Algoritmos, lenguajes, grafos y grupos profinitos

por

Luis Ribes

1. Introducción

El propósito de este artículo con un título tan largo y heterogéneo es precisamente un intento de mostrar, a pequeña escala, que la heterogeneidad de las matemáticas es, a veces, sólo aparente.

El artículo describe una serie de problemas en temas dispares, en forma de cinco conjeturas, que en principio parecen muy diferentes. Las Conjeturas $1-4$ describen en realidad problemas equivalentes. La Conjetura 5 es una generalización de las anteriores. Todas estas preguntas tienen respuestas positivas, como se indica en las secciones 5, 8 y 9.

La primera conjetura utiliza una terminología cuasi-lógica y se refiere a la posible existencia de un algoritmo para decidir si cierto tipo de objetos (monoides o semigrupos finitos) pertenecen o no a una cierta clase dada (una variedad). La segunda conjetura es puramente combinatoria; dado un objeto descrito de forma muy concreta (un monoide finito), el problema es encontrar un método general para calcular los elementos de un cierto subconjunto (el 'núcleo' del monoide) que se puede describir también en términos sencillos. Estas dos primeras conjeturas surgieron en el ámbito de la computación teórica.

La tercera conjetura se plantea en términos de lenguajes 'racionales' (o, si se prefiere, de la teoría de autómatas o de gramáticas formales regulares) y en términos topológicos. En este caso, el problema es el de la existencia de un procedimiento constructivo para calcular la clausura de ciertos subconjuntos (lenguajes racionales) de ciertos espacios topológicos (monoides libres con la topología 'profinita').

En la cuarta conjetura, la conexión con las matemáticas discretas es menos clara y, en todo caso, la relación con las conjeturas anteriores parece ténua. De hecho, esta conjetura es equivalente a las anteriores. La pregunta en este caso es si el producto de un número finito de subgrupos finitamente generados de un grupo libre es un conjunto cerrado con respecto a una cierta topología. Las Conjeturas 3 y 4 (así como otras que no mencionamos aquí), surgieron en el proceso de intentar resolver la Conjetura 2.

En este artículo se presenta un esquema de cómo dar una respuesta afirmativa a todas estas preguntas. El método que indicamos aquí tiene poco de combinatorio. Las herramientas básicas que se utilizan son mas bien topológicas: grupos topológicos compactos y totalmente discontinuos y su forma de operar sobre ciertos espacios topológicos que poseen al mismo tiempo una estructura de grafos.

No se incluyen demostraciones. Tan solo he pretendido describir unos problemas y hacer accesibles algunas de las ideas que intervienen en su resolución.

A lo largo del artículo y en la útima sección, se mencionan algunas de las fuentes donde se puede encontrar el enunciado de los problemas originales así como las demostraciones de los teoremas.

2. Variedades de Monoides Finitos

Recordemos que un **semigrupo** es un conjunto no vacío dotado de una operación binaria asociativa. Un semigrupo que posee un elemento neutro con respecto a su operación se denomina un **monoide**. Por ejemplo, el subconjunto de los números enteros no negativos $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ es un monoide con respecto a la operación '+', mientras que $S = \{1, 2, 3, \dots\}$ es un solamente un semigrupo. Un **grupo** es un monoide en el que todo elemento tiene un 'inverso'. Así, el monoide de todos los números enteros $\mathbf{Z}$ es también un grupo.

Decimos que una clase $\mathcal{V}$ no vacía de semigrupos (o de monoides) finitos es una *variedad* si contiene todos los subsemigrupos, los cocientes y los productos directos finitos de los semigrupos en $\mathcal{V}$. Se puede especificar una variedad de muchas maneras. Por ejemplo, dando una lista de los semigrupos en $\mathcal{V}$ junto con sus tablas de multiplicar; o bien, como el conjunto de todos los semigrupos (monoides) finitos que satisfagan ciertas ecuaciones (e.g., los semigrupos en los que $xy = yx$ para todo x, y en el semigrupo, forman la variedad de los semigrupos abelianos); o bien, como la variedad *generada* por un conjunto dado $\{S_1, \dots S_n\}$ de semigrupos (monoides), es decir, la variedad que se obtiene considerando todos los semigrupos (monoides) finitos que surgen tomando los subsemigrupos, cocientes y productos directos finitos de los semigrupos $S_1, \dots S_n$, e iterando este proceso.

Otros Ejemplos de Variedades de Monoides

1. $\mathcal{A}$, la colección de los monoides aperiódicos (un monoide M es aperiódico si para todo $a \in M$, existe $n \in \mathbf{N}$ tal que $a^n = a^{n+1}$; o, de manera equivalente, si siempre que N sea un subsemigrupo de M que sea un grupo, se sigue que N consiste en un solo elemento).

2. $\mathcal{B}$, la colección de los monoides que son bandas (monoides en los que cada elemento a es un idempotente, es decir, $a^2 = a$).

3. $\mathcal{G}$, la colección de todos los grupos finitos es una variedad de monoides, pues, como se verifica con facilidad, un submonoide de un grupo finito es un subgrupo.

