Resultados de imposibilidad en álgebra y topología

Mariano Suárez-Alvarez

18 de mayo, 2007
1º de junio, 2007

El décimo problema de Hilbert

10. Determination of the solvability of a diophantine equation

Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

David Hilbert, 2º International Congress of Mathematicians, Paris, 1900.

Entscheidungsproblem

¿Existe un procedimiento efectivo que, dada una proposición matemática, decida si es verdadera o falsa?

David Hilbert, Wilhelm Ackermann, 'Grundzüge der theoretischen Logik.' Die Grundlehren der mathematischen Wissenschaften Bd. 27, Springer. Berlin, 1928.

Entscheidungsproblem

Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.* Monatsh. Math. Phys. 38 (1931), no. 1, 173–198.

Entscheidungsproblem

Alonzo Church, *An Unsolvable Problem of Elementary Number Theory.* Amer. J. Math. 58 (1936), no. 2, 345–363.

Alan Turing, *On computable numbers, with an application to the Entscheidungsproblem.* Proc. Lond. Math. Soc., II. Ser. 42, 230-265 (1936).

El décimo problema de Hilbert

Yuri Matijasevich, *On recursive unsolvability of Hilbert's tenth problem.* Proceedings of Fourth International Congress on Logic, Methodology and Philosophy of Science, Bucharest, 1971. Amsterdam: North-Holland (1973), 89–110

Entscheidungsproblem

Alonzo Church, *An Unsolvable Problem of Elementary Number Theory.* Amer. J. Math. 58 (1936), no. 2, 345–363.

Alan Turing, *On computable numbers, with an application to the Entscheidungsproblem.* Proc. Lond. Math. Soc., II. Ser. 42, 230-265 (1936).

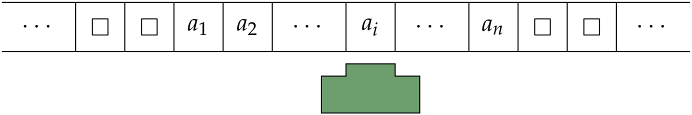
La tesis de Church-Turing

The expression "machine process" of course means one which could be carried out by the type of machine I was considering.

Alan Turing, 'On Computable Numbers, with an Application to the Entscheidungsproblem'. Proceedings of the London Mathematical Society, series 2, 42 (1936-37), 230-265.

Máquinas de Turing

Máquinas de Turing



Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \Box, \Sigma, \delta, q_0, F)$$

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \square, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \square, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \square, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;
- Un símbolo $\square \in \Gamma$, el *blanco*;

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \Box, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;
- Un símbolo $\Box \in \Gamma$, el *blanco*;
- $\Sigma \subset \Gamma \setminus \{\Box\}$, el conjunto de *símbolos de entrada*;

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \Box, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;
- Un símbolo $\Box \in \Gamma$, el *blanco*;
- $\Sigma \subset \Gamma \setminus \{\Box\}$, el conjunto de *símbolos de entrada*;
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$, la *función de transición*;

Máquinas de Turing

Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \square, \Sigma, \delta, q_0, F)$$

con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;
- Un símbolo $\square \in \Gamma$, el *blanco*;
- $\Sigma \subset \Gamma \setminus \{\square\}$, el conjunto de *símbolos de entrada*;
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$, la *función de transición*;
- $q_0 \in Q$, el *estado inicial*;

Máquinas de Turing

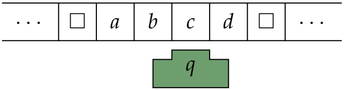
Una *máquina de Turing* es una 7-upla

$$M = (Q, \Gamma, \square, \Sigma, \delta, q_0, F)$$

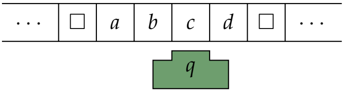
con

- Q un conjunto finito de *estados*;
- Γ un conjunto finito de *símbolos de cinta* tal que $\Gamma \cap Q = \varnothing$;
- Un símbolo $\square \in \Gamma$, el *blanco*;
- $\Sigma \subset \Gamma \setminus \{\square\}$, el conjunto de *símbolos de entrada*;
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$, la *función de transición*;
- $q_0 \in Q$, el *estado inicial*; y
- $F \subset Q$, el conjunto de *estados finales*.

Máquinas de Turing: estado instantáneo

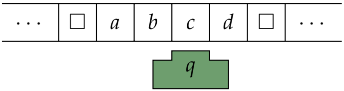


Máquinas de Turing: estado instantáneo



$\rightsquigarrow \quad abqcd$

Máquinas de Turing: estado instantáneo



$\rightsquigarrow \quad abqcd$

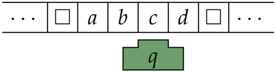
Un *estado instantáneo* es una palabra

$$\alpha_1 q \alpha_2 \in \Gamma^* Q \Gamma^*$$

que no empieza ni termina con el blanco $\square$.

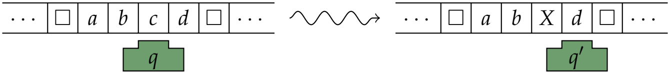
Máquinas de Turing: transiciones

Si $\delta(q, c) = (q', X, R)$, entonces:



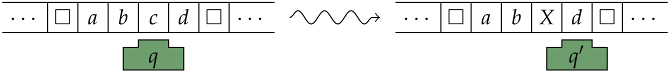
Máquinas de Turing: transiciones

Si $\delta(q, c) = (q', X, R)$, entonces:

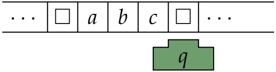


Máquinas de Turing: transiciones

Si $\delta(q, c) = (q', X, R)$, entonces:

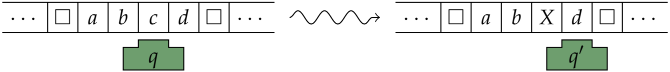


Si $\delta(q, \square) = (q', X, R)$, entonces:

