Grupo de trenzas y su aplicación en criptografía

Fernando de la Hoz Moreno

Doble Grado en Ingeniería Informática y Matemáticas

Universidad de Granada

Índice

- Trenzas y grupo de trenzas:
  - Construcción topológica.
  - Definición algebraica.
- Plataforma criptográfica:
  - Características del grupo plataforma.
  - Problema de búsqueda del conjugado.
  - Monoide de Garside exhaustivo.
- Métodos criptográficos:
  - Esquema Anshel-Anshel-Goldfeld.
  - Esquema Diffie-Helman.
- Criptoanálisis:
  - Heurística.
- Conclusión y trabajos futuros.

Emil Artin

- Matemático austriaco (1898-1962).
- Universidad de Gotinga y Universidad de Princeton.
- Teoría de números, teoría algebraica de anillos asociativos y números hipercomplejos.
- Acuñó los términos *trenza* y *grupo de trenzas* por primera vez en el año 1925.

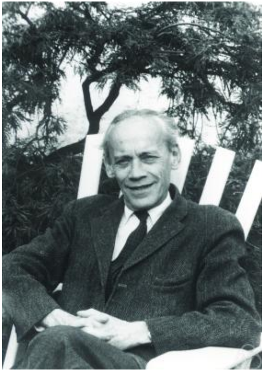


Figura: Fotografía de Emil Artin.

Trenza Geométrica

Una **trenza geométrica** de n hebras, con $n \geq 1$, es un subconjunto $\mathcal{B} \subset \mathbb{R}^2 \times I$ ($I = [0,1]$), formado por n intervalos topológicos (subconjuntos de $\mathbb{R}^2 \times I$ homeomorfos al intervalo $[0,1]$) disjuntos llamados hebras de tal manera que la proyección $\mathbb{R}^2 \times I \to I$ establezca un homeomorfismo de cada hebra en I y

$$\mathcal{B} \cap (\mathbb{R}^2 \times \{0\}) = \{(1,0,0), (2,0,0), ..., (n,0,0)\},$$

$$\mathcal{B} \cap (\mathbb{R}^2 \times \{1\}) = \{(1,0,1), (2,0,1), ..., (n,0,1)\}.$$

Cada hebra de $\mathcal{B}$ interseca con el plano $\mathbb{R}^2 \times \{t\}$ con $t \in I$ en un único punto y conecta un punto $(i,0,0)$ con un punto $(s(i),0,1)$ donde $i, s(i) \in \{1,2,...,n\}$. La sucesión $(s(1), s(2), ..., s(n))$ es una permutación del conjunto $\{1,2,...,n\}$ llamada permutación subyacente de $\mathcal{B}$.

Trenza Geométrica

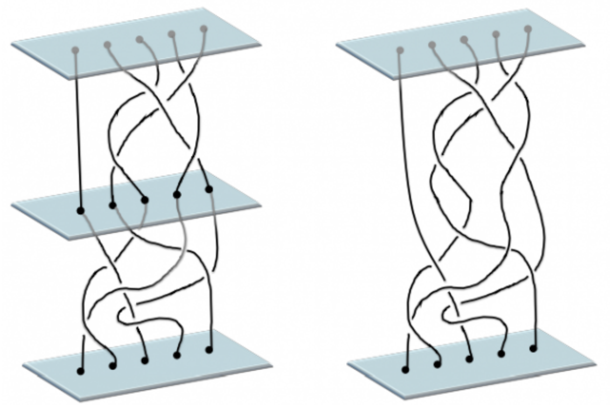


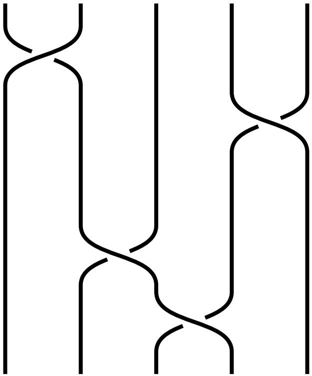
Figura: Trenza Geométrica.

Isotopía

Dos trenzas geométricas $\mathcal{B}$ y $\mathcal{B}'$ son **isotópicas** si podemos deformar de manera continua $\mathcal{B}$ en $\mathcal{B}'$.