4. Sea p un número primo y sea C_p el grupo cíclico de orden p. La variedad de monoides generada por C_p es simplemente la clase de todos los espacios vectoriales de dimensión finita sobre el cuerpo $\mathbf{F}_p$ con p elementos.

Una variedad $\mathcal{V}$ de semigrupos (monoides) finitos se llama **decidible** si existe un algoritmo que permite determinar si cualquier semigrupo (monoide) finito dado pertenece o no a la variedad. Por ejemplo, está claro que las

las variedades que hemos mencionado más arriba son todas decidibles. Para ejemplos de variedades no decidibles, consultar [Rhodes 90].

Consideremos una variedad $\mathcal{V}$ de monoides finitos y supongamos que $\mathcal{L}$ es una variedad de grupos finitos. El **producto de Malcev** $\mathcal{V} \bowtie \mathcal{L}$ se define como la variedad de monoides finitos generada por todos los monoides M para los que existe un epimorfismo $\pi : M \longrightarrow G$ sobre un grupo $G \in \mathcal{L}$ de manera que $\pi^{-1}(1) \in \mathcal{V}$ (1 es el elemento identidad del grupo G):

$$1 \longrightarrow \pi^{-1}(1) \longrightarrow M \longrightarrow G \longrightarrow 1.$$

Conjetura 1 *Si una variedad de monoides finitos $\mathcal{V}$ es decidible, también lo es el producto de Malcev $\mathcal{V} \bowtie \mathcal{G}$, donde $\mathcal{G}$ es la variedad de todos los grupos finitos.*

3. Una Conjetura de Rhodes

En esta sección exponemos una pregunta famosa de J. Rhodes, la cual ha servido, en realidad, de motivación a todas las conjeturas que mencionamos en este artículo. Para una descripción de los antecedentes del trabajo de Rhodes y las interrelaciones de esa pregunta con otros problemas de computación teórica, el lector puede consultar [Henckell-Margolis-Pin-Rhodes 91]. La cuestión planteada por Rhodes es si se puede describir algorítmicamente un cierto submonoide de un monoide finito, el llamado 'núcleo' del monoide. Nosotros nos limitamos aquí a definir ese núcleo.

Sean M y N monoides finitos. Un *morfismo relacional* de M a N es una función

$$\tau : M \longrightarrow \mathcal{P}(N)$$

de M al conjunto de todos los subconjuntos $\mathcal{P}(N)$ de N tal que

(i) $\tau(m) \neq \emptyset \quad (m \in M)$;

(ii) $\tau(mm') \supseteq \tau(m)\tau(m') \quad (m, m' \in M)$; y

(iii) $1 \in \tau(1)$ (por abuso de notación, 1 representa el elemento identidad de cada monoide).

Por ejemplo, si $\rho : N \longrightarrow M$ es un homomorfismo de monoides, entonces $\tau = \rho^{-1}$ es un morfismo relacional de M a N.

Dado un monoide finito M, definimos el *núcleo* $K(M)$ de M de la siguiente manera:

$$K(M) = \bigcap_{\tau} \tau^{-1}(1),$$

donde τ recorre el conjunto de todos los morfismos relacionales de M a cualquier grupo finito.

Conjetura 2. *Existe un algoritmo para computar el núcleo de cualquier monoide finito.*

4. Lenguajes

Sea A un conjunto finito no vacío, que aquí denominaremos un **alfabeto**. Consideremos el conjunto A^* de todas la *palabras* en el alfabeto A, es decir, expresiones formales $a_1a_2\cdots a_n$ donde los símbolos $a_1,\ldots,a_n$ son *letras* en el alfabeto A. La palabra vacía será denotada mediante 1. Definamos una multiplicación en A^* por concatenación:

$$(a_1a_2\cdots a_n)(b_1b_2\cdots b_m) = a_1a_2\cdots a_nb_1b_2\cdots b_m.$$

Con respecto a esta operación, A^* es un monoide infinito, el llamado **monoide libre** sobre la base A. Un **lenguaje** en el alfabeto A es simplemente un conjunto de palabras en el alfabeto A, es decir, un subconjunto de A^*. Nos interesamos en un tipo especial de lenguajes, los llamados lenguajes racionales. Se dice que un lenguaje L en el alfabeto A es **racional** si pertenece a la colección $\mathcal{R}$ de lenguajes definidos por el siguiente procedimiento inductivo:

1. El lenguaje vacío y todo lenguaje consistente en una sola palabra están en $\mathcal{R}$.
2. La unión de un conjunto finito de lenguajes en $\mathcal{R}$, pertenece a $\mathcal{R}$.
3. Si $L \in \mathcal{R}$, entonces $L^* \in \mathcal{R}$ (L^* es el submonoide de A^* generado por L, es decir, el conjunto de todas las palabras que se obtienen formando productos finitos de palabras en L).

La 'mayoría' de los lenguajes no son racionales; de hecho la colección de todos los lenguajes racionales en el alfabeto A es numerable. Un ejemplo de lenguaje no racional en el alfabeto $\{a,b\}$ es

$$\{a^nb^n \mid n \in \mathbf{N}\}.$$

Una manera equivalente de describir los lenguajes racionales es mediante autómatas. Los lenguajes racionales son precisamente los que se pueden 'reconocer' por autómatas con un número finito de estados (cf. [Eilenberg 74]).

