Problemas algorítmicos en grupos de Artin-Tits de tipo finito

LXXXVI Encuentro anual de la SOMACHI

Matthieu Calvez (Universidad de La Frontera)

Noviembre 2017

Problemas de Dehn

Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Max Dehn, 1911

Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

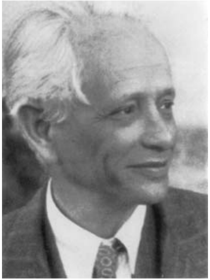
Max Dehn, 1911

Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Max Dehn, 1911

G un grupo con un conjunto finito de generadores X.



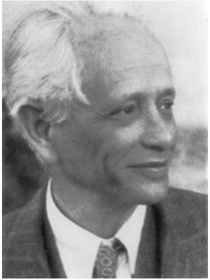
Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Max Dehn, 1911

G un grupo con un conjunto finito de generadores X.

- **Problema de la palabra.** Decidir si dos palabras sobre $X \cup X^{-1}$ representan el mismo elemento de G.



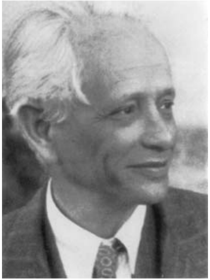
Problemas de Dehn

- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Max Dehn, 1911

G un grupo con un conjunto finito de generadores X.

- **Problema de la palabra.** Decidir si dos palabras sobre $X \cup X^{-1}$ representan el mismo elemento de G.
- **Problema de la conjugación.** Decidir si dos palabras sobre $X \cup X^{-1}$ representan elementos conjugados de G.



Problemas de Dehn

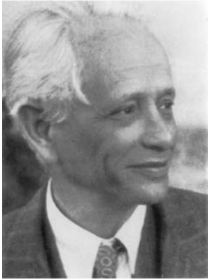
- 1882: Primera definición formal de grupo por generadores y relaciones, Walther Von Dyck.

Max Dehn, 1911

G un grupo con un conjunto finito de generadores X.

- **Problema de la palabra.** Decidir si dos palabras sobre $X \cup X^{-1}$ representan el mismo elemento de G.
- **Problema de la conjugación.** Decidir si dos palabras sobre $X \cup X^{-1}$ representan elementos conjugados de G.

$g_1, g_2 \in G$ son *conjugados* si existe $h \in H$ tal que $g_1 = hg_2h^{-1}$



Formas normales

Formas normales

En muchos casos, se pueden definir formas normales.

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Problema de la palabra

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \, \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$r \in \mathbb{N}$,

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \, \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$r \in \mathbb{N}, \qquad x_{i_1}, \ldots, x_{i_r} \in X,$

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \dots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$$r \in \mathbb{N}, \qquad x_{i_1}, \dots, x_{i_r} \in X, \qquad \varepsilon_1, \dots, \varepsilon_r \in \{\pm 1\}$$

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$$r \in \mathbb{N}, \qquad x_{i_1}, \ldots, x_{i_r} \in X, \qquad \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$$

tales que

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \dots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$$r \in \mathbb{N}, \qquad x_{i_1}, \dots, x_{i_r} \in X, \qquad \varepsilon_1, \dots, \varepsilon_r \in \{\pm 1\}$$

tales que

- $x_{i_{j+1}}^{\varepsilon_{j+1}} \neq x_{i_j}^{-\varepsilon_j}$ y

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$$r \in \mathbb{N}, \qquad x_{i_1}, \ldots, x_{i_r} \in X, \qquad \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$$

tales que

- $x_{i_{j+1}}^{\varepsilon_{j+1}} \neq x_{i_j}^{-\varepsilon_j}$ y
- $x_{i_1}^{\varepsilon_1} \ldots x_{i_r}^{\varepsilon_r}$ representa g.

Formas normales

En muchos casos, se pueden definir formas normales.
Ejemplo: grupo libre $F = \langle x_1, \ldots, x_n | \emptyset \rangle$.

Problema de la palabra

Para todo $g \in F$, existen únicos

$$r \in \mathbb{N}, \qquad x_{i_1}, \ldots, x_{i_r} \in X, \qquad \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$$

tales que

- $x_{i_{j+1}}^{\varepsilon_{j+1}} \neq x_{i_j}^{-\varepsilon_j}$ y
- $x_{i_1}^{\varepsilon_1} \ldots x_{i_r}^{\varepsilon_r}$ representa g.

Forma normal, forma reducida.

Formas normales

Conjugación

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1}$$

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}$$

Formas normales

Conjugación

$$
\begin{array}{c}
w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida} \\
\Downarrow \\
\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}
\end{array}
$$

Iteración produce finalmente una palabra *cíclicamente reducida* $\overline{w}$.

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}$$

Iteración produce finalmente una palabra *cíclicamente reducida* $\overline{w}$.

Dado w_1, w_2:

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}$$

Iteración produce finalmente una palabra *cíclicamente reducida* $\overline{w}$.

Dado w_1, w_2:

- Calcular $\overline{w_1}$ y $\mathcal{E}(w_1)$ conjunto de sus permutaciones cíclicas.

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}$$

Iteración produce finalmente una palabra *cíclicamente reducida* $\overline{w}$.

Dado w_1, w_2:

- Calcular $\overline{w_1}$ y $\mathcal{E}(w_1)$ conjunto de sus permutaciones cíclicas.
- w_2 conjugado a w_1 ssi $\overline{w_2} \in \mathcal{E}(w_1)$.