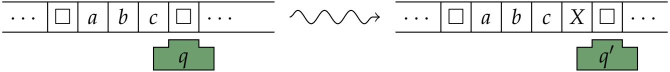


Máquinas de Turing: transiciones

Si $\delta(q, c) = (q', X, R)$, entonces:

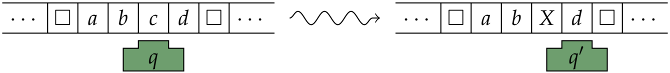


Si $\delta(q, \Box) = (q', X, R)$, entonces:

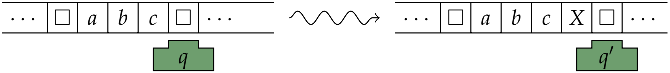


Máquinas de Turing: transiciones

Si $\delta(q, c) = (q', X, R)$, entonces:



Si $\delta(q, \Box) = (q', X, R)$, entonces:



&c…

Máquinas de Turing: transiciones

Definimos una relación $\vdash_M$ entre estados instantáneos:

Si $\delta(q, Y) = (q', Y', L)$,

$$\alpha_1 X q Y \alpha_2 \vdash_M \alpha_1 q' X Y' \alpha_2$$

$$q Y \alpha_2 \vdash_M q' \Box Y' \alpha_2$$

Si $\delta(q, \Box) = (q', Y', L)$,

$$\alpha_1 X q \vdash_M \alpha_1 q' X Y'$$

$$q \vdash_M q' Y'$$

Si $\delta(q, Y) = (q', Y', R)$,

$$\alpha_1 q Y \alpha_2 \vdash_M \alpha_1 Y' q' \alpha_2$$

Si $\delta(q, \Box) = (q', Y', R)$,

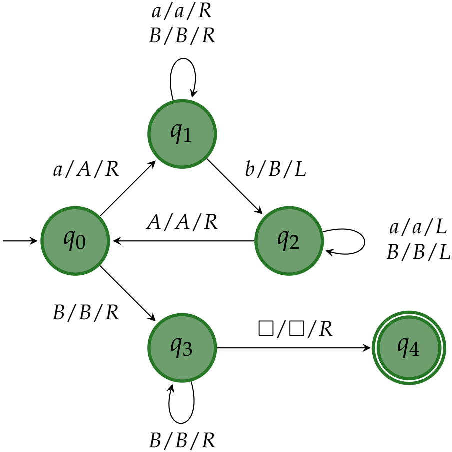
$$\alpha_1 q \vdash_M \alpha_1 Y' q'$$

Máquinas de Turing: aceptación

El *lenguaje aceptado* por una máquina de Turing M es

$$\mathscr{L}(M) = \{w \in \Sigma^* : \exists\, p \in F,\ \exists\, \alpha_1, \alpha_2 \in \Gamma^*,\ q_0 w \vdash_M^* \alpha_1 q \alpha_2\}.$$

Máquinas de Turing: aceptación



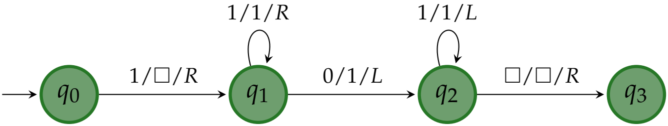
$$\Gamma = \{a, b, A, B\}$$
$$\Sigma = \{a, b\}$$
$$Q = \{q_0, \ldots, q_4\}$$
$$F = \{q_4\}$$
$$\mathscr{L}(M) = \{a^n b^n : n \in \mathbb{N}_0\}$$

Máquinas de Turing: cálculo de funciones

Una máquina de Turing M calcula la función parcial $f : \mathbb{N}^k \to \mathbb{N}$ si $\Sigma = \{0, 1\}$ y

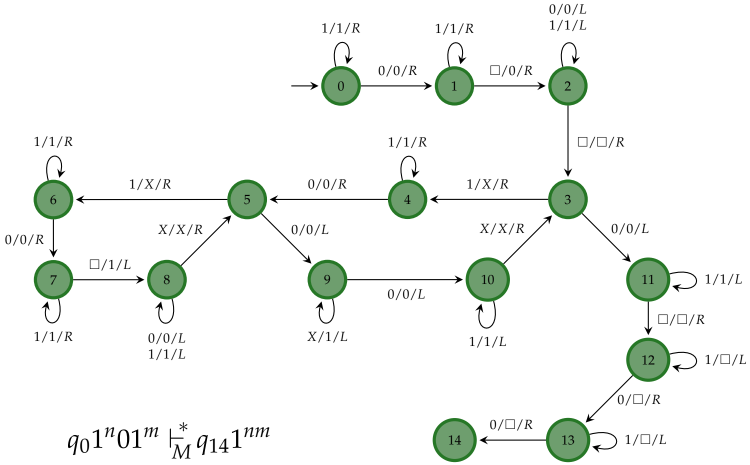
$$f(n_1, \ldots, n_k) = m \iff \begin{cases} \exists\, q \in Q,\ q1^{n_1}01^{n_2}0 \cdots 01^{n_k} \vdash_M^* q1^m, \\ q1^m \text{ es un estado de parada} \end{cases}$$

Máquinas de Turing: cálculo de funciones



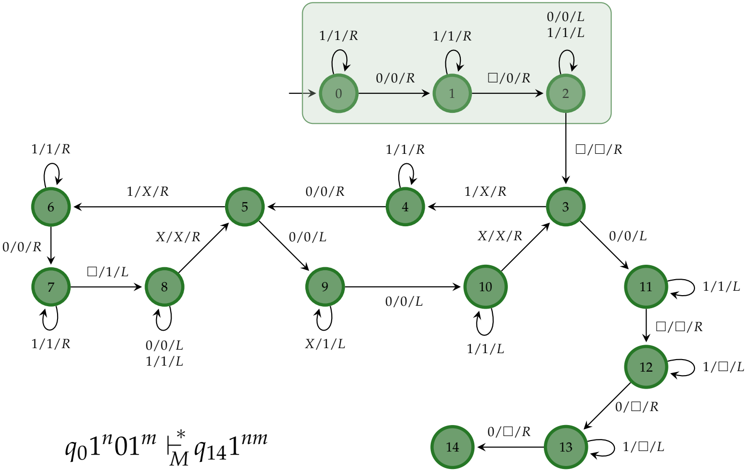
$$q_0 1^n 0 1^m \vdash_M^* q_3 1^{n+m}$$

