Morfismos, Vol. 20, No. 2, 2016, pp. 67–76

Tríadas pitagóricas y semiautómatas

Guillermo Morales-Luna

Noviembre de 2016

Resumen

Se considera la obtención de tríadas pitagóricas mediante las matrices que generan tríadas reducidas. Vistas como elementos de un lenguaje, estas matrices dan origen a semiautómatas que enumeran de manera sistemática a las tríadas. Se discute aquí algunos aspectos procedimentales de dichos semiautómatas, vistos también como gráficas dirigidas.

2010 Mathematics Subject Classification: 11A67, 68Q45, 05A17.
Palabras y expresiones claves: procedimientos de enumeración, tríadas pitagóricas, semiautómatas

1 Introduction

En la década de los 80, Ronald Graham planteó el *problema booleano de tríadas pitagóricas*, a saber: ¿Puede partirse el conjunto de los enteros $\mathbb{Z}$ en dos subconjuntos de manera que ninguna tríada pitagórica quede en alguno de esos conjuntos? En otras palabras, ¿existe una función booleana $f\colon \mathbb{Z} \to \{0,1\}$ tal que para cualesquiera tres enteros $a,b,c \in \mathbb{Z}$ tales que $c \neq 0$ y $a^2 + b^2 = c^2$ se tenga $\{a,b,c\} \cap f^{-1}(0) \neq \emptyset \neq \{a,b,c\} \cap f^{-1}(1)$? O como un tercer planteamiento equivalente: ¿existe una bicoloración de $\mathbb{Z}$ de manera que ninguna tríada pitagórica sea monocromática?

Recientemente se dió una prueba de que la respuesta a este problema es negativa [2]. Lo extraordinario de la demostración presentada es que fueron utilizados grandes recursos computacionales para ella, y, ya completa, ocupa un espacio de 200 terabytes. Los autores de ella [2] pusieron a disposición de todo el mundo una versión ultracomprimida de la prueba para ser descargada, descomprimida y eventualmente revisada a plenitud. A grandes rasgos, en el enfoque presentado, el problema booleano de tríadas pitagóricas se reduce a una colección de instancias del *problema de satisfactibilidad de fórmulas booleanas* (SAT) y se revisa si acaso éstas últimas son satisfactibles o no.

En este contexto, surge como una pregunta natural, la enumeración efectiva y eficiente de las tríadas pitagóricas. Desde tiempos remotos se presentaron varias sucesiones cuyos términos son todos tríadas pitagóricas [5].

Como un mero ejercicio de la Teoría de Autómatas [1, 3, 4], presentamos aquí un semiautómata para enumerar a las tríadas pitagóricas. Estos semiautómatas pueden ser vistos también como gráficas dirigidas y como subsemigrupos de un grupo finitamente generado, el cual a su vez se incluye de manera homomorfa en el semigrupo de palabras sobre el alfabeto consistente de sus generadores

2 Generación de tríadas pitagóricas

Una *tríada pitagórica* es una tripleta ordenada $(a, b, c) \in \mathbb{Z}^2 \times (\mathbb{Z} - \{0\})$ tal que $a^2 + b^2 = c^2$. Denotemos por $\mathcal{T}$ a la colección de tales tríadas. Una tríada $(a, b, c) \in \mathcal{T}$ se dice ser *reducida* si a y b son primos relativos, es decir si $\mathrm{mcd}\,(a, b) = 1$.

Para cualquier tríada pitagórica $\mathbf{a} = (a, b, c) \in \mathcal{T}$, diremos que su *tipo* es

$$\tau(\mathbf{a}) = (a^2 \bmod 8, b^2 \bmod 8, c^2 \bmod 8) \in \mathbb{Z}_8^3.$$

Ya que los residuos cuadrados de $\mathbb{Z}_8$ son sólo $0, 1, 4$ y los tipos provienen de tríadas pitagóricas, los únicos tipos posibles son

$$(0,0,0)\ ,\ (1,0,1)\ ,\ (0,1,1)\ ,\ (4,0,4)\ ,\ (0,4,4). \tag{1}$$

Correspondientemente, las "primeras" tríadas pitagóricas que tienen los tipos éstos son

$$(4,0,4)\ ,\ (1,0,1)\ ,\ (0,1,1)\ ,\ (2,0,2)\ ,\ (0,2,2). \tag{2}$$

Recordemos someramente algunas sucesiones con valores en las tríadas pitagóricas, todas éstas ya clásicas [5].

Es bien sabido que la función

$$U : \mathbb{Z} \to \mathcal{T}\ ,\ m \mapsto U(m) = (2m, m^2 - 1, m^2 + 1),$$

define una sucesión de tríadas pitagóricas. Se tiene

$$\forall m \in \mathbb{Z} : \ \tau(U(m)) = \begin{cases} (0,1,1) & \text{si } m = 0 \bmod 2 \\ (4,0,4) & \text{si } m = 1 \bmod 2 \end{cases} \tag{3}$$

Similarmente, la función

$$V : \mathbb{Z}^2 \to \mathcal{T} \ , \ (u,v) \mapsto V(u,v) = (v^2 - u^2, 2uv, v^2 + u^2),$$

define una sucesión de tríadas pitagóricas. Se tiene

$$\forall (u,v) \in \mathbb{Z}^2 : \ \tau(V(u,v)) = \begin{cases} (0,0,0) & \text{si } (u,v) = (0,0) \bmod 2 \\ (1,0,1) & \text{si } (u,v) = (0,1) \bmod 2 \\ (1,0,1) & \text{si } (u,v) = (1,0) \bmod 2 \\ (4,0,4) & \text{si } (u,v) = (1,1) \bmod 2 \end{cases} \tag{4}$$

Una tercera manera muy popular para generar tríadas pitagóricas es la siguiente.

Inicialmente, para una pareja de enteros $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ defínase una sucesión $F(a,b) = (f_n(a,b))_{n\in\mathbb{N}}$ al estilo de la de Fibonacci:

$$f_0(a,b) = a \ , \ f_1(a,b) = b \ , \ \forall n \geq 2 : \ f_n(a,b) = f_{n-1}(a,b) + f_{n-2}(a,b).$$

Así, por ejemplo, $F(0,1)$ es la sucesión convencional de Fibonacci. Al definir

$$\begin{aligned} \forall n \geq 0 : \ t_n(a,b) = (\ & f_n(a,b) f_{n+3}(a,b) \, , \\ & 2 f_{n+1}(a,b) f_{n+2}(a,b) \, , \\ & f_{n+1}(a,b)^2 + f_{n+2}(a,b)^2 \ ), \end{aligned}$$

se tiene que $t_n(a,b)$ es una tríada pitagórica. Mediante la utilización de cualquier programa de cálculo simbólico, se puede formular la siguiente:

Observación 2.1. La sucesión de tipos $(\tau(t_n(a,b)))_{n\in\mathbb{N}}$ es periódica con un período $T(a,b)$ de longitud 3. De hecho, al considerar los tipos

$$\mathbf{c} = (0,0,0) \ , \ \mathbf{u} = (1,0,1) \ , \ \mathbf{v} = (4,0,4)$$

entonces

$$\forall (a,b) \in \mathbb{Z}^2 : \ T(a,b) = \begin{cases} \mathbf{ccc} & \text{si } (a,b) = (0,0) \bmod 2 \\ \mathbf{vuu} & \text{si } (a,b) = (0,1