Formas normales

Conjugación

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} \text{ reducida}$$

$$\Downarrow$$

$$\mathfrak{c}(w) = x_{i_2}^{\varepsilon_2} \dots x_{i_r}^{\varepsilon_r} x_{i_1}^{\varepsilon_1} \Longrightarrow \text{ reducir}$$

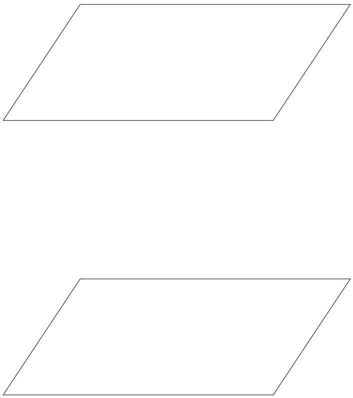
Iteración produce finalmente una palabra *cíclicamente reducida* $\overline{w}$.

Dado w_1, w_2:

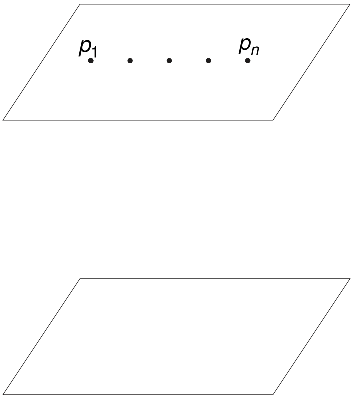
- Calcular $\overline{w_1}$ y $\mathcal{E}(w_1)$ conjunto de sus permutaciones cíclicas.
- w_2 conjugado a w_1 ssi $\overline{w_2} \in \mathcal{E}(w_1)$.

Nota: $\mathcal{E}(w_1), \mathcal{E}(w_2)$ son iguales o disjuntos.

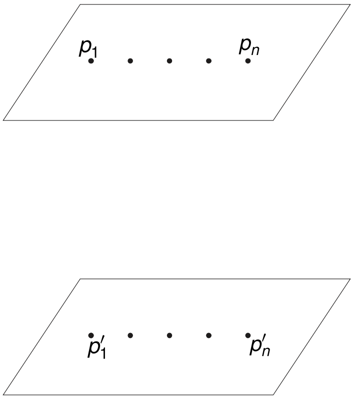
Trenzas geométricas



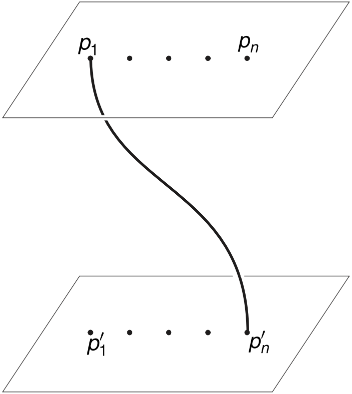
Trenzas geométricas



Trenzas geométricas



Trenzas geométricas

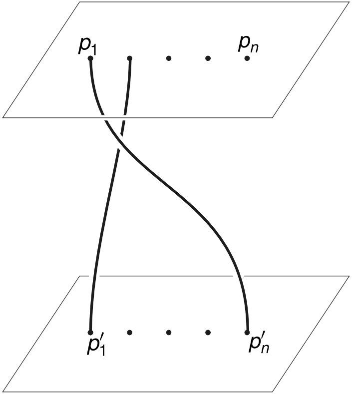


Definición (trenza geométrica)

n caminos continuos $f_i : [0,1] \longrightarrow \mathbb{R}^3$ (las **cuerdas***)*

- *no se cruzan en $\mathbb{R}^3$,*
- *monótonos.*

Trenzas geométricas

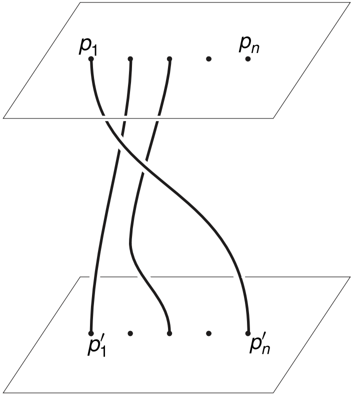


Definición (trenza geométrica)

n caminos continuos $f_i : [0,1] \longrightarrow \mathbb{R}^3$ (las **cuerdas***)*

- *no se cruzan en $\mathbb{R}^3$,*
- *monótonos.*

Trenzas geométricas

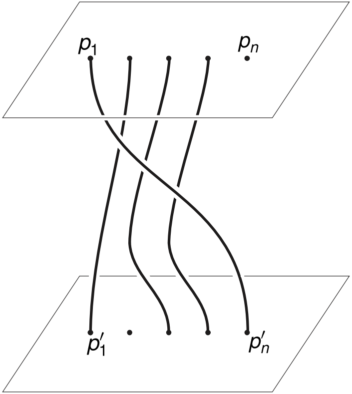


Definición (trenza geométrica)

*n caminos continuos $f_i : [0,1] \longrightarrow \mathbb{R}^3$ (las **cuerdas**)*

- *no se cruzan en $\mathbb{R}^3$,*
- *monótonos.*

Trenzas geométricas

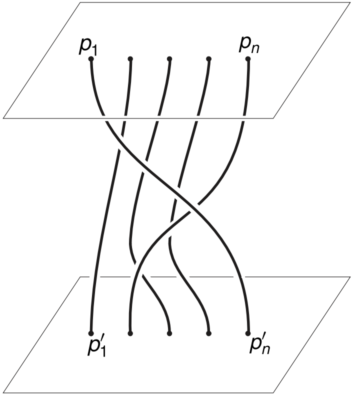


Definición (trenza geométrica)

n caminos continuos $f_i : [0,1] \longrightarrow \mathbb{R}^3$ (las **cuerdas***)*