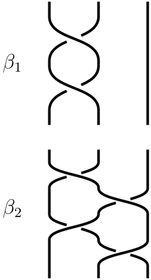
La relación de isotopía establece una relación de equivalencia y al conjunto de clases de equivalencia se les denomina **trenzas de n hebras**, denotándolo por $\mathcal{B}_n$.

Diagrama de trenzas

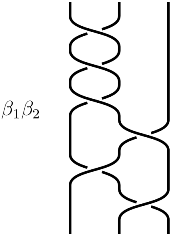


Producto de trenzas

Sean $\beta_1, \beta_2 \in \mathcal{B}_3$, cuyos diagramas se pueden ver en (a), el resultado del producto $\beta_1\beta_2$ se representa en (b).

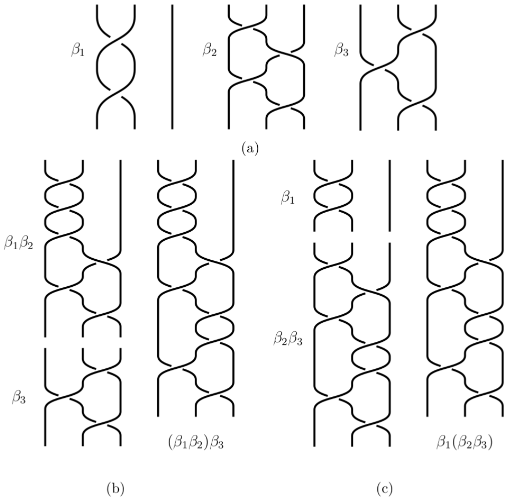


(a)

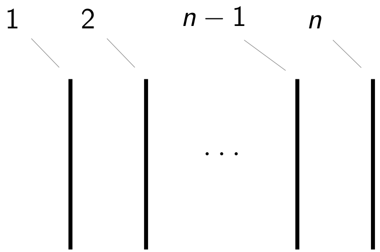


(b)

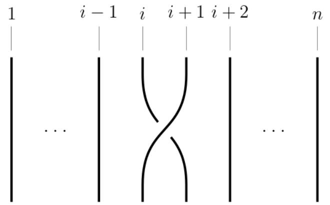
Asociatividad



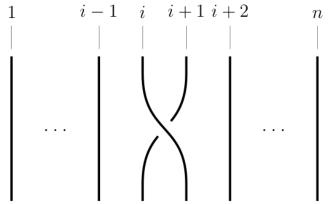
Elemento neutro



Trenzas elementales



σ_i^+



σ_i^-

Inverso

Lema

El conjunto de trenzas elementales genera $\mathcal{B}_n$ como monoide.

Corolario

Sea $\beta \in \mathcal{B}_n$, existe un elemento $\beta^{-1} \in \mathcal{B}_n$ que es el inverso por ambos lados de β.

Ejemplo

Sea $\beta \in \mathcal{B}_6$.

$$\beta = \sigma_3^+ \sigma_1^- \sigma_5^+ \sigma_2^+ \qquad \beta^{-1} = \sigma_2^- \sigma_5^- \sigma_1^+ \sigma_3^-$$

Grupo de trenzas de Artin

El **grupo de trenzas de Artin** B_n es el grupo generado por $n-1$ elementos $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ y las relaciones de trenza

$$\sigma_i \sigma_j = \sigma_j \sigma_i,$$

para todo $i, j \in \{1, 2, ..., n-1\}$ con $|i-j| \geq 2$ y

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1},$$

para todo $i \in \{1, 2, ..., n-2\}$.

Grupo de trenzas de Artin

Teorema

Para $\varepsilon \in \{+, -\}$, existe un único homomorfismo $\varphi_\varepsilon : B_n \to \mathcal{B}_n$ tal que $\varphi_\varepsilon(\sigma_i) = \sigma_i^\varepsilon$ para cada $i \in \{1, 2, ..., n-1\}$. El homomorfismo φ_ε es un **isomorfismo**.