Máquinas de Turing: cálculo de funciones



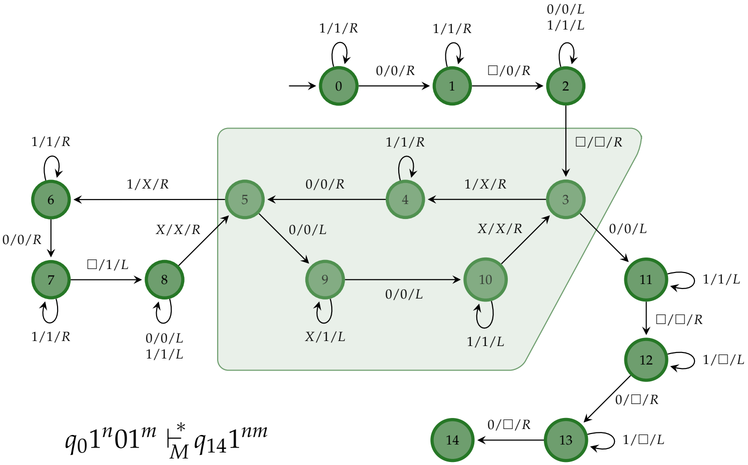
$$q_0 1^n 0 1^m \vdash_M^* q_{14} 1^{nm}$$

Máquinas de Turing: cálculo de funciones



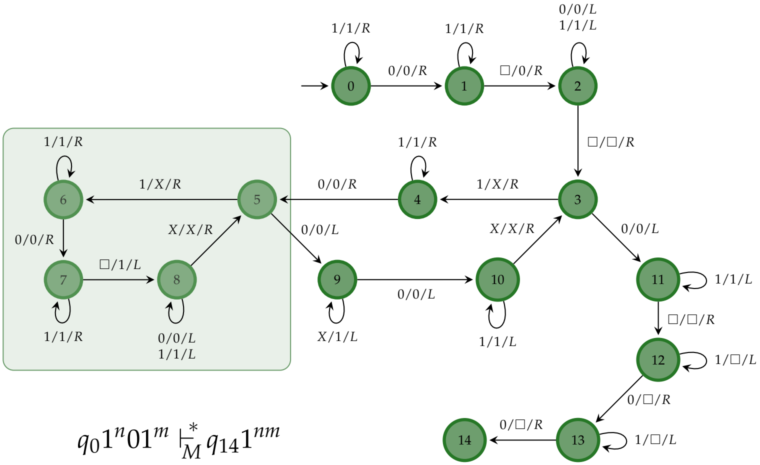
$$q_0 1^n 0 1^m \vdash_M^* q_{14} 1^{nm}$$

Máquinas de Turing: cálculo de funciones



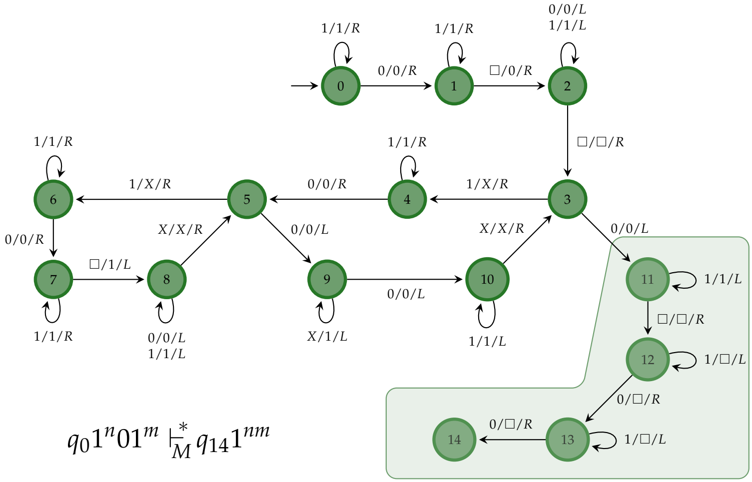
$$q_0 1^n 0 1^m \vdash_M^* q_{14} 1^{nm}$$

Máquinas de Turing: cálculo de funciones



$$q_0 1^n 0 1^m \vdash_M^* q_{14} 1^{nm}$$

Máquinas de Turing: cálculo de funciones



$$q_0 1^n 0 1^m \vdash_M^* q_{14} 1^{nm}$$

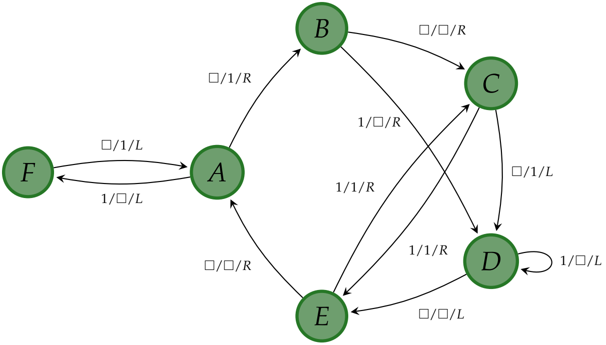
La tesis de Church-Turing

The expression "machine process" of course means one which could be carried out by the type of machine I was considering.

Alan Turing, 'On Computable Numbers, with an Application to the Entscheidungsproblem'. Proceedings of the London Mathematical Society, series 2, 42 (1936-37), 230-265.