- *no se cruzan en $\mathbb{R}^3$,*
- *monótonos.*

Trenzas geométricas



Definición (trenza geométrica)

n caminos continuos $f_i : [0,1] \longrightarrow \mathbb{R}^3$ (las **cuerdas***)*

- *no se cruzan en $\mathbb{R}^3$,*
- *monótonos.*

Grupo de trenzas

Definición (Grupo de trenzas con n cuerdas $\mathcal{B}_n$)

Clases de isotopía de trenzas geométricas, con concatenación.

Grupo de trenzas

Definición (Grupo de trenzas con n cuerdas $\mathcal{B}_n$)

Clases de isotopía de trenzas geométricas, con concatenación.

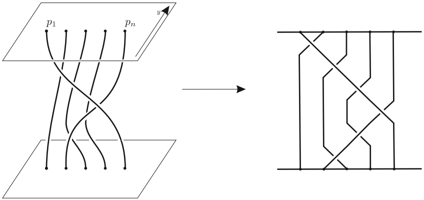
Representación 2D más cómoda:

Grupo de trenzas

Definición (Grupo de trenzas con *n* cuerdas $\mathcal{B}_n$)

Clases de isotopía de trenzas geométricas, con concatenación.

Representación 2D más cómoda:

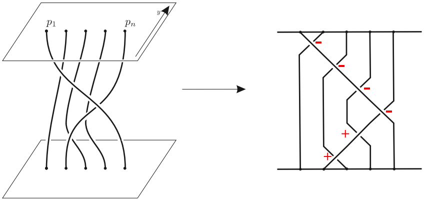


Grupo de trenzas

Definición (Grupo de trenzas con n cuerdas $\mathcal{B}_n$)

Clases de isotopía de trenzas geométricas, con concatenación.

Representación 2D más cómoda:

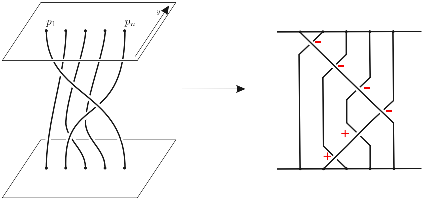


Grupo de trenzas

Definición (Grupo de trenzas con n cuerdas $\mathcal{B}_n$)

Clases de isotopía de trenzas geométricas, con concatenación.

Representación 2D más cómoda:



Modulo isotopía, los puntos múltiples de la proyección son dobles e indicamos cruce positivo o negativo.

Presentación

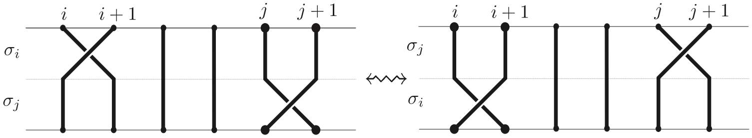
Teorema (Artin, 1947)

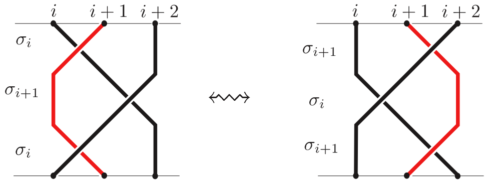
$$\mathcal{B}_n = \left\langle \sigma_1, \sigma_2 \dots, \sigma_{n-1} \;\middle|\; \begin{array}{cc} \sigma_i\sigma_j = \sigma_j\sigma_i & |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & |i-j| = 1 \end{array} \right\rangle.$$

Presentación

Teorema (Artin, 1947)

$$\mathcal{B}_n = \left\langle \sigma_1, \sigma_2 \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{cc} \sigma_i\sigma_j = \sigma_j\sigma_i & |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & |i-j| = 1 \end{array} \right\rangle.$$





Grupos de Artin-Tits

Definición (Grupo de Artin-Tits)

Generado por un número finito de generadores sujetos a relaciones equilibradas de la forma $ab\ldots = ba\ldots$.

Grupos de Artin-Tits

Definición (Grupo de Artin-Tits)

Generado por un número finito de generadores sujetos a relaciones equilibradas de la forma $ab\ldots = ba\ldots$.

Generadores de orden 2 $\Longrightarrow$ *grupo de Coxeter* asociado.

Grupos de Artin-Tits

Definición (Grupo de Artin-Tits)

Generado por un número finito de generadores sujetos a relaciones equilibradas de la forma $ab\ldots = ba\ldots$.

Generadores de orden 2 $\Longrightarrow$ *grupo de Coxeter* asociado.
En el caso de $\mathcal{B}_n$, obtenemos el grupo simétrico:

$$\mathfrak{S}_n = \left\langle \tau_1, \tau_2 \ldots, \tau_{n-1} \;\middle|\; \begin{array}{cc} \tau_i\sigma_j = \tau_j\sigma_i & |i-j| \geqslant 2 \\ \tau_i\tau_j\tau_i = \tau_j\tau_i\tau_j & |i-j| = 1 \\ \tau_i^2 = 1 & \forall i = 1, \ldots, n-1 \end{array} \right\rangle.$$

Permutaciones

La proyección

$$\begin{array}{ccc} \mathcal{B}_n & \xrightarrow{\pi} & \mathfrak{S}_n \\ \sigma_i & \longmapsto & \tau_i = [i, i+1] \end{array}$$

lleva una trenza a la permutación que induce sobre las extremidades de las cuerdas.

