Grupo de trenzas y su aplicación en criptografía

Fernando de la Hoz Moreno

Emil Artin

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

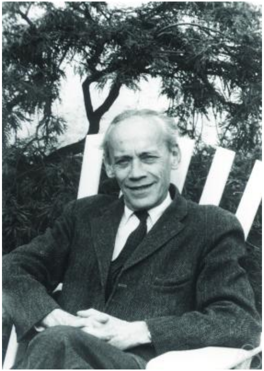


Figura: Fotografía de Emil Artin.

Trenza Geométrica

Una **trenza geométrica** de n hebras, con $n \geq 1$, es un subconjunto $\mathcal{B} \subset \mathbb{R}^2 \times I$ 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

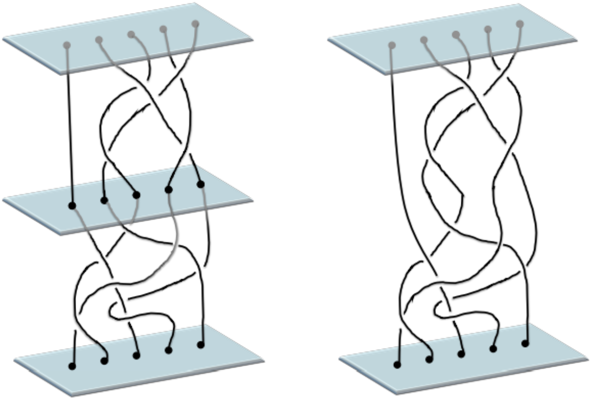


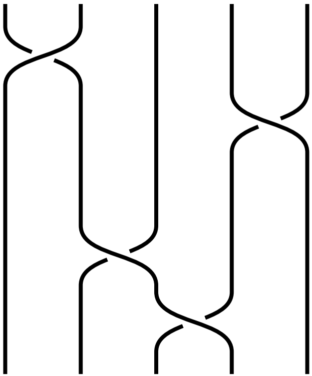
Figura: Trenza Geométrica.

Isotopía

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

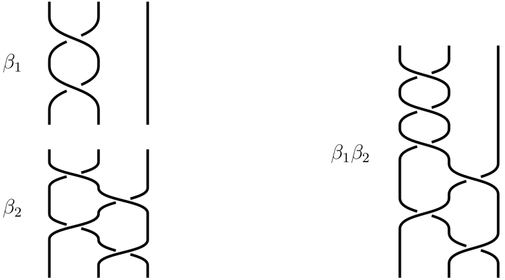
La relación de isotopía establece una relación de equivalencia y al conjunto de clases de equivalencia se les denomina **trenzas de n hebras**, denotándolo por $\mathcal{B}_n$.

Diagrama de trenzas



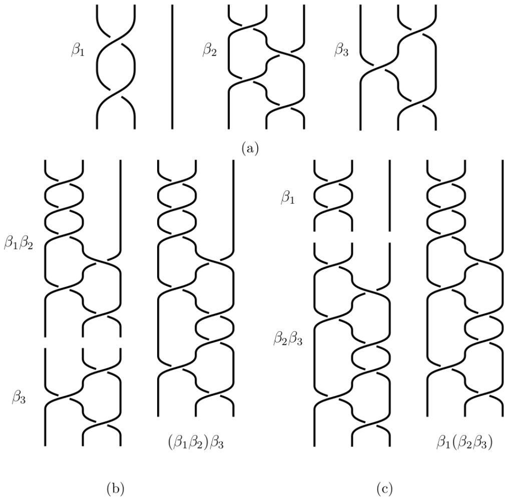
Producto de trenzas

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).