Introduzcamos ahora una topología en el monoide libre A^* de manera que se convierta en un monoide topológico; en otras palabras, de forma que la multiplicación en A^* sea una función continua. La manera mas sencilla de describir esta topología es la de sumergir A^* en un grupo y definir una topología en este grupo. El grupo en cuestión es el grupo *libre* $F = F(A)$ en el conjunto A. Recordemos que los elementos de F se pueden representar como palabras 'reducidas' en el alfabeto $A \cup A^{-1}$, es decir palabras de la forma $a_1^{\epsilon_1}\cdots a_n^{\epsilon_n}$, donde $\epsilon_i = \pm 1$, de manera que estas palabras sean 'reducidas'. Esto quiere decir simplemente que no se permite que en tales palabras aparezcan subpalabras de la forma aa^{-1} o de la forma $a^{-1}a$ ($a \in A$). La multiplicación en F se hace por concatenación y una 'simplificación' natural para convertir el producto de dos palabras reducidas en una palabra reducida. (Esta manera de definir un grupo libre es muy intuitiva, pero requiere, como se sabe, un pequeño, pero

delicado, razonamiento para asegurarnos de que la multiplicación está bien definida.)

Claramente $A^* \subseteq F(A)$; de hecho, esta inclusión es un homomorfismo de monoides. Definamos una topología en el grupo libre $F = F(A)$. Sea $\mathcal{N}$ el conjunto de todos los subgrupos normales N de F tales que F/N sea un grupo finito. La topología en F es la única topología que hace de F un grupo topológico y de manera que $\mathcal{N}$ sea un sistema fundamental de entornos del elemento 1 de F. De forma equivalente, los entornos básicos de un elemento $f \in F$ son las clases fN ($N \in \mathcal{N}$). La topología en F así definida se denomina la **topología profinita** de F. A su vez, esta topología induce en A^* una topología que también llamamos profinita.

Conjetura 3 *Sea L un lenguaje racional en un alfabeto finito A. Entonces existe un algoritmo para computar la clausura $\bar{L}$ de L en la topología profinita de A^*. Además, $\bar{L}$ es un lenguaje racional en el alfabeto A.*

5. La Conjetura de Pin y Reutenauer

Se puede demostrar que las Conjeturas 1, 2 y 3, aparentemente tan distintas, son en realidad maneras equivalentes de plantear el mismo problema. Para una buena exposición de estas conjeturas y las relaciones entre ellas véase el artículo [Pin 89] de J-E. Pin. En un intento de hacer más inteligible el problema, J-E. Pin y Ch. Reutenauer establecen en [Pin-Reutenauer 91] otra conjetura que a su vez es equivalente a las anteriores.

Conjetura 4 *Sea $F = F(A)$ un grupo libre sobre un conjunto finito A. Supongamos que $H_1, H_2, \ldots, H_n$ sean subgrupos finitamente generados de F. Entonces el producto $H_1 H_2 \cdots H_n$ es un subconjunto cerrado en la topología profinita de F.*

Nótese que, en general, $H_1 H_2 \cdots H_n$ es solamente un subconjunto, no un subgrupo, de F. La única indicación dada por Pin y Reutenauer de que efectivamente esta conjetura pudiera tener una respuesta positiva es un resultado de M. Hall de 1950: si H es un subgrupo finitamente generado de un grupo libre F de rango finito, entonces H es la intersección de los subgrupos de F que contienen a H y son de índice finito en F. Es decir,

Teorema 1 ([Hall 50]) *La Conjetura 4 es cierta si $n = 1$.*

Aunque esta nueva conjetura de Pin y Reutenauer no parece hacer avanzar la solución del problema, sin embargo el hecho de que esté enunciada en términos de grupos y no de monoides o lenguajes es en realidad un progreso importante. La teoría de grupos es más rígida que la teoría de monoides o autómatas y existen muchos más métodos que uno puede intentar utilizar. La verificación de la Conjetura 4, y por tanto de todas las conjeturas, se sigue del próximo resultado.

Teorema 2 *Sea G un grupo virtualmente libre (es decir, G contiene un subgrupo libre de índice finito). Supongamos que $H_1, H_2, \ldots, H_n$ sean subgrupos*

finitamente generados de F. Entonces el producto $H_1H_2\cdots H_n$ es un subconjunto cerrado en la topología profinita de G.

Las secciones 6-8 de este artculo estn dedicadas a dar una somera indicación de los principales ingredientes para la demostración de este teorema.

6. Grupos Profinitos Libres

Un **grupo profinito** es un grupo topológico compacto, Hausdorff y totalmente discontinuo (esto último significa que cada punto es su propia componente conexa). De forma equivalente, un grupo profinito es un límite proyectivo de grupos finitos

$$G = \varprojlim_{i \in I} G_i$$

Todo grupo finito con la topología discreta es profinito; todo subgrupo cerrado de un producto cartesiano $\prod_{i\in I} G_i$ de grupos finitos discretos es un grupo profinito. La motivación mas importante para el estudio de grupos profinitos proviene de la teoría algebraica de números, pues un grupo profinito es exactamente un grupo de Galois de una extensión galoisiana de cuerpos dotado de una topología natural, la topología de Krull.