Plataformas criptográficas

Una **plataforma criptográfica** es un método criptográfico basado en un objeto matemático. Si este objeto es un grupo, se le denomina **grupo plataforma**. La seguridad de la plataforma depende de la dificultad, computacional o teórica, de resolver un problema de teoría de grupos en el grupo plataforma.

Plataformas criptográficas

Entre las propiedades que necesita un grupo de plataforma se encuentran:

- Una **representación finita**.
- Una **forma normal** FN para representar de forma única a los elementos del grupo.
- FN debe tener **buena difusión**, es decir, que dado $FN(\beta_1\beta_2)$ con $\beta_1, \beta_2 \in B_n$ sea difícil computacionalmente calcular $FN(\beta_1)$ y $FN(\beta_2)$.
- Un **problema** $\mathcal{P}$ de teoría de grupos que sea generalmente complejo.

Problema de búsqueda del conjugado

Definición

El **problema de búsqueda del conjugado** en el grupo B_n consiste en, dados $\alpha, \beta \in B_n$ con $\alpha = \gamma\beta\gamma^{-1}$ donde $\gamma \in B_n$, calcular el elemento γ llamado *trenza conjugadora*.

Monoide de Garside

Un **monoide de Garside exhaustivo** es un par (M, Δ), donde M es un monoide y Δ un elemento de M (**elemento de Garside**) que cumplen ciertas características. Consideramos G_M como el grupo de fracciones de M. Entre las propiedades que nos proporciona un monoide de Garside exhaustivo se encuentra la obtención de una forma normal en G_M.

Monoide de Garside

Para cualquier $n \geq 1$, denotamos por B_n^+ el monoide generado por $n-1$ generadores $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ y las relaciones

$$\sigma_i \sigma_j = \sigma_j \sigma_i \quad si \ |i-j| \geq 2,$$

$$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_i \quad si \ |i-j| = 1,$$

donde $i, j \in \{1, 2, \ldots, n-1\}$. El monoide B_n^+ se llama **monoide de trenzas** de n hebras. Consideramos el elemento de Garside

$$\Delta_n = (\sigma_1 \cdots \sigma_{n-2} \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1 \sigma_2) \sigma_1$$

Entonces (B_n^+, Δ_n) es un monoide de Garside exhaustivo y $G_{B_n^+} = B_n$.

Forma normal

Forma normal greedy

Para $n \geq 2$, cualquier $\beta \in B_n$ puede ser escrito únicamente en la forma $\beta = \Delta_n^s b$, donde $s \in \mathbb{Z}$ y $b \in B_n^+ \subset B_n$ no es un múltiplo por la derecha de Δ_n .

Ejemplo

Sea $\beta \in B_3$.

$$\beta = \sigma_1^{-1}\sigma_2 \qquad FN(\beta) = \Delta_3^{-1}\sigma_1\sigma_2\sigma_2$$

Anshel-Anshel-Goldfeld

Es un método de intercambio de llave público propuesto por Anshel & al en 1999. Las llaves públicas consisten en dos conjuntos de trenzas $\{p_1, ..., p_l\}, \{q_1, ..., q_m\} \subset B_n$. La llave privada es una palabra formada a partir de uno de estos conjuntos.

La seguridad está basada en la dificultad de resolver una variante del problema de búsqueda del conjugado en B_n, que es llamado el problema de búsqueda del conjugado múltiple, en el cual se intenta encontrar una trenza conjugadora de una familia finita de pares de trenzas $(p_1, p'_1), ..., (p_l, p'_l)$.

Anshel-Anshel-Goldfeld

1. Alicia calcula la trenza $s = u(p_1, ..., p_l)$ y lo usa para calcular los conjugados $q_1' = sq_1s^{-1}, ..., q_m' = sq_ms^{-1}$. Ella envía $q_1', ..., q_m'$.
2. Bruno calcula la trenza $r = v(q_1, ..., q_m)$ y lo usa para calcular los conjugados $p_1' = rp_1r^{-1}, ..., p_l' = rp_lr^{-1}$. Él envía $p_1', ..., p_l'$.
3. Alicia calcula $t_A = su(p_1', ..., p_l')^{-1}$.
4. Bruno calcula $t_B = v(q_1', ..., q_m')r^{-1}$.

La llave compartida es $t_A = t_B$.

