπτογραφία

- Κρυπτογραφία

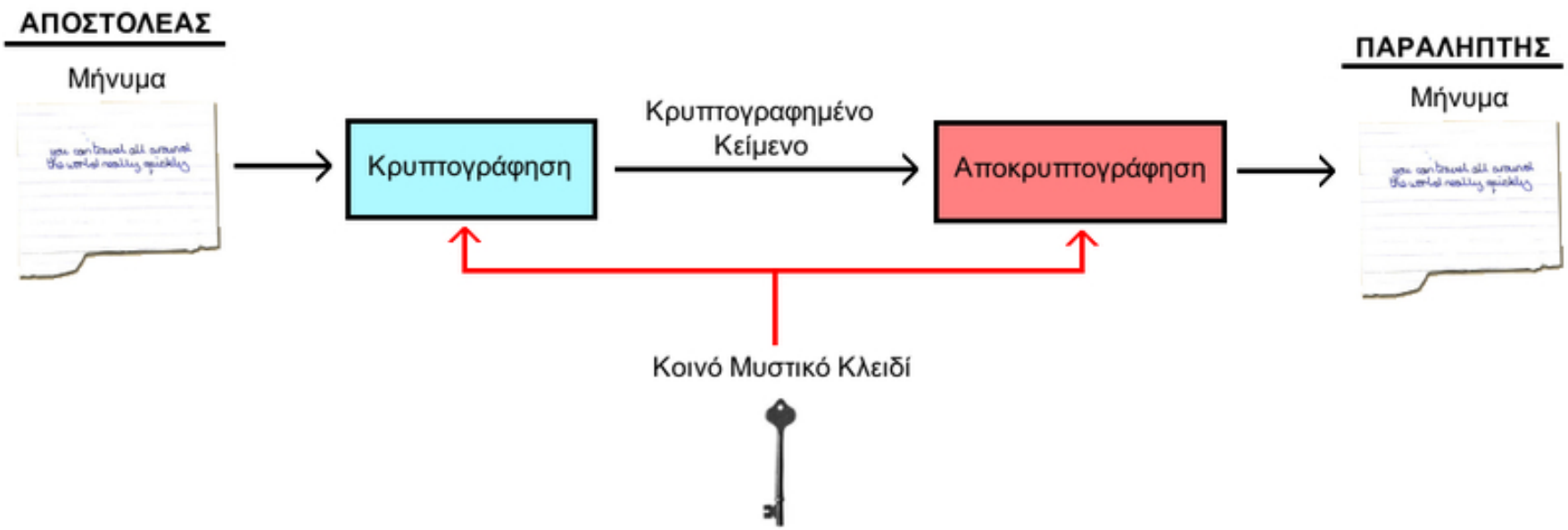
Εφαρμογές στην Κρυπτογραφία

- Κρυπτογραφία
- Ιστορικά

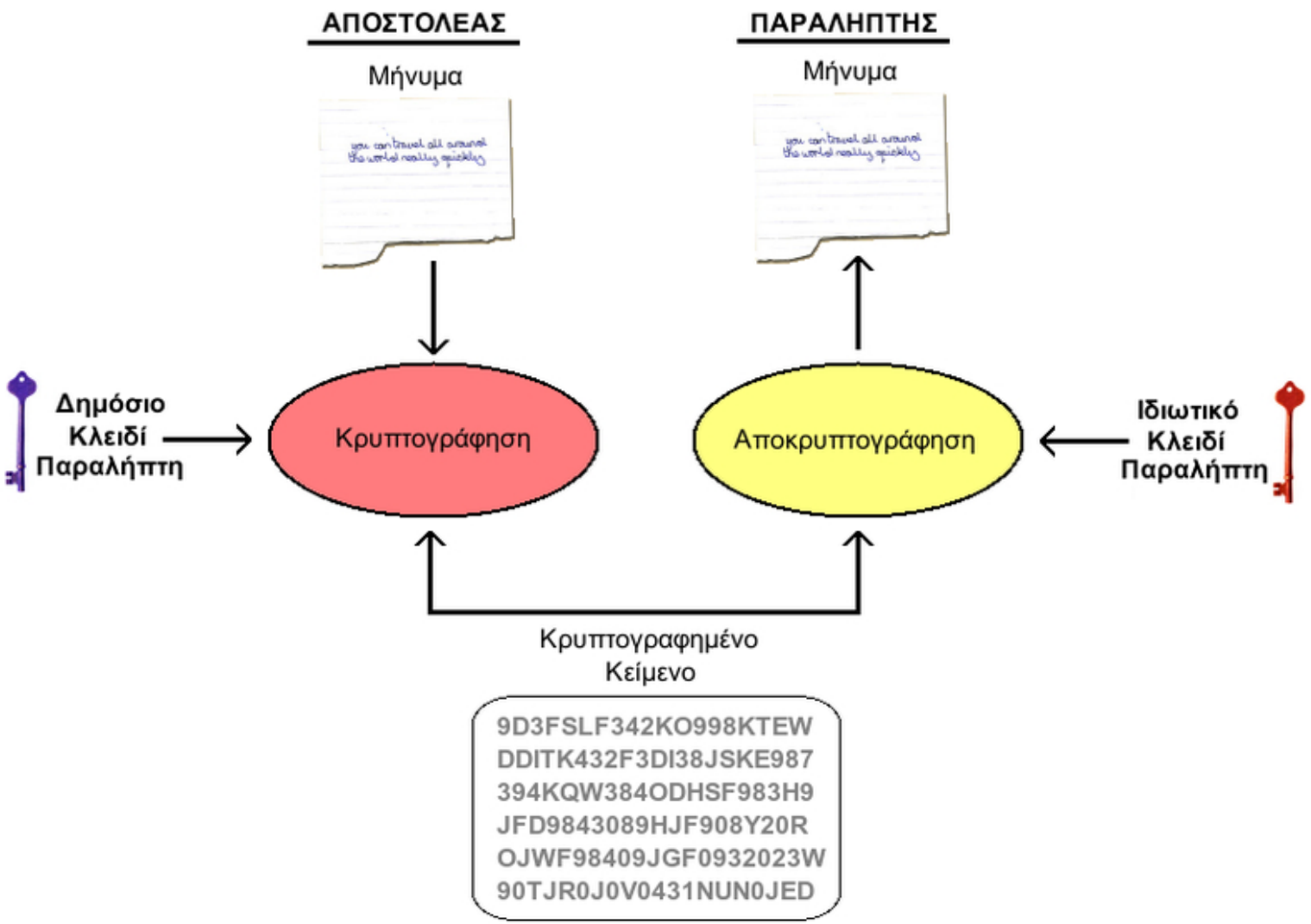
Εφαρμογές στην Κρυπτογραφία

- Κρυπτογραφία
- Ιστορικά
- Ορισμοί

Κρυπτογράφηση Συμμετρικού κλειδιού:



Κρυπτογράφηση Ασύμμετρου κλειδιού:



Εφαρμογές στην Κρυπτογραφία

Γιατί οι ομάδες των πλεξίδων;

Εφαρμογές στην Κρυπτογραφία

Γιατί οι ομάδες των πλεξίδων;

- Τα στοιχεία της περιγράφονται ως δεδομένα εύκολα διαχειρίσιμα από τους υπολογιστές

Εφαρμογές στην Κρυπτογραφία

Γιατί οι ομάδες των πλεξίδων;

- Τα στοιχεία της περιγράφονται ως δεδομένα εύκολα διαχειρίσιμα από τους υπολογιστές
- Η πράξη της ομάδας είναι απλή. Το γινόμενο δύο στοιχείων a, b είναι η αλληλουχία ab

Εφαρμογές στην Κρυπτογραφία

Γιατί οι ομάδες των πλεξίδων;

- Τα στοιχεία της περιγράφονται ως δεδομένα εύκολα διαχειρίσιμα από τους υπολογιστές
- Η πράξη της ομάδας είναι απλή. Το γινόμενο δύο στοιχείων a, b είναι η αλληλουχία ab
- Για τις ανάγκες της κρυπτογραφίες μπορούμε να κρύψουμε τους παράγοντες του ab μετετρέποντας το στην κανονική του μορφή

Εφαρμογές στην Κρυπτογραφία