Por ejemplo, sea L un cuerpo finito, digamos con q elementos, y denotemos mediante $\bar{L}$ una clausura algebraica fija de L. Sea p un número primo. Definamos K como el conjunto de las raices en $\bar{L}$ de todos los polinomios

$$X^{q^{p^n}} - X \quad (n \in \mathbf{N}).$$

Entonces K es un cuerpo que contiene a L; y $K|L$ es una extension galoisiana infinita cuyo grupo de Galois es $\mathbf{Z}_p$, el grupo de los números enteros p-ádicos:

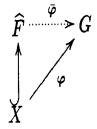
$$\mathbf{Z}_p = \{\sum_{i=1}^{\infty} a_i p^i \mid a_i \in \mathbf{Z}, 0 \leq a_i < p\}.$$

En este artículo sólo vamos a utilizar los grupos profinitos en relación con las conjeturas planteadas en las secciones precedentes. Nuestra herramienta fundamental son los llamados grupos profinitos libres. Estos son los objetos libres en la categoría de grupos profinitos y homomorfismos continuos, que definimos en detalle a continuación. Sea X un espacio topológico compacto, Haussdorff y totalmente discontinuo. Nos referimos a este tipo de espacios con el nombre de **espacios profinitos** pues, como se ve con facilidad, se pueden expresar como límites proyectivos de espacios finitos X_i con la topolgía discreta:

$$X = \varprojlim_{i \in I} X_i$$

Supongamos que X sea un subespacio cerrado de un grupo profinito $\widehat{F}$. Decimos entonces que $\widehat{F}$ es un **grupo profinito libre** sobre X si se satisface

la siguiente propiedad universal. Siempre que $\varphi : X \longrightarrow G$ sea una función continua de X a un grupo profinito G, existe un homomorfismo continuo $\bar{\varphi} : \widehat{F} \longrightarrow G$ que coincide con φ en X



Dado X, no es difícil demostrar que existe un único grupo profinito libre $\widehat{F} = \widehat{F}(X)$ sobre X. La construcción de $\widehat{F}$ se puede hacer de la siguiente manera. Sea $\Phi = \Phi(X)$ el grupo abstracto libre sobre X. (véase la sección 4). Consideremos el conjunto $\mathcal{N}$ de todos los subgrupos normales N of Φ de índice finito y tales que $N \cap X$ sea un subconjunto cerrado de X. Definamos $\widehat{F}$ como el límite proyectivo

$$\widehat{F} = \varprojlim_{N \in \mathcal{N}} \Phi/N$$

Se puede comprobar con poco trabajo que X es homeomorfo con el subespacio

$$\varprojlim_{N \in \mathcal{N}} X/N \cap X$$

de $\widehat{F}$. Se verifica sin dificultad que la propiedad universal se cumple.

Como ejemplo, observemos que el grupo profinito libre sobre el espacio $X = \{1\}$ con un solo punto, es el grupo clásico

$$\widehat{\mathbf{Z}} = \prod_{p \in \mathcal{P}} \mathbf{Z}_p,$$

donde $\mathcal{P}$ es el conjunto de todos los números primos y $\mathbf{Z}_p$ es el grupo de los números p-ádicos.

7. Grafos

Un grafo Γ consiste en un conjunto de **vértices** $V = V(\Gamma)$, un conjunto de **aristas** orientadas $A = A(\Gamma)$ y dos funciones

$$A \underset{d_1}{\overset{d_0}{\rightrightarrows}} V.$$

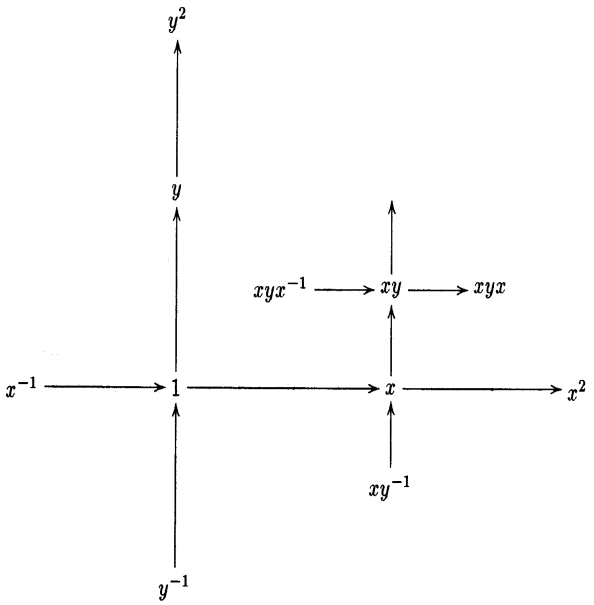
Si $a \in A$, decimos que $d_0(a)$ y $d_1(a)$ son el **origen** y el **terminal** de a. Es conveniente además introducir aristas 'opuestas' a las aristas en A. Si $a \in A$, definimos símbolos $a^1 (= a)$ y a^{-1}. Pongamos

$$A^{-1} = \{a^{-1} \mid a \in A\}.$$

Por definición, $d_i(a^{-1}) = d_{1-i}(a) \quad (a \in A \ ; \ i = 0, 1)$. Para hacer más flexible nuestra notación adoptaremos la siguiente convención: $(a^{-1})^{-1} = a \quad (a \in A)$.