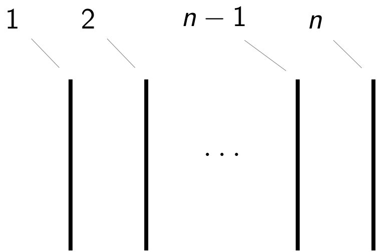


(a) (b)

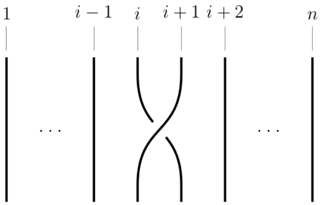
Asociatividad



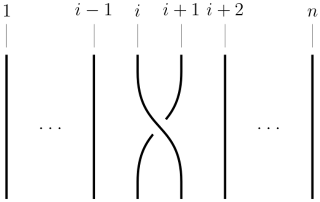
Elemento neutro



Trenzas elementales



σ_i^+



σ_i^-

Inverso

Lema

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

Colorario

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

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

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** para representar de forma única a los elementos del grupo.
- Un **problema** $\mathcal{P}$ de teoría de grupos que sea generalmente complejo.

Problema del conjugado

Definición

El **problema del conjugado** en el grupo B_n consiste en encontrar un procedimiento que nos permita, dados $\alpha, \beta \in B_n$, decidir si existe $\gamma \in B_n$ tal que $\alpha = \gamma\beta\gamma^{-1}$.

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. Algunas de las propiedades que nos proporciona un monoide de Garside exhaustivo son:

- Obtenemos una **forma normal** en G_M.
- Da una **solución** al problema del conjugado 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 $G_{B_n^+} = B_n$.

Anshel-Anshel-Goldfeld

Es un método de intercambio de llave público propuesto por Anshel & al en 1999. La llave pública consiste en dos conjuntos de trenzas $\{p_1, ..., p_l\}, \{q_1, ..., q_m\} \subset B_n$. La llave secreta es una palabra formada a partir 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

Muestras	n	l	Tiempo	Desviación Estándar	Mínimo	Máximo
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

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 encontrar la trenza $rp'r^{-1}$ o $sp''s^{-1}$.

Diffie-Helman

Muestras	n	l	Tiempo	Desviación Estándar	Mínimo	Máximo
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

Criptoanálisis

Ataques al problema de la 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 %

Bibliografía

- Emil Artin, *Theorie der zöpfe*, 1925.
- Emil Artin, *Theory of braids*, Vol. 48, No. 1, January, 1947.
- Patrick Dehornoy, *Braid-based cryptography*.
- Elsayed A. Elrifai,Hugh R. Morton, *Algorithms for positive braids*.
- Dennis Hofheinz,Rainer Steinwandt, *A Practical Attack on Some Braid Group Based Cryptographic Primitives*.
- Stevev Roman, *Fundamentals of group theory. An advance aproach*.
- *Algebra abstracta* https://es.wikibooks.org/wiki/Matemáticas_Universitarias/Álgebra_A

Bibliografía

- Pierre Antoine Brillet, *Abstract algebra*. 2007.
- B. Suri, *Free groups - basics*. 2010.
- John M. Howie, *Fundamentals of semigroup theory*.
- Christian Kassel, Vladimir Turaev, *Braid groups*.
- Kunio Murasugi, Bohdan l. Kurpita, *A study of braids*.
- Hans Delfs, Helmut Knebl, *Introduction to cryptography. Principles and Applications*.
- Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger, *A course in mathematical cryptography*.

Bibliografía

- I. Anshel, M. Anshel, D. Goldfeld, *New key agreement protocols in braid group cryptography*. 2001.
- K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Hang, J.S. Kang, C. Park, *New public-key cryptosystem using braid groups*. 2000.
- K.H. Ko, P. Dehornoy, M. Girault, J.W. Lee, *New signature scheme using conjugacy problem, Preprint*. 2002.
- H. Sibert, D.H. Choi, M.S. Cho, J.W. Lee, *Entity authentication schemes using braid word reduction*. 2003.
- *Imagen de Emil Artin*. De Konrad Jacobs, Erlangen - Mathematisches Forschungsinstitut Oberwolfach, https://commons.wikimedia.org/w/index.php?curid=3898471