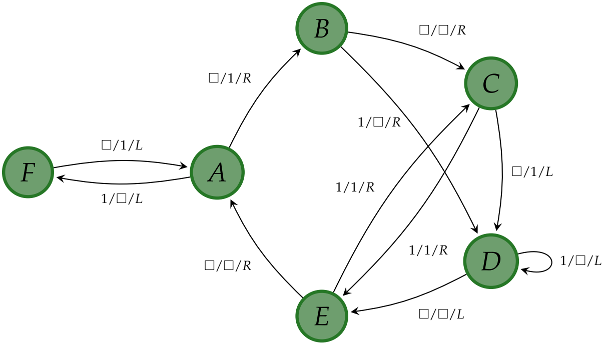
La tesis de Church-Turing

- Comportamiento increíblemente complejo:



La tesis de Church-Turing

- Comportamiento increíblemente complejo:



$\geq 3 \cdot 10^{1730}$ pasos empezando en una cinta en blanco

La tesis de Church-Turing

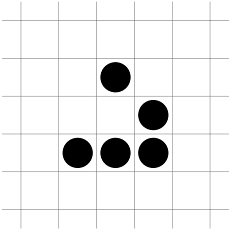
- Variaciones

La tesis de Church-Turing

- Variaciones
- Otros modelos de cálculo:
    - Funciones recursivas
    - λ-cálculo
    - Sistemas de Post
    - $\ldots$

La tesis de Church-Turing

- Variaciones
- Otros modelos de cálculo:
  - Funciones recursivas
  - λ-cálculo
  - Sistemas de Post
  - … (¡incluído el juego de la vida!)



Decibilidad

Sea Σ un alfabeto y sea $\mathscr{L} \subset \Sigma^*$.

- $\mathscr{L}$ es *recursivamente enumerable* si existe una máquina de Turing M tal que $\mathscr{L} = \mathscr{L}(M)$.

Decibilidad

Sea Σ un alfabeto y sea $\mathscr{L} \subset \Sigma^*$.

- $\mathscr{L}$ es *recursivamente enumerable* si existe una máquina de Turing M tal que $\mathscr{L} = \mathscr{L}(M)$.

El *lenguaje aceptado* por una máquina de Turing M es

$$\mathscr{L}(M) = \{w \in \Sigma^* : \exists\, p \in F,\ \exists\, \alpha_1, \alpha_2 \in \Gamma^*,\ q_0 w \vdash_M^* \alpha_1 q \alpha_2\}.$$

Decibilidad

Sea Σ un alfabeto y sea $\mathscr{L} \subset \Sigma^*$.

- $\mathscr{L}$ es *recursivamente enumerable* si existe una máquina de Turing M tal que $\mathscr{L} = \mathscr{L}(M)$.

El *lenguaje aceptado* por una máquina de Turing M es

$$\mathscr{L}(M) = \{w \in \Sigma^* : \exists\, p \in F,\ \exists\, \alpha_1, \alpha_2 \in \Gamma^*,\ q_0 w \vdash_M^* \alpha_1 q \alpha_2\}.$$

- $\mathscr{L}$ es *recursivo* o *decidible* si existe una máquina de Turing M tal que $\mathscr{L} = \mathscr{L}(M)$ y M para cualquiera sea su entrada.

Decibilidad

Teorema.

Existen lenguajes $\mathscr{L} \subset \{0, 1\}^*$ *no recursivamente enumerables.*

Decibilidad

Teorema.

Existen lenguajes $\mathscr{L} \subset \{0, 1\}^*$ *no recursivamente enumerables.*

Demostración.

Hay más lenguajes que máquinas de Turing. $\square$

Decibilidad

Teorema.

Existen lenguajes $\mathscr{L} \subset \{0, 1\}^*$ no recursivamente enumerables.

Otra demostración.

Consideramos biyecciones

$$\begin{aligned} i \in \mathbb{N} &\longmapsto M_i \in TM \\ i \in \mathbb{N} &\longmapsto w_i \in \{0, 1\}^* \end{aligned}$$

y definimos

$$\mathscr{D} = \{w_i : w_i \notin \mathscr{L}(M_i)\}.$$

Entonces no existe $M \in TM$ tal que $\mathscr{D} = \mathscr{L}(M)$.

$\square$

Decibilidad

Teorema.
Existen lenguajes $\mathscr{L} \subset \{0, 1\}^*$ *no recursivamente enumerables.*

Teorema.
Existen lenguajes $\mathscr{L} \subset \{0, 1\}^*$ *recursivamente enumerables no recursivos.*

Decibilidad

Consideremos una ‘codificación’

$$(M, w) \in TM \times \{0, 1\}^* \longmapsto \langle M, w \rangle \in \{0, 1\}^*$$

y el lenguaje

$$\mathscr{U} = \{\langle M, w \rangle : w \in \mathscr{L}(M)\}.$$

Decibilidad

Consideremos una 'codificación'

$$(M, w) \in TM \times \{0, 1\}^* \longmapsto \langle M, w\rangle \in \{0, 1\}^*$$

y el lenguaje

$$\mathscr{U} = \{\langle M, w\rangle : w \in \mathscr{L}(M)\}.$$

Teorema.

$\mathscr{U}$ es recursivamente enumerable.

Decibilidad

Consideremos una ‘codificación’

$$(M, w) \in TM \times \{0, 1\}^* \longmapsto \langle M, w \rangle \in \{0, 1\}^*$$

y el lenguaje

$$\mathscr{U} = \{\langle M, w \rangle : w \in \mathscr{L}(M)\}.$$

Teorema.

$\mathscr{U}$ es recursivamente enumerable.

Demostración.