Γιατί οι ομάδες των πλεξίδων;

- Τα στοιχεία της περιγράφονται ως δεδομένα εύκολα διαχειρίσιμα από τους υπολογιστές
- Η πράξη της ομάδας είναι απλή. Το γινόμενο δύο στοιχείων a, b είναι η αλληλουχία ab
- Για τις ανάγκες της κρυπτογραφίες μπορούμε να κρύψουμε τους παράγοντες του ab μετετρέποντας το στην κανονική του μορφή
- Υπάρχουν ακόμα άλυτα ή και δύσκολα προβλήματα να χρησιμοποιηθούν

Εφαρμογές στην Κρυπτογραφία

- 1999, I. Anshel, M. Anshel, D. Goldfeld

Εφαρμογές στην Κρυπτογραφία

- 1999, I. Anshel, M. Anshel, D. Goldfeld
- Κρυπτογραφικό πρωτόκολλο για μη αβελιανές ομάδες

Εφαρμογές στην Κρυπτογραφία

- 1999, I. Anshel, M. Anshel, D. Goldfeld
- Κρυπτογραφικό πρωτόκολλο για μη αβελιανές ομάδες
- Υπόθεση: Το conjugacy problem είναι δύσκολο

Εφαρμογές στην Κρυπτογραφία

- 1999, I. Anshel, M. Anshel, D. Goldfeld
- Κρυπτογραφικό πρωτόκολλο για μη αβελιανές ομάδες
- Υπόθεση: Το conjugacy problem είναι δύσκολο
- Εφαρμόζεται και σε άλλες ομάδες

Εφαρμογές στην Κρυπτογραφία

- 2000, Ko, Lee, Cheon, Han, Kang και Park

Εφαρμογές στην Κρυπτογραφία

- 2000, Ko, Lee, Cheon, Han, Kang και Park
- Μοιάζει με το κρυπτοσύστημα El Gamal