Grupos de A.-T. de tipo finito...

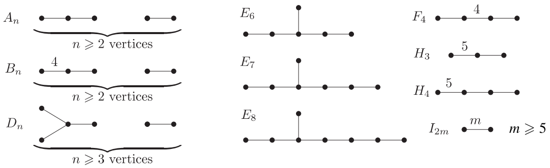
...Si el grupo de Coxeter asociado es finito.

Grupos de A.-T. de tipo finito...

...Si el grupo de Coxeter asociado es finito.

Teorema (Coxeter, 1935)

Grupos de Coxeter irreducibles finitos.

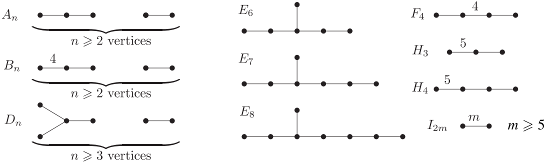


Grupos de A.-T. de tipo finito...

...Si el grupo de Coxeter asociado es finito.

Teorema (Coxeter, 1935)

Grupos de Coxeter irreducibles finitos.



Ejemplos:

- grupos dihedrales I_{2m},
- grupo simétrico A_n,
- grupo del cubo B_3,
- grupo del dodecaedro H_3.

Frank Garside, 1969

- Nueva solución al problema de la palabra en $\mathcal{B}_n$

Frank Garside, 1969

- Nueva solución al problema de la palabra en $\mathcal{B}_n$
- Primera solución al problema de la conjugación en $\mathcal{B}_n$

Frank Garside, 1969

- Nueva solución al problema de la palabra en $\mathcal{B}_n$
- Primera solución al problema de la conjugación en $\mathcal{B}_n$
- Todo adaptable a grupos de Artin-Tits de tipo finito (Deligne, Brieskorn-Saito (1972))

Frank Garside, 1969

- Nueva solución al problema de la palabra en $\mathcal{B}_n$
- Primera solución al problema de la conjugación en $\mathcal{B}_n$
- Todo adaptable a grupos de Artin-Tits de tipo finito (Deligne, Brieskorn-Saito (1972))
- Definición de los “grupos de Garside” (Dehornoy-Paris 1999)

Frank Garside, 1969

- Nueva solución al problema de la palabra en $\mathcal{B}_n$
- Primera solución al problema de la conjugación en $\mathcal{B}_n$
- Todo adaptable a grupos de Artin-Tits de tipo finito (Deligne, Brieskorn-Saito (1972))
- Definición de los "grupos de Garside" (Dehornoy-Paris 1999)
- Múltiples mejoras subsecuentes de los algorítmos

Joan Birman	Ki-Hyoung Ko
M. C.	Eong-Kyung Lee
Elsayed ElRifai	Sang-Jin Lee
Nuno Franco	Hugh Morton
Volker Gebhardt	William Thurston
Juan González-Meneses	Bert Wiest

Trenzas simples

Definición

$\mathcal{S}_n$: trenzas **simples**. *Positivas y cada par de cuerdas se cruza a lo más una vez.*

Trenzas simples

Definición

$\mathcal{S}_n$: *trenzas* **simples**. *Positivas y cada par de cuerdas se cruza a lo más una vez.*

- $\mathcal{S}_n \xrightarrow{\pi \text{ biy.}} \mathfrak{S}_n$

Trenzas simples

Definición

$\mathcal{S}_n$: *trenzas* **simples**. *Positivas y cada par de cuerdas se cruza a lo más una vez.*

- $\mathcal{S}_n \xrightarrow{\pi \text{ biy.}} \mathfrak{S}_n$
- Para $x \in \mathcal{S}_n$,
  cuerdas i, j se cruzan $\Longleftrightarrow$ (i, j) inversión en $\pi(x)$.

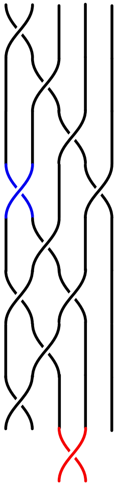
Trenzas simples

Definición

$\mathcal{S}_n$: *trenzas* **simples**. *Positivas y cada par de cuerdas se cruza a lo más una vez.*

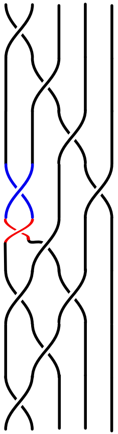
- $\mathcal{S}_n \xrightarrow{\pi \text{ biy.}} \mathfrak{S}_n$
- Para $x \in \mathcal{S}_n$,
  cuerdas i, j se cruzan $\Longleftrightarrow$ (i, j) inversión en $\pi(x)$.
- $\Delta = \pi^{-1}\begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$ es "maximal" en $\mathcal{S}_n$.