Existen máquinas de Turing universales. $\square$

Decibilidad

Consideremos una 'codificación'

$$(M, w) \in TM \times \{0, 1\}^* \longmapsto \langle M, w \rangle \in \{0, 1\}^*$$

y el lenguaje

$$\mathscr{U} = \{\langle M, w \rangle : w \in \mathscr{L}(M)\}.$$

Teorema.
$\mathscr{U}$ es recursivamente enumerable.

Teorema.
$\mathscr{U}$ no es recursivo.

Decibilidad

- Un lenguaje $\mathscr{L}$ es recursivo sii su complemento $\mathscr{L}^c$ es recursivo.

Decibilidad

- Un lenguaje $\mathscr{L}$ es recursivo sii su complemento $\mathscr{L}^c$ es recursivo.

- En particular,
$$\mathscr{D}^c = \{w_i : w_i \in \mathscr{L}(M_i)\}$$
no es recursivo.

Decibilidad

- Un lenguaje $\mathscr{L}$ es recursivo sii su complemento $\mathscr{L}^c$ es recursivo.
- En particular,
$$\mathscr{D}^c = \{w_i : w_i \in \mathscr{L}(M_i)\}$$
no es recursivo.
- Supongamos que $\mathscr{U}$ es recursivo.
Entonces el siguiente algoritmo decide el problema de pertenencia a $\mathscr{D}^c$, lo que es imposible:

Entrada: $w \in \{0, 1\}^*$
Encontrar $i \in \mathbb{N}$ **tal que** $w = w_i$
Encontrar $M \in MT$ **tal que** $\langle M \rangle = i$
Aceptar w **sii** $\langle M, w \rangle \in \mathscr{U}$

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M \rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *y* $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *son no recursivamente enumerables.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *y* $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *son no recursivamente enumerables.*
- (Rice) *Sea S un conjunto de lenguajes recursivamente enumerables no trivial. Entonces* $\{\langle M\rangle : \mathscr{L}(M) \in S\}$ *es indecidible.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M \rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M \rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M \rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *y* $\{\langle M \rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *son no recursivamente enumerables.*
- (Rice) *Sea S un conjunto de lenguajes recursivamente enumerables no trivial. Entonces* $\{\langle M \rangle : \mathscr{L}(M) \in S\}$ *es indecidible.*

Teorema.

(Propiedades de máquinas)

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M\rangle : \mathscr{L}(M)$ *es recursivo*$\}$ *y* $\{\langle M\rangle : \mathscr{L}(M)$ *es recursivo*$\}$ *son no recursivamente enumerables.*
- (Rice) *Sea* S *un conjunto de lenguajes recursivamente enumerables no trivial. Entonces* $\{\langle M\rangle : \mathscr{L}(M) \in S\}$ *es indecidible.*

Teorema.

(Propiedades de máquinas)

- *Es indecidible si una máquina de Turing sobre* $\{0, 1, \square\}$ *alguna vez escribe tres* 1*s seguidos en su cinta.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *y* $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *son no recursivamente enumerables.*
- (Rice) *Sea S un conjunto de lenguajes recursivamente enumerables no trivial. Entonces* $\{\langle M\rangle : \mathscr{L}(M) \in S\}$ *es indecidible.*

Teorema.

(Propiedades de máquinas)

- *Es indecidible si una máquina de Turing sobre* $\{0, 1, \square\}$ *alguna vez escribe tres* 1*s seguidos en su cinta.*
- *Es indecidible si un máquina de Turing no para para alguna entrada.*

Decibilidad

Teorema.

(Propiedades de lenguajes)

- $\{\langle M\rangle : \mathscr{L}(M) \neq \varnothing\}$ *es recursivamente enumerable pero no recursivo.*
- $\{\langle M\rangle : \mathscr{L}(M) = \varnothing\}$ *no es recursivamente enumerable.*
- $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *y* $\{\langle M\rangle : \mathscr{L}(M) \text{ es recursivo}\}$ *son no recursivamente enumerables.*
- (Rice) *Sea S un conjunto de lenguajes recursivamente enumerables no trivial. Entonces $\{\langle M\rangle : \mathscr{L}(M) \in S\}$ es indecidible.*

Teorema.

(Propiedades de máquinas)

- *Es indecidible si una máquina de Turing sobre $\{0, 1, \square\}$ alguna vez escribe tres 1s seguidos en su cinta.*
- *Es indecidible si un máquina de Turing no para para alguna entrada.*
- *Es indecidible si dos máquinas de Turing hacen lo mismo.*

El problema de las palabras

Consideremos un grupo finitamente presentado por generadores y relaciones:

$$G = \langle x_1, \ldots, x_n : r_1, \cdots, r_m \rangle = \frac{\mathsf{L}(x_1, \ldots, x_n)}{\langle\langle r_1, \ldots, r_m \rangle\rangle}.$$

El problema de las palabras

Consideremos un grupo finitamente presentado por generadores y relaciones:

$$G = \langle x_1, \ldots, x_n : r_1, \cdots, r_m \rangle = \frac{\mathsf{L}(x_1, \ldots, x_n)}{\langle\langle r_1, \ldots, r_m \rangle\rangle}.$$

Decimos que *el problema de las palabras para G es soluble* si existe un algoritmo para resolver el siguiente problema:

Dada una palabra $w \in \mathsf{L}(x_1, \ldots, x_n)$*, ¿es* $w = 1$ *en G?*

[1] M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. **71** (1911), no. 1, 116–144.

El problema de las palabras

Usando el teorema de Tietze que describe todas las posibles presentaciones finitas de un grupo finitamente presentado, uno puede probar:

Proposición.

Si el problema de las palabras para un grupo G es soluble con respecto a una presentación finita, lo es con respecto a todas.

El problema de las palabras: grupos libres

Proposición.

El problema de las palabras para un grupo libre $\mathsf{L}(x_1, \ldots, x_n)$ *es soluble.*

El problema de las palabras: grupos libres

Proposición.

El problema de las palabras para un grupo libre $\mathsf{L}(x_1, \ldots, x_n)$ *es soluble.*

Demostración.