Anshel-Anshel-Goldfeld

Muestras	n	l	Tiempo (s)	Desviación Estándar (s)	Mínimo (s)	Máximo (s)
3	5	5	6.28	0.67	5.77	7.05
3	5	10	14.77	14.62	2.81	31.07
3	10	5	192.54	199.27	42.88	418.74
1	10	10	658.55	0	658.55	658.55
2	15	5	416.68	465.42	87.58	745.79
1	15	10	423.07	0	423.07	423.07
3	20	5	235.87	165.23	81.02	409.83
1	20	10	1246.68	0	1246.68	1246.68
1	25	5	2350.10	0	2350.10	2350.10

n = número de hebras.

l = longitud de palabra.

Diffie-Helman

Este esquema de intercambio de llave Diffie-Hellman es propuesto por Ko, Lee & al. En él hace uso de subgrupos de B_n, donde los elementos de uno conmutan con los elementos de otro. En concreto se utilizan los subgrupos $LB_n = \langle \sigma_1, ..., \sigma_{m-1} \rangle$ y $UB_n = \langle \sigma_{m+1}, ..., \sigma_{n-1} \rangle$ con $m = [n/2]$. La llave pública es una trenza de B_n y las llaves privadas son trenzas de LB_n y UB_n.

La seguridad también está basada en la dificultad de resolver una variante del problema de búsqueda del conjugado donde dada una trenza p de B_n y las trenzas $p' = sps^{-1}$ y $p'' = rpr^{-1}$, con s y r pertenecientes a LB_n y UB_n respectivamente, hay que determinar o s o r.

Diffie-Helman

1. Alicia calcula el conjugado $p' = sps^{-1}$ con $s \in LB_n$, y se lo envia a Bruno.
2. Bruno calcula el conjugado $p'' = rpr^{-1}$ con $r \in UB_n$, y se lo envia a Alicia.
3. Alicia calcula $t_A = sp''s^{-1}$.
4. Bruno calcula $t_B = rp'r^{-1}$.

La llave compartida es $t_A = t_B$.

Diffie-Helman

Muestras	n	l	Tiempo (s)	Desviación Estándar (s)	Mínimo (s)	Máximo (s)
3	5	5	1.94	0.10	1.83	2.03
3	5	10	6.46	3.26	4.06	10.17
3	10	5	28.66	11.48	15.40	35.52
3	10	10	180.22	56.13	117.33	225.24
3	15	5	105.46	26.22	76.81	128.27
1	15	10	643.59	0	643.59	643.59
1	20	5	477.95	0	477.95	477.95
1	20	10	1318.74	0	1318.74	1318.74
1	25	5	665.31	0	665.31	665.31

n = número de hebras.

l = longitud de palabra.

Criptoanálisis

Ataques al problema de búsqueda del conjugado:

- Super conjuntos cumbre.
- Ataques basados en longitud.
- Ataques teóricos de representación.

Heurística

n	l	Muestras	Tasa de éxito
5	5	10	50.0 %
5	10	10	10.0 %
10	5	10	90.0 %
10	10	10	0.0 %
15	5	10	70.0 %
15	10	10	30.0 %
20	5	10	80.0 %
20	10	10	50.0 %
25	5	10	70.0 %

$n =$ número de hebras.

$l =$ longitud de palabra.

Conclusión y trabajos futuros

- **Generación de llaves**: utilizar trenzas con mejor difusión como llaves.
- **Cambiar el problema**: sustituir el problema de búsqueda del conjugado por otros, como pueden ser los problemas de raíz o problemas de longitud mínima.
- **Operaciones más exóticas**: cambiar en el problema la operación producto definida por el grupo por otras que añadan complejidad.

Referencias

Implementaciones:

- *https://github.com/ferhm/TFG/tree/main/src*

Bibliografía:

- PATRICK DEHORNOY, *Braid-based cryptography*.
- CHRISTIAN KASSEL, VLADIMIR TURAEV, *Braid groups*.
- DENNIS HOFHEINZ,RAINER STEINWANDT, *A Practical Attack on Some Braid Group Based Cryptographic Primitives*.
- STEVEV ROMAN, *Fundamentals of group theory. An advance aproach*.

Gracias por su atención.