Propiedades de Delta



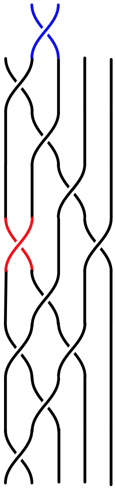
$\Delta\sigma_i$

Propiedades de Delta



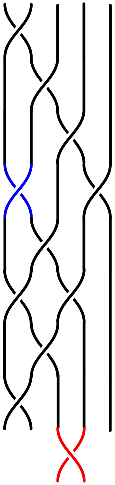
$\Delta\sigma_i$

Propiedades de Delta



$$\Delta\sigma_i = \sigma_{n-i}\Delta$$

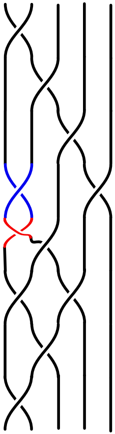
Propiedades de Delta



$$\Delta{\color{red}\sigma_i}={\color{blue}\sigma_{n-i}}\Delta$$

$$\Delta\sigma_i^{-1}$$

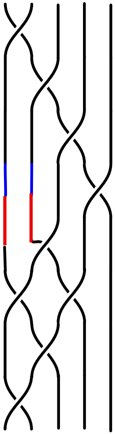
Propiedades de Delta



$\Delta \sigma_i = \sigma_{n-i} \Delta$

$\Delta \sigma_i^{-1}$

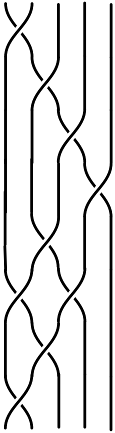
Propiedades de Delta



$$\Delta\sigma_i = \sigma_{n-i}\Delta$$

$$\Delta\sigma_i^{-1}$$

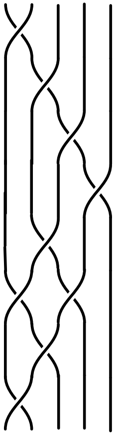
Propiedades de Delta



$$\Delta\sigma_i = \sigma_{n-i}\Delta$$

$\Delta\sigma_i^{-1}$ positivo

Propiedades de Delta



$$\Delta\sigma_i = \sigma_{n-i}\Delta$$

$\Delta\sigma_i^{-1}$ positivo

w palabra en los σ_i
$\Longrightarrow \Delta^j w'$, $j \in \mathbb{Z}$, w' positivo.

Cómo definir formas normales

Cambio de generadores: $\mathcal{S}_n$ en vez de $\{\sigma_i\}$

$$w \rightsquigarrow \Delta^{-j} w' \rightsquigarrow \Delta^{-j} s_1 \dots s_r.$$

¿Palabra reducida?

Retículo

$(\mathfrak{S}_n, \preccurlyeq)$ orden débil a la izquierda; retículo.

Un par de "letras" s_1, s_2 es *reducido* si $s_1^{-1}\Delta \wedge s_2 = 1$.

Retículo

$(\mathfrak{S}_n, \preccurlyeq)$ orden débil a la izquierda; retículo.
Usando $\pi : \mathcal{S}_n \xrightarrow{\text{bij.}} \mathfrak{S}_n$

$$(\mathcal{S}_n, \preccurlyeq) \text{ es retículo.}$$

Un par de "letras" s_1, s_2 es *reducido* si $s_1^{-1}\Delta \wedge s_2 = 1$.

Retículo

$(\mathfrak{S}_n, \preccurlyeq)$ orden débil a la izquierda; retículo.
Usando $\pi : \mathcal{S}_n \xrightarrow{\text{bij.}} \mathfrak{S}_n$

$$(\mathcal{S}_n, \preccurlyeq) \text{ es retículo.}$$

Todo funciona igual en grupos de A.-T. de tipo finito.

Un par de "letras" s_1, s_2 es *reducido* si $s_1^{-1}\Delta \wedge s_2 = 1$.

Retículo

$(\mathfrak{S}_n, \preccurlyeq)$ orden débil a la izquierda; retículo.
Usando $\pi : \mathcal{S}_n \xrightarrow{\text{bij.}} \mathfrak{S}_n$

$$(\mathcal{S}_n, \preccurlyeq) \text{ es retículo.}$$

Todo funciona igual en grupos de A.-T. de tipo finito.

Definición aproximativa: *grupo de Garside* = generado por un retículo finito.

Un par de "letras" s_1, s_2 es *reducido* si $s_1^{-1}\Delta \wedge s_2 = 1$.

Reducción en trenzas

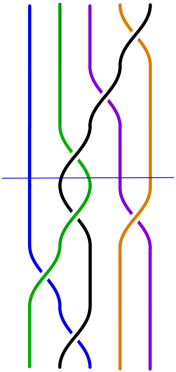
Definición

El par s_1, s_2 es reducido si s_1 es máximo $\Longleftrightarrow$ no se pueden deslizar cruces iniciales de s_2 a s_1.

Reducción en trenzas

Definición

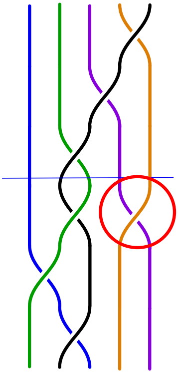
El par s_1, s_2 es reducido si s_1 es máximo $\iff$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

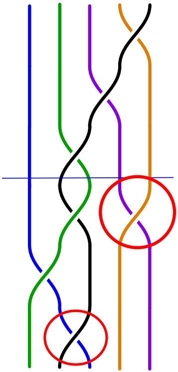
El par s_1, s_2 es reducido si s_1 es máximo $\iff$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