Sea $w \in L(x_1, \ldots, x_n)$ y $\bar{w}$ la palabra reducida correspondiente.
Entonces $w = 1$ sii $\bar{w} = 1$. $\square$

El problema de las palabras: grupos finitos

Proposición.

Si G es un grupo finito, entonces el problema de las palabras para G es soluble.

El problema de las palabras: grupos finitos

Proposición.

Si G es un grupo finito, entonces el problema de las palabras para G es soluble.

Demostración.

Si $G = \langle x_1, \ldots, x_n : r_1, \cdots, r_m \rangle$ es finito, el algoritmo de Todd-Coxeter permite construir el grafo de Cayley $\mathscr{C}$ para G con respecto al conjunto generador $\{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$.

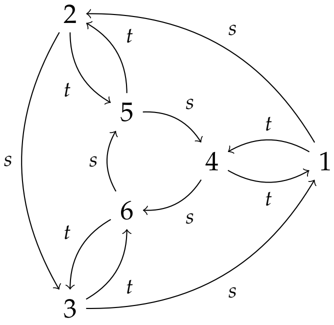
Para ver si una palabra $w \in \mathsf{L}(x_1, \ldots, x_n)$ es trivial en G, uno recorre el camino que empieza en $1 \in \mathscr{C}$ siguiente las letras que aparecen en w. Este camino es cerrado sii $w = 1$ en G. $\square$

El problema de las palabras: grupos finitos

$$S_3 = \langle s, t : s^3,\, t^2,\, tsts^{-2} \rangle$$

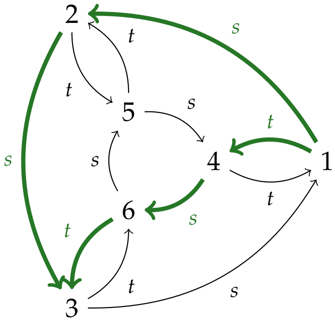
El problema de las palabras: grupos finitos

$$S_3 = \langle s, t : s^3,\ t^2,\ tsts^{-2} \rangle$$



El problema de las palabras: grupos finitos

$$S_3 = \langle s, t : s^3,\ t^2,\ tsts^{-2} \rangle$$



$$w = s^{-1}s^{-1}tst = 1$$

Un desvío
El problema de las palabras para semigrupos

Semigrupos: congruencias

Sea S un semigrupo.

Una *congruencia* en S es una relación de equivalencia $\equiv$ tal que

$$a \equiv a', \, b \equiv b' \implies ab \equiv a'b'.$$

Es claro que podemos definir un *semigrupo cociente* $S/\equiv$.

Semigrupos: congruencias

Proposición.

Si S es un semigrupo, y $\Gamma \subset S \times S$, existe una menor congruencia $\equiv$ tal que

$$(s, s') \in \Gamma \implies s \equiv s'$$

Llamamos a $\equiv$ la congruencia generada por Γ y la escribimos $\langle\langle \Gamma \rangle\rangle$.

Semigrupos: congruencias

Proposición.

Si S es un semigrupo, y $\Gamma \subset S \times S$, existe una menor congruencia $\equiv$ tal que

$$(s, s') \in \Gamma \implies s \equiv s'$$

Llamamos a $\equiv$ la congruencia generada por Γ y la escribimos $\langle\langle \Gamma \rangle\rangle$.

Demostración.

La congruencia $\langle\langle \Gamma \rangle\rangle$ es

$$\bigcap_{\substack{C \subset S \times S \text{ congruencia en } S \\ \Gamma \subset C}} C$$

$\square$

Semigrupos: presentaciones

Si S es un semigrupo, una presentación para S es un isomorfismo

$$S \cong \frac{\mathsf{S}(x_1, \ldots, x_n)}{\langle\!\langle l_1 \equiv r_1, \ldots, l_m \equiv r_m \rangle\!\rangle}.$$

donde $\mathsf{S}(x_1, \ldots, x_n)$ es el semigrupo libre sobre $\{x_1, \ldots, x_m\}$.
Escribimos

$$S = \langle x_1, \ldots, x_n : l_1 = r_1, \ \ldots, \ l_m = r_m \rangle$$

Semigrupos: presentaciones

Si S es un semigrupo, una presentación para S es un isomorfismo

$$S \cong \frac{\mathsf{S}(x_1, \ldots, x_n)}{\langle\langle l_1 \equiv r_1, \ldots, l_m \equiv r_m \rangle\rangle}.$$

donde $\mathsf{S}(x_1, \ldots, x_n)$ es el semigrupo libre sobre $\{x_1, \ldots, x_m\}$.
Escribimos

$$S = \langle x_1, \ldots, x_n : l_1 = r_1, \ \ldots, \ l_m = r_m \rangle$$

Por ejemplo,

$$\mathbb{N}_0^3 = \langle x_1, x_2, x_3 : x_1x_2 = x_2x_1, \ x_2x_3 = x_3x_2, \ x_1x_3 = x_3x_1 \rangle$$

El problema de las palabras para semigrupos

Consideremos un semigrupo finitamente presentado por generadores y relaciones:

$$S = \langle x_1, \ldots, x_n : l_1 = r_1, \cdots , l_m = r_m \rangle$$

Decimos que *el problema de las palabras para S es soluble* si existe un algoritmo para resolver el siguiente problema:

Dadas palabras $w, w' \in \mathsf{S}(x_1, \ldots, x_n)$*, ¿es* $w = w'$ *en S?*

El problema de las palabras para semigrupos

Teorema. (Markov–Post, 1947)

Existe un semigrupo finitamente presentado S con problema de las palabras insoluble.

[1] A. Markoff, *On the impossibility of certain algorithms in the theory of associative systems*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **55** (1947), 583–586.

[2] Emil L. Post, *Formal reductions of the general combinatorial decision problem*, Amer. J. Math. **65** (1943), 197–215.