Εφαρμογές στην Κρυπτογραφία

- 2000, Ko, Lee, Cheon, Han, Kang και Park
- Μοιάζει με το κρυπτοσύστημα El Gamal
- Βασίζεται στην δυσκολία επίλυσης του Generalized Conjugacy Search Problem

Εφαρμογή στα Πολυμερή

Εφαρμογή στα Πολυμερή

- Διαπλοκές

Εφαρμογή στα Πολυμερή

- Διαπλοκές
- Μοντέλο σωλήνα

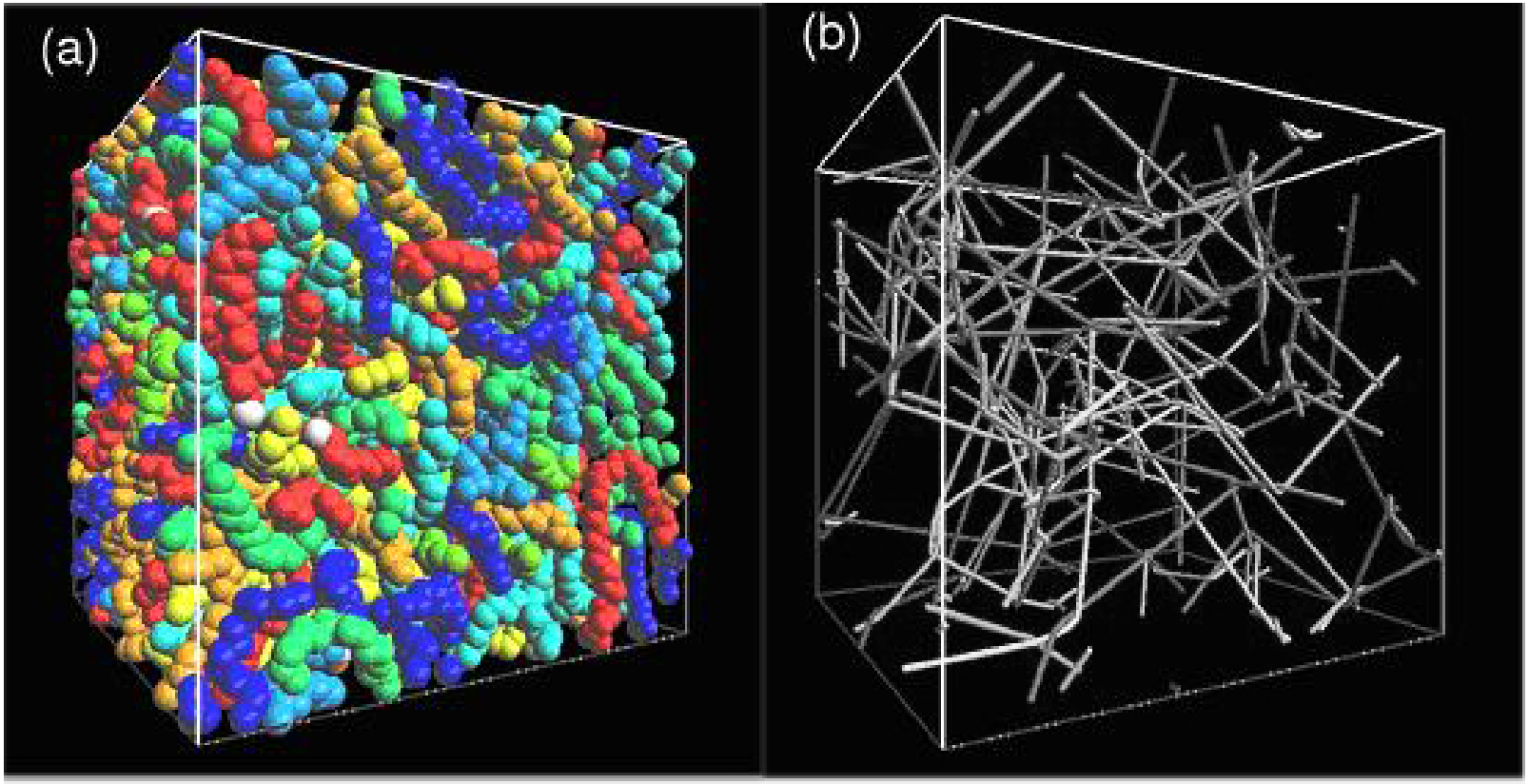
Εφαρμογή στα Πολυμερή

- Διαπλοκές
- Μοντέλο σωλήνα
- Πρωταρχικό μονοπάτι

Εφαρμογή στα Πολυμερή

- Διαπλοκές
- Μοντέλο σωλήνα
- Πρωταρχικό μονοπάτι
- Αλγόριθμος CReTA

Εφαρμογή στα Πολυμερή



(α) Αντιπροσωπευτικό ατομιστικό δείγμα *PE* (πολυαιθυλενίου) και (b) το αντίστοιχο παραγόμενο δίκτυο

Ευχαριστώ πολύ για τον χρόνο σας