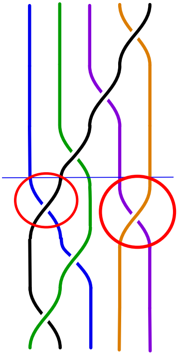
El par s_1, s_2 es reducido si s_1 es máximo $\Longleftrightarrow$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

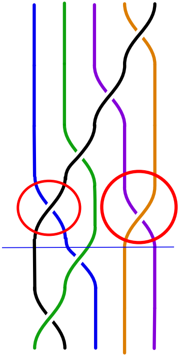
El par s_1, s_2 es reducido si s_1 es máximo $\Longleftrightarrow$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

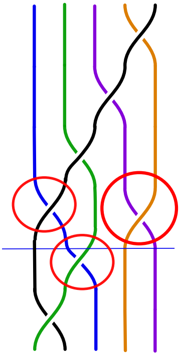
El par s_1, s_2 es reducido si s_1 es máximo $\iff$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

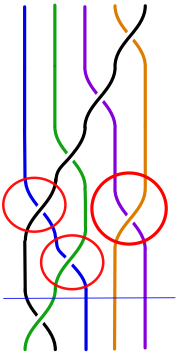
El par s_1, s_2 es reducido si s_1 es máximo $\Longleftrightarrow$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

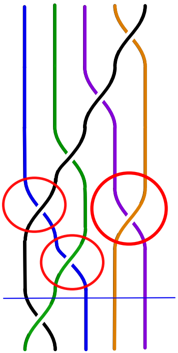
El par s_1, s_2 es reducido si s_1 es máximo $\Longleftrightarrow$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Reducción en trenzas

Definición

El par s_1, s_2 es reducido si s_1 es máximo $\iff$ no se pueden deslizar cruces iniciales de s_2 a s_1.



Formas normales

Teorema

Para todo $x \in B_n$, existe único $p \in \mathbb{Z}$, $r \in \mathbb{N}$, $x_1, \ldots, x_r \in \mathcal{S}_n - \{1, \Delta\}$, tales que

- (x_i, x_{i+1}) *es reducido.*
- $\Delta^p x_1 \ldots x_r$ *representa* x.

Formas normales

Teorema

Para todo $x \in B_n$, existe único $p \in \mathbb{Z}$, $r \in \mathbb{N}$, $x_1, \ldots, x_r \in \mathcal{S}_n - \{1, \Delta\}$, tales que

- (x_i, x_{i+1}) *es reducido.*
- $\Delta^p x_1 \ldots x_r$ *representa* x.

Hay distintas formas de medir la longitud de una forma normal (de una trenza); notación L.

Conjugación

$$w = x_1 \dots x_r \rightsquigarrow \mathfrak{c}(w) = x_2 \dots x_r x_1.$$

Ojo: “Reducción” no solo afecta x_r, x_1.

Conjugación

$$w = x_1 \dots x_r \rightsquigarrow \mathfrak{c}(w) = x_2 \dots x_r x_1.$$

Ojo: "Reducción" no solo afecta x_r, x_1.

Propiedad.

$$L(\mathfrak{c}(w)) \leqslant L(w)$$

alcanza largo minimal en la clase de conjugación

Conjugación

$$w = x_1 \dots x_r \rightsquigarrow \mathfrak{c}(w) = x_2 \dots x_r x_1.$$

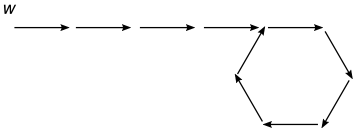
Ojo: “Reducción” no solo afecta x_r, x_1.

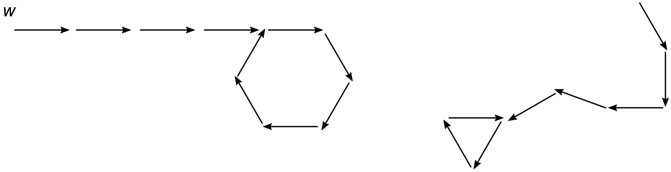
Propiedad.

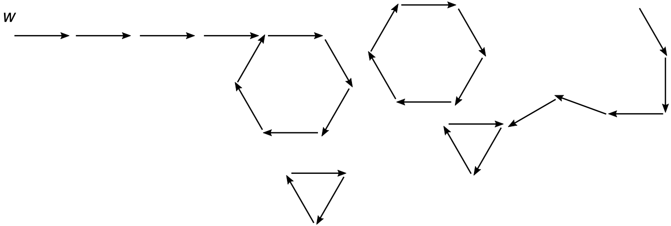
$$L(\mathfrak{c}(w)) \leqslant L(w)$$

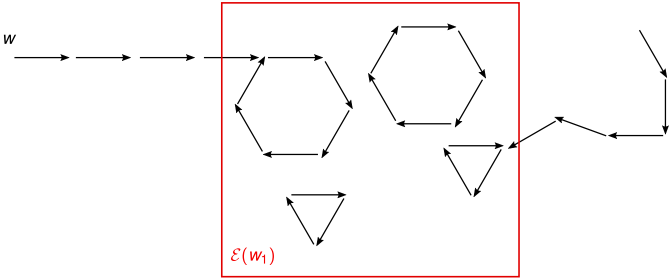
alcanza largo minimal en la clase de conjugación