El problema de las palabras para semigrupos

Sea $M = (Q, \Gamma, \Box, \Sigma, \delta, q_0, F)$ una máquina de Turing con

$$\Gamma = \{s_0 = \Box, s_1, \ldots, s_n\}$$
$$Q = \{q_0, \ldots, q_N\}$$

Construimos un semigrupo finitamente presentado

$$S(M) = \langle s_0, \ldots, s_n, q_0 \ldots, q_N, q, h : R\rangle$$

con q y h dos símbolos nuevos y R un conjunto finito de igualdades.

El problema de las palabras para semigrupos

El conjunto R de relaciones contiene por un lado:

Si $\delta(q_i, s_j) = (q_k, s_l, L)$,

$$s_u q_i s_j = q_k s_u s_l, \qquad \forall u \in \{1, \ldots, n\};$$

$$h q_i s_j = h q_k s_0 s_l;$$

Si $\delta(q_i, s_0) = (q_k, s_l, L)$,

$$s_u q_i h = q_k s_u s_l h, \qquad \forall u \in \{1, \ldots, n\};$$

$$h q_i h = h q_k s_l h;$$

Si $\delta(q_i, s_j) = (q_k, s_l, R)$,

$$q_i s_j = s_l q_k;$$

Si $\delta(q_i, s_0) = (q_k, s_l, R)$,

$$q_i h = s_l q_k h.$$

El problema de las palabras para semigrupos

…y por otro:

$$
\begin{aligned}
q_u s_i &= q_u, && \forall q_u \in F,\ i \in \{0, \dots, n\}; \\
s_i q_u h &= q_u h, && \forall q_u \in F,\ i \in \{0, \dots, n\};
\end{aligned}
$$

y finalmente

$$
hq_u h = q, \qquad \forall q_u \in F.
$$

El problema de las palabras para semigrupos

Proposición.

Sea $w \in \Sigma^*$. Entonces

$$w \in \mathscr{L}(M) \iff hq_0wh = q \text{ en } S(M).$$

El problema de las palabras para semigrupos

Teorema. (Markov–Post, 1947)

Existe un semigrupo finitamente presentado S con problema de las palabras insoluble.

[1] A. Markoff, *On the impossibility of certain algorithms in the theory of associative systems*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **55** (1947), 583–586.

[2] Emil L. Post, *Formal reductions of the general combinatorial decision problem*, Amer. J. Math. **65** (1943), 197–215.

El problema de las palabras para semigrupos

Demostración.

Consideremos el lenguaje

$$\mathscr{U} = \{\langle M, w\rangle : w \in \mathscr{L}(M)\}.$$

Recordemos que $\mathscr{U}$ es recursivamente enumerable pero no recursivo. Sea $M_{\mathscr{U}}$ una máquina de Turing que reconoce a $\mathscr{U}$.

Entonces el problema

> *Dada una máquina de Turing M y una palabra $w \in \Sigma(M)^*$, si $u = \langle M, w\rangle$, ¿es $u \in \mathscr{L}(M)$?*

es equivalente al problema

> *Dada una máquina de Turing M y una palabra $w \in \Sigma(M)^*$, si $u = \langle M, w\rangle$, ¿es $hq_0uh = q$ en $S(M_{\mathscr{U}})$?*

$\square$

El problema de las palabras

Teorema. (Novikov–Britton–Boone, 1955)

Existen grupos finitamente presentados con problema de las palabras insoluble.

El problema de las palabras

Teorema. (Novikov–Britton–Boone, 1955)

Existen grupos finitamente presentados con problema de las palabras insoluble.

[1] William W. Boone, *Certain simple, unsolvable problems of group theory. I*. I, Nederl. Akad. Wetensch. Proc. Ser. A. **57** (1954), 231–237 = Indag. Math. 16, 231–237 (1954); II, Nederl. Akad. Wetensch. Proc. Ser. A. **57** (1954), 492–497 = Indag. Math. 16, 492–497 (1954); III, Nederl. Akad. Wetensch. Proc. Ser. A. **58** (1955), 252–256 = Indag. Math. 17, 252–256 (1955); IV, Nederl. Akad. Wetensch. Proc. Ser. A. 58 = Indag. Math. **17** (1955), 571–577; V, IV, Nederl. Akad. Wetensch. Proc. Ser. A. 60 = Indag. Math. **19** (1957), 22–27, 227–232.

[2] J. L. Britton, *The word problem for groups*, Proc. London Math. Soc. (3) **8** (1958), 493–506.

[3] P. S. Novikov, *Ob algoritmičeskoĭ nerazrešimosti problemy toždestva slov v teorii grupp*, Trudy Mat. Inst. im. Steklov. no. 44, Izdat. Akad. Nauk SSSR, Moscow, 1955.

Problemas indecidibles en teoría de grupos

Definición.

Una clase $\mathscr{P}$ de grupos finitamente presentados es una propiedad de Markov *si*

- *es invariante por isomorfismo:*

$$G \cong G' \in \mathscr{P} \implies G \in \mathscr{P}.$$

- $\mathscr{P} \neq \emptyset$.
- *Existe un grupo G finitamente presentado que no es subgrupo de ningún grupo de $\mathscr{P}$.*

Problemas indecidibles en teoría de grupos

Las siguientes son propiedades de Markov:

- ser trivial;
- ser finito;
- tener exponente finito;
- ser un p-grupo;
- ser abeliano;
- ser soluble;
- ser nilpontente;
- ser simple;
- ser de torsión;
- ser sin-torsión;
- ser libre;
- tener problema de las palabras soluble;
- tener problema de conjugación soluble.

Problemas indecidibles en teoría de grupos

Teorema. (Adian–Rabin, 1958)
Si $\mathscr{P}$ es una propiedad de Markov, entonces $\mathscr{P}$ no es decidible.