Sean v y w vértices del grafo Γ. Un **camino** $c_{v,w}$ de v a w es simplemente una sucesión finita de aristas $a_1^{\epsilon_1}, \ldots, a_n^{\epsilon_n}$ de forma que $v = d_0(a_1^{\epsilon_1})$, $w = d_n(a_n^{\epsilon_n})$ y $d_1(a_i^{\epsilon_i}) = d_0(a_{i+1}^{\epsilon_{i+1}})$ para todo $i = 1, \ldots, n-1$. La **longitud** de $c_{v,w}$ es n. Se dice que $c_{v,w}$ es un camino **reducido** si $a_i^{\epsilon_i} \neq a_{i+1}^{-\epsilon_{i+1}}$, para todo i. Un camino reducido de v a v se llama un **circuito** si tiene longitud $n \geq 1$. Un grafo Γ es **conexo** si para cualquier par de vértices v y w de Γ, existe un camino $c_{v,w}$. Un **árbol** es un grafo conexo y sin circuitos.

Ejemplo Sea G un grupo y X un subconjunto de G. Definamos un grafo $\Gamma = \Gamma(G, X)$ (el **grafo de Cayley**) de la manera siguiente. Los vértices de Γ son los elementos de G. Una arista es un par (g, x), donde $g \in G$ y $x \in X$. Pongamos $d_0(g, x) = g$ y $d_1(g, x) = gx$. Si, por ejemplo, $G = F$ es un grupo libre sobre el conjunto $X = \{x, y\}$, entonces el grafo de Cayley correspondiente $\Gamma(G, X)$ se puede representar geométricamente así



Es importante observar que el grupo G opera (por la izquierda) de forma natural en el grafo $\Gamma(G, X)$. En general, si un grupo opera por la izquierda en un grafo Γ, denotaremos mediante $G\backslash\Gamma$ su grafo cociente (los vértices y las aristas de $G\backslash\Gamma$ son las órbitas de los vértices y las aristas de Γ bajo la acción de G, respectivamente).

Decimos que un grafo Γ es un **grafo profinito** si $V(\Gamma)$ y $A(\Gamma)$ son espacios topológicos compactos, Hausdorff, totalmente discontinuo, y además las funciones d_0 y d_1 son continuas. Por ejemplo, todo grafo finito es profinito. Si G es un grupo profinito y X es un subespacio cerrado de G, entonces el

grafo de Cayley $\Gamma(G, X)$ es un grafo profinito. En este caso, la acción de G en $\Gamma(G, X)$ es continua.

En el contexto de grafos profinitos es más difícil describir la definición apropiada del concepto de árbol. En vez de dar una definición precisa, que es algo técnica, nos limitaremos a dar un ejemplo (para una definición explícita véase [Ribes-Gildenhuys 78] o [Zalesskii-Melnikov 91]. Sea $\widehat{F} = \widehat{F}(X)$ un grupo profinito sobre un espacio compacto, Hausdorff, totalmente discontinuo X. Construyamos el grafo de Cayley $\Gamma(\widehat{F}, X)$. Entonces $\Gamma(\widehat{F}, X)$ es un grafo profinito; de hecho $\Gamma(\widehat{F}, X)$ es un árbol profinito.

8. Demostración del Teorema 2

Sólo daremos un esquema muy breve de la demostración, indicando las ideas principales. Para simplificar el problema, supongamos que $G = F$ sea de hecho un grupo libre abstracto de rango finito (es decir, con una base finita). Supondremos también que el número n de subgrupos es 2. Por tanto el problema ahora es el siguiente. Sea F un grupo libre abstracto con una base finita X; supongamos que H y K sean subgrupos de F finitamente generados. Tenemos que demostrar que el conjunto HK es cerrado en la topología profinita de F. Recordemos que todo subgrupo de un grupo libre es libre (Teorema de Schreier). Otra reducción del problema se consigue mediante un teorema de M. Hall. Este teorema dice que (puesto que K está finitamente generado), existe un subgrupo U de índice finito en F de manera que $K \leq U$ y toda base del grupo K se puede extender a una base de U. Un sencillo y corto razonamiento permite reducir el problema al caso en el que $F = U$. Podemos pues suponer que $Y = X \cap K$ es una base del grupo libre K.

Denotemos mediante $\widehat{F}$ el grupo profinito libre sobre X. Se sigue de la construcción de $\widehat{F}$ que hemos indicado más arriba, que F se puede identificar con un subgrupo denso de $\widehat{F}$. La topología profinita de F coincide con la topología inducida en F por la topología de $\widehat{F}$. Además, la clausura de K en $\widehat{F}$ es el grupo libre profinito sobre Y. De esta manera obtenemos inclusiones naturales $\Gamma(K, Y) \subseteq \Gamma(F, X) \subset \Gamma(\widehat{F}, X)$.