$\mathfrak{c}$ es periódico a partir de cierto rango

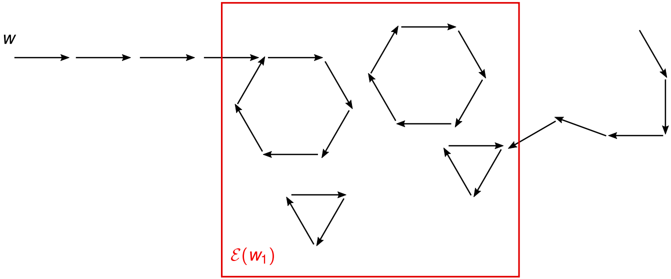

w


w


w

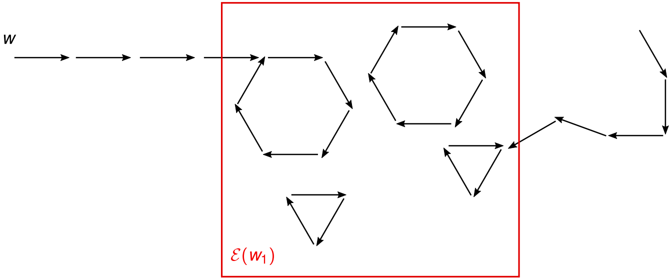


$\mathcal{E}(w_1)$={conjugados de w_1 que pertenecen a un circuito}.



$\mathcal{E}(w_1)$={conjugados de w_1 que pertenecen a un circuito}.

Computable a partir de uno de sus elementos [Franco, González-Meneses]



$\mathcal{E}(w_1)$={conjugados de w_1 que pertenecen a un circuito}.

Computable a partir de uno de sus elementos [Franco, González-Meneses]

$$w_2 \text{ conjugado a } w_1 \iff \mathcal{E}(w_1) \text{ contiene un circuito de } w_2$$
$$\iff \mathcal{E}(w_1) = \mathcal{E}(w_2).$$

En la práctica

- Aplicación a la criptografía : calcular un conjugado es fácil, reconocer trenzas conjugadas es difícil.
- Complejidad teórica de la solución es **exponencial** respecto a L.

Dos elementos clave para probar una mejor complejidad (polinomial):

- Número de iteraciones de $\mathfrak{c}$ hasta la primera repetición.
- Cardinal de $\mathcal{E}(w)$

Otra definición de las trenzas

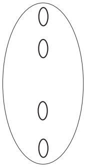
$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

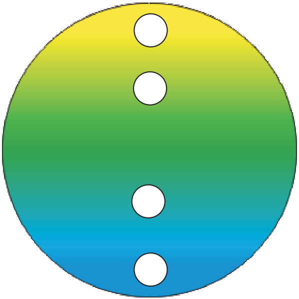
Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

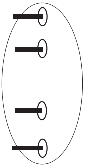


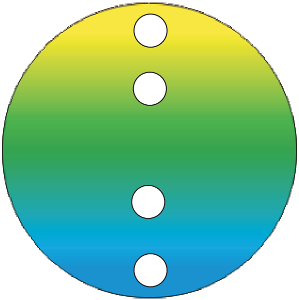


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

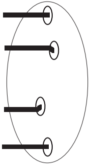


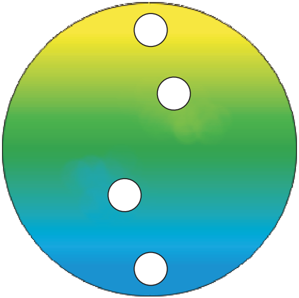


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

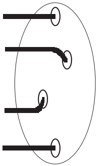


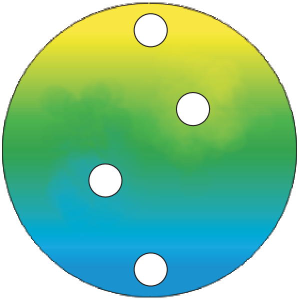


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

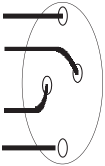


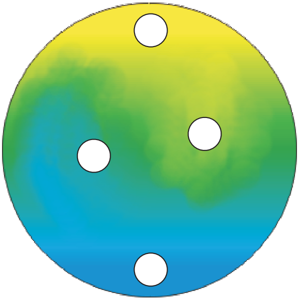


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

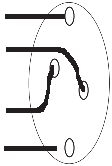


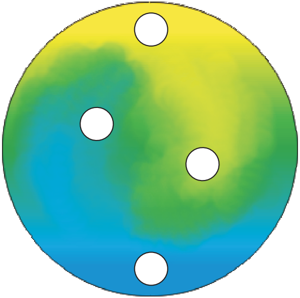


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

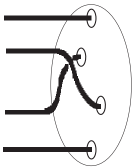


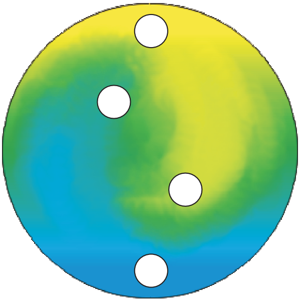


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.

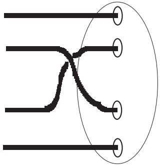


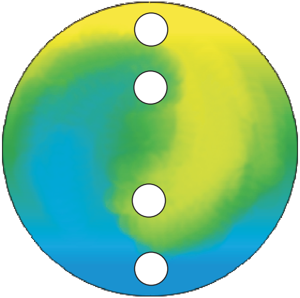


Otra definición de las trenzas

$$\mathcal{B}_n \cong \mathcal{MCG}(\mathbb{D}_n).$$

Homeomorfismos de un disco pinchado con n agujeros modulo isotopia.