Problemas indecidibles en teoría de grupos

Teorema. (Adian–Rabin, 1958)
Si $\mathscr{P}$ es una propiedad de Markov, entonces $\mathscr{P}$ no es decidible.

Corolario.
No hay un algoritmo uniforme para decidir si dos presentaciones finitas determinan grupos isomorfos.

Demostración.
Un algoritmo para resolver este problema podría ser usado para resolver el problema de decidir si un grupo es trivial. $\square$

Consecuencias algebraicas de la decibilidad

Consecuencias algebraicas de la decibilidad

Teorema. (Higman, 1961)

Un grupo finitamente generado G es subgrupo de algún grupo finitamente presentado sii G puede ser presentado recursivamente.

Consecuencias algebraicas de la decibilidad

Teorema. (Higman, 1961)

Un grupo finitamente generado G es subgrupo de algún grupo finitamente presentado sii G puede ser presentado recursivamente.

Teorema. (Boone–Higman, 1973)

Un grupo finitamente generado tiene problema de las palabras soluble sii es un subgrupo de un subgrupo simple de un grupo finitamente presentado.

Restricción del dominio de la lucha

Grupos con problema de las palabras decidible

- Grupos libres
- Grupos finitos
- Grupos policíclicos
- Grupos hiperbólicos
- Grupos de movimientos
- Grupos de Coxeter y de trenzas
- Grupos residualmente finitos

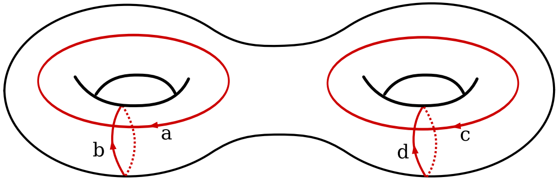
Grupos con problema de las palabras decidible

- Grupos libres
- Grupos finitos
- Grupos policíclicos
- Grupos hiperbólicos
- Grupos de movimientos
- Grupos de Coxeter y de trenzas

Grupos automáticos

- Grupos residualmente finitos

Grupos fundamentales de superficies



$$\pi_1(M_2) = \langle a, b, c, d : aba^{-1}b^{-1}cdc^{-1}d^{-1} \rangle$$

Grupos fundamentales de superficies

En general, la superficie compacta orientable de género g tiene grupo fundamental

$$\pi_1(M_g) = \langle x_i, y_i,\, 1 \leq i \leq g : [x_1, y_1] \cdots [x_g, y_g] \rangle$$

Grupos fundamentales de superficies

En general, la superficie compacta orientable de género g tiene grupo fundamental

$$\pi_1(M_g) = \langle x_i, y_i,\ 1 \leq i \leq g : [x_1, y_1] \cdots [x_g, y_g] \rangle$$

Teorema. (Max Dehn, 1912)

El grupo fundamental de una superficie compacta tiene problema de las palabras soluble.

[1] M. Dehn, *Transformation der Kurven auf zweiseitigen Flächen*, Math. Ann. **72** (1912), no. 3, 413–421.

Grupos fundamentales de superficies

Demostración.

Vale el *algoritmo de Dehn*:

> *Si w es una palabra reducida en los generadores y $w = 1$ en $\pi_1(M_g)$, entonces w contiene más de la mitad de una permutación cíclica de la relación o de su inversa.*

□

Grupos con una relación

Teorema. (Magnus, 1932)

Si $G = \langle x_1, \cdots x_n : r\rangle$ *puede ser finitamente presentado con* una *relación, entonces* G *tiene problema de las palabras soluble.*

Teoría de la cancelación

Sea $G = \langle X : R \rangle$ un grupo finitamente presentado con R simétrico y cíclicamente cerrado.

Definición.

Si $r_1, r_2 \in R$ son tales que $r_1 = bc_1$ y $r_2 = bc_2$ (sin cancelación), decimos que b es una pieza *para R.*

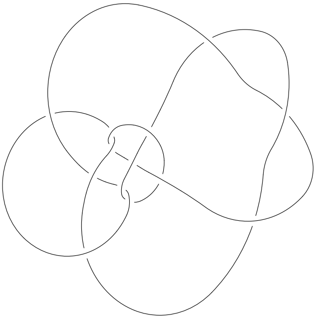
Decimos que G satisface la condición $C(p)$ si

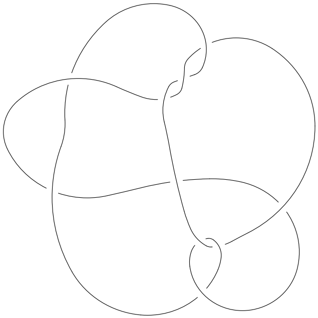
$$\textit{ningún elemento de } R \textit{ es producto de menos de } p \textit{ piezas}.$$

Teoría de la cancelación

Teorema.
Si G admite una presentación $\langle X : R \rangle$ que satisface la condición $C(6)$, entonces G tiene problema de las palabras soluble.

El grupo fundamental del complemento de un nudo





El grupo fundamental del complemento de un nudo

Teorema. (Waldhausen, 1968)

El grupo fundamental de un nudo manso tiene problema de las palabras resoluble.

[1] Friedhelm Waldhausen, *The word problem in fundamental groups of sufficiently large irreducible 3-manifolds*, Ann. of Math. (2) **88** (1968), 272–280.

Referencias

[1] Elwyn R. Berlekamp, John H. Conway, and Richard K. Guy, *Winning ways for your mathematical plays*, 2nd ed., Vol. 4, Natick, MA: A K Peters., 2004.

[2] John E. Hopcroft and Jeffrey D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley Publishing Co., Reading, Mass., 1979. Addison-Wesley Series in Computer Science.

[3] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995.

[4] John Stillwell, *Classical topology and combinatorial group theory*, 2nd ed., Graduate Texts in Mathematics, vol. 72, Springer-Verlag, New York, 1993.

[5] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer-Verlag, Berlin, 1977. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 89.