Si T es un subconjunto de $\widehat{F}$, denotemos por $\bar{T}$ su clausura topológica. Con esta notación el teorema se reduce a demostrar que

$$HK = \overline{HK} \cap F;$$

es decir, hay que demostrar que si $h \in \bar{H}$ y $k \in \bar{K}$ y si $hk \in F$, entonces $hk \in HK$.

Supongamos que $r_1, \ldots, r_s$ sea un conjunto de generadores de H. Consideramos a cada r_i como un vértice de $\Gamma(F, X)$. Puesto que $\Gamma(F, X)$ un árbol, existe un solo camino de longitud mínima $[1, r_i]$ en $\Gamma(F, X)$ del vértice 1 al vértice r_i. Se comprueba entonces que

$$\Delta = \bigcup_{j=1}^{s} \bar{H}[1, r_j]$$

es un subárbol profinito de $\Gamma(\widehat{F}, X)$ y mínimo con respecto a la propiedad de que $\bar{H}$ actua sobre él.

Con algo de trabajo se demuestra que podemos suponer que $k \in [h^{-1}, 1] \subseteq \Delta$. Consideremos el epimorfismo natural de grafos

$$\pi : \Delta \longrightarrow \bar{H}\backslash\Delta.$$

Se sigue de la definición de Δ que $\bar{H}\backslash\Delta$ es un grafo finito. Pongamos $T = \Delta \cap \Gamma(\bar{K}, Y)$. De ésto se deduce que la acción del grupo profinito $\bar{H} \cap \bar{K}$ en T sólo tiene un número finito de órbitas, es decir que

$$(\bar{H} \cap \bar{K})\backslash T$$

es un grafo finito. Mas aún, $(\bar{H} \cap \bar{K})\backslash T$ es isomorfo al grafo $\pi(T)$. Finalmente, un argumento ligeramente delicado utilizando grafos finitos, permite concluir que $hk \in HK$. (Para una demostración mas detallada, veáse [Ribes-Zalesskii 93].)

9. Algoritmos en Grupos Libres

La conjetura 1 planteada en la segunda sección, tiene una generalización interesante y útil para la teoría de autómatas. Sea p un número primo fijo. Denotemos mediante $\mathcal{G}_p$ la variedad de todos los p-grupos finitos.

Conjetura 5 *Si una variedad de monoides finitos $\mathcal{V}$ es decible, también lo es la variedad producto $\mathcal{V} \bowtie \mathcal{G}_p$.*

La respuesta a esta conjetura también es positiva. Pero esa respuesta, además de un resultado análogo al Teorema 2, requiere la existencia de un algoritmo relacionado con los grupos libres. Este algoritmo tiene, quizás, un interés independiente. El resto de esta sección está dedicado a explicar cuál es el problema y cuál es el algoritmo que lo resuelve.

Sea F un grupo libre abstracto. Sea

$$\mathcal{N}_p = \{N \mid N \lhd F,\ |F/N| = p^n,\ n \in \mathbf{N}\}$$

el conjunto de todos los subgrupos normales de F cuyo índice es una potencia de p. Entonces $\mathcal{N}_p$ define en F una topología, que llamamos la **topología pro-p** de F. Tenemos entonces el siguiente resultado,

Teorema 3 *Existe un algoritmo para computar la clausura* $\mathrm{Cl}(H)$ *de cualquier subgrupo finitamente generado H de F, en la topología pro-p de F.*

Conviene entender con precisión el significado de 'computar' en este contexto. Comenzamos con un grupo libre F, que supondremos es de rango finito, con una base $X = \{x_1, \ldots, x_n\}$. Se nos 'da' un subgrupo H finitamente generado de F, es decir, se nos da un conjunto finito $\{h_1, \ldots, h_r\}$ de palabras reducidas en el alfabeto $X \cup X^{-1}$, que generan el subgrupo H. No es obvio

que la clausura $\mathrm{Cl}(H)$ de H en la topología pro-p de F tenga que ser necesariamente un grupo finitamente generado. El teorema afirma que efectivamente $\mathrm{Cl}(H)$ está finitamente generado y además existe un algoritmo que calcula un conjunto finito de generadores de $\mathrm{Cl}(H)$.

La descripción de este algoritmo utiliza dos conceptos combinatorios simples: el grafo de Cayley de un grupo abstracto con respecto a un subconjunto (ver sección sobre grafos) y, por otra parte, el grupo fundamental de un espacio. Los espacios que nos ocupan aquí son grafos y, en este caso, la descripción del grupo fundamental es muy sencilla; recordamos a continuación la definición y sus principales propiedades.