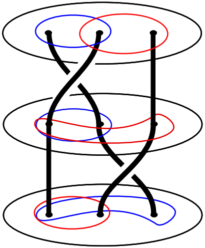
Alternativa al iterar la acción de trenzas en $\mathbb{D}_n$:

- preservan un conjunto de curvas cerradas –*curvas de reducción*.
- enredan cualquier curva cerrada.

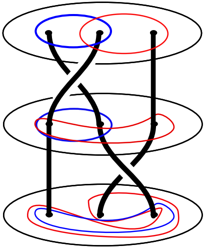
Alternativa al iterar la acción de trenzas en $\mathbb{D}_n$:

- preservan un conjunto de curvas cerradas –*curvas de reducción*.
- enredan cualquier curva cerrada.

$\sigma_1\sigma_2$



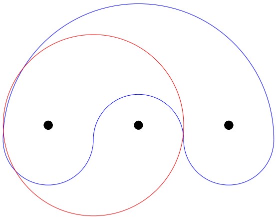
$\sigma_1\sigma_2^{-1}$



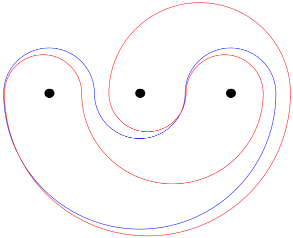
Alternativa al iterar la acción de trenzas en $\mathbb{D}_n$:

- preservan un conjunto de curvas cerradas –*curvas de reducción*.
- enredan cualquier curva cerrada.

$\sigma_1\sigma_2$

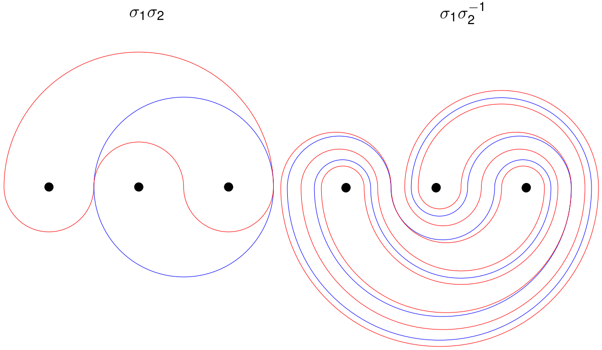


$\sigma_1\sigma_2^{-1}$



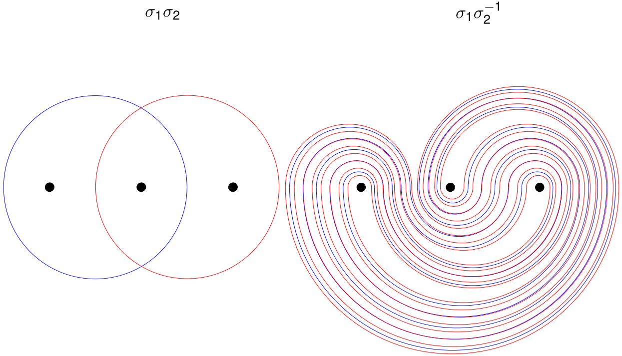
Alternativa al iterar la acción de trenzas en $\mathbb{D}_n$:

- preservan un conjunto de curvas cerradas –*curvas de reducción*.
- enredan cualquier curva cerrada.



Alternativa al iterar la acción de trenzas en $\mathbb{D}_n$:

- preservan un conjunto de curvas cerradas –*curvas de reducción*.
- enredan cualquier curva cerrada.



Dos trenzas conjugadas son del mismo tipo.
Idea: Estudiar el problema de conjugación independientemente en cada tipo.
Problema auxiliar: reconocer el tipo.

Definición (Curva *redonda*)

= círculo (ningún enredo).

Es fácil reconocer si una trenza tiene una curva de reducción redonda.

Definición (Curva *redonda*)

= *círculo (ningún enredo).*

Es fácil reconocer si una trenza tiene una curva de reducción redonda.

Para decidir reducibilidad de x, calcular conjugado x' de x tal que x' es reducible ssi preserva una curva redonda.

Definición (Curva *redonda*)

= círculo (ningún enredo).

Es fácil reconocer si una trenza tiene una curva de reducción redonda.

Para decidir reducibilidad de x, calcular conjugado x' de x tal que x' es reducible ssi preserva una curva redonda.

Teorema (Benardete-Guttierez-Nitecki 1995, C. 2012)

Si x preserva una curva redonda, entonces $\mathfrak{c}(x)$ también.

Grafo de curvas

El *grafo de curvas* de $\mathbb{D}_n$ es un grafo (localmente infinito) que recoge información sobre las curvas en $\mathbb{D}_n$.

Teorema (Masur-Minsky 1999)

Es Gromov-hiperbólico.

Teorema (Masur/Minsky 2000, Tao 2013)

Existe una constante K tal que si x, y son conjugados, pueden serlo mediante un conjugador de largo a lo más $K(L(x) + L(y))$.

Teorema (C. Wiest 2012, C. 2014)

Existe un algoritmo polinomial que resuelve el problema auxiliar.

Teorema (C. Wiest 2012, C. 2014)

Existe un algoritmo polinomial que resuelve el problema auxiliar.

Teorema (C.-Wiest 2014)

Solución polinomial al problema de conjugación en $\mathcal{B}_4$.

En curso

Trabajo conjunto con Wiest (2016, 2017). Desarrollar análogos de curvas y grafo de curvas para otros grupos de Artin-Tits.