Sea Γ un grafo conexo. Fijemos un vértice $v \in V(\Gamma)$. Sea $\pi(\Gamma, v)$ el conjunto de todos los circuitos $c_{v,v}$ (es decir, los caminos que empiezan y terminan en v). Sea $c_{v,v} = a_1^{\epsilon_1}, \ldots, a_n^{\epsilon_n}$ un camino de v a v. Supongamos que existe un subíndice i tal que $a_i^{\epsilon_i} = a_{i+1}^{-\epsilon_{i+1}}$. Decimos entonces que $c_{v,v}$ y el camino $c'_{v,v} = a_1^{\epsilon_1}, \ldots, a_{i-1}^{\epsilon_{i-1}} a_{i+1}^{\epsilon_{i+1}} a_n^{\epsilon_n}$ son 'elementalmente equivalentes'. En general, decimos que dos caminos son equivalentes si se puede pasar de uno al otro por medio de una serie finita de equivalencias elementales. Definamos una multiplicación de dos circuitos en $\pi(\Gamma, v)$ simplemente por concatenación. Esta multiplicación induce a su vez una multiplicación en el conjunto $\pi_1(\Gamma, v)$ de las clases de equivalencia de los caminos en $\pi(\Gamma, v)$. Es inmediato verificar que, con esta multiplicación, $\pi_1(\Gamma, v)$ es un grupo, llamado el **grupo fundamental** del grafo Γ. Este grupo depende, en principio, del vértice v. Se deduce facilmente de nuestra hipótesis (Γ es conexo), que si w es otro vértice de Γ, entonces los correspondientes grupos fundamentales $\pi_1(\Gamma, v)$ y $\pi_1(\Gamma, w)$ son isomorfos. Por tanto, de ahora en adelante, utilizaremos la notación $\pi_1(\Gamma)$ para referirnos al grupo fundamental de Γ, prescindiendo de toda referencia al vértice v.
Un resultado básico y no difícil de demostrar es el siguiente.

Proposición *Sea Γ un grafo conexo.*

(a) *$\pi_1(\Gamma)$ es un grupo libre.*

(b) *Si Δ es un subgrafo conexo de Γ, entonces $\pi_1(\Delta)$ es un factor libre de $\pi_1(\Gamma)$ (esto significa que toda base de $\pi_1(\Delta)$ se puede extender a una base del grupo $\pi_1(\Gamma)$).*

Algoritmo para calcular la Clausura $\mathrm{Cl}(H)$ de H en la Topología pro-p de F

Sea F un grupo libre abstracto con una base finita dada X. Sea H un subgrupo de F generado por $\{h_1, \ldots, h_r\}$ (cada h_i es una palabra en el alfabeto $X \cup X^{-1}$). Denotemos mediante $\Gamma = \Gamma(F, X)$ el grafo de Cayley de F con respecto a X. Si m es un número natural, $U(m)$ denota la intersección de todos los subgrupos abiertos (en la topología pro-p) de F de índice menor o igual a m y que contengan H.

PRIMER PASO. Construir los (únicos) caminos reducidos c_{1,h_i} en Γ de 1 a h_i $(i = 1, \ldots, r)$. Sea $T = \bigcup_{i=1}^{r} c_{1,h_i}$. Poner $n := p$.
SEGUNDO PASO. Construir $U(m)$ (*existe un algoritmo para encontrar un conjunto de generadores de* $U(m)$). Si $U(m) = F$ (*existe un algoritmo para decidir si estos grupos coinciden*), entonces $F = \mathrm{Cl}(H)$, y el algoritmo termina.
TERCER PASO. Construir el grafo finito cociente $U(m)\backslash\Gamma$. Construir la imagen T_m de T en $U(m)\backslash\Gamma$ utilizando el morfismo natural de grafos $\Gamma \longrightarrow U(m)\backslash\Gamma$.
CUARTO PASO. Construir la imagen de $c_{1,h_i}(m)$ en $U(m)\backslash\Gamma$ del camino c_{1,h_i} $(i = 1, \ldots, r)$. Estas imágenes son circuitos reducidos en T_m puesto que $H \leq U(m)$, y por tanto representan elementos de $\pi_1(T_m)$. Comprobar si existe algún subgrupo abierto de $\pi_1(T_m)$ de índice p que contenga cada uno de los elementos representados por $c_{1,h_i}(m)$ $(i = 1, \ldots, r)$. (*Todos estos procesos se pueden llevar a cabo algorítmicamente.*) Si no existe ninguno, entonces $\mathrm{Cl}(H) = \pi_1(T_m)$ y el algoritmo termina. Si existe alguno, poner $m := pm$ e ir al Segundo Paso.

Teorema 4 *El algoritmo termina después de un número finito de pasos, y su resultado final es* $\mathrm{Cl}(H)$. *En particular,* $\mathrm{Cl}(H)$ *está finitamente generado.*

La demostración de este teorema consiste en un estudio detallado del comportamiento de los grafos T_m y sus correspondientes grupos fundamentales. Para más detalles el lector puede consultar [Ribes-Zalesskii 94] o [Ribes-Zalesskii 00].

10. COMENTARIOS

El libro [Almeida 94] de J. Almeida contiene una buena introducción a la teoría de semigrupos y monoides. Para la teoría de lenguajes véase, por ejemplo, [Eilenberg 74]. Sobre la teoría de grupos que operan sobre grafos abstractos se puede consultar [Serre 80] o [Dicks-Dunwoody 89]. Para grafos profinitos [Gi ldenhuys-Ribes 78], [Zaleskii-Melnikov 89] o el libro de próxima aparición [Ribes-Zalesskii 00].

La primera demostración de la Conjetura 2, obtenida de manera independiente de la que describimos aquí, se debe a C. J. Ash [Ash 91]. Su enfoque y las herramientas que utiliza son puramente combinatorias; su demostración es sin duda muy ingeniosa y difícil.

Mi interés en estas cuestiones se debe al excelente trabajo de J-E. Pin y de Ch. Reuteneauer en [Pin 89] y sobre todo en [Pin-Reutenanuer 91]. Aunque en estos artículos no se exhiben nuevos casos en los que la Conjeturas 1 y 2 tienen respuesta positiva, su aportación, al expresar las conjeturas en términos topológicos, ha sido muy importante. Sin su trabajo es muy poco probable que ni Zalesskii ni yo nos hubiéramos interesado por estas cuestiones.

Los Teoremas 2, 3 y 4 son fruto de una colaboración con Pavel Zalesskii [Ribes-Zalesskii 91], [Ribes-Zalesskii 94]. Los grupos profinitos aparecen históricamente como una herramienta de la teoría de números. Los resultados sobre grupos y grafos profinitos que están en la base de los teoremas del presente artículo tienen dos motivaciones principales. Por una parte, su origen

está en un intento de entender la estructura de los subgrupos de grupos libres, productos libres etc. en la categoría de los grupos profinitos. Por otra, están muy relacionados con la teoría de grupos abstractos que operan sobre árboles debida a Bass y Serre. Por ello es quizás sorprendente que tengan utilidad en cuestiones como las que tratamos en este trabajo.

Tengo noticia de otra demostración del Teorema 2 que utiliza lo que parecen ser métodos completamente distintos de los nuestros. Se debe a B. Herwig y D. Lascar y su enfoque está basado en métodos de la lógica matemática. He oido hablar de la presentación de esta demostración en conferencias y/o reuniones en Alemania, Francia, Inglaterra, Italia, Portugal, ... , pero nunca he visto un manuscrito con la demostración.

Bibliografía

[Almeida 94] Almeida, U.:, "Finite Semigroups and Universal Algebra", *World Scientific,* Singapur (1994).

[Ash 91] Ash, C.J.: "Inevitable graphs: a proof of the type II conjecture and some related decision procedures", *Int. J. Algebra and Computation* **1**(1991) 127–146.

[Dicks-Dunwoody 89] Dicks, W., Dunwoody, M.J.: "Groups Acting on Graphs", *Cambridge Univ. Press, Cambridge*, 1989.

[Eilenberg 74] Eilenber, S.: "Automata, Languages and Machines", *Vol. A, Acad. Press*, Nueva York, 1974.

[Gildenhuys-Ribes 78] Gildenhuys, D., Ribes, L.: "Profinite groups and boolean graphs", *J. Pure Appl. Algebra*, **12** (1978) 21–47.

[Hall 50] Hall, M.: "A topology for free groups and related groups", *Annals of Math.* **52** (1950) 127–139.

[Henckell-Margolis-Pin-Rhodes 91] Henckell, K., Margolis, S.W. Pin, J-E., Rhodes, J.: "Ash's Type II theorem, profinite topology and Malcev products. Part I", *Int. J. Algebra and Computation*, **1** (1991) 411–436 .

[Margolis-Pin 92] Margolis, S.W. Pin, J.E.: "New results on the conjecture of Rhodes and on the topological conjecture", *J. Pure Appl. Algebra*, **80** (1992) 305–313.

[Pin 89] Pin, J.E.: "On a conjecture of Rhodes", *Semigroup Forum*, **39** (1989) 1–15.

[Pin-Reutenauer 91] Pin, J.E., Reutenauer, Ch.: "A conjecture on the Hall topology for the free group", *Bull. London Math. Soc.* **23** (1991) 356–362 .

[Rhodes 90] Rhodes, J.: "Survey of global semigroup theory, in *Lattices, Semigroups and Universal Algebra*", J. Almeida, G. Bordalo y P Dwinger (Eds.), New York, 1990, Plenum, 243-269.

[Ribes-Zalesskii 93] Ribes, L., Zalesskii, P.: "On the profinite topology on a free group", *Bull. London Math. Soc.*, 25 (1993) 37-43.

[Ribes-Zalesskii 94] Ribes, L., Zalesskii, P.: "The pro-p topology of a free group and algorithmic problems in semigroups", *Int. J. Algebra and Computation*, **4** (1994) 359–374.

[Ribes-Zalesskii 00] Ribes, L., Zalesskii, P.: "Profinite Groups", *Springer-Verlag*, Berlín, próxima aparición.

[Serre 80] Serre, J-P.: Springer-Verlag, Berlín, 1980.

[Zalesskii-Melnikov 89] ZALESSKII, P., MEL'NIKOV, O.: "Subgroups of profinite groups acting on trees", *Math USSR Sbornik* **63** (1989) 405–424.

Luis Ribes. School of Mathematics and Statistics
Carleton University. Ottawa, Ont. Canada K1S 5B6
correo electrónico:lribes@math.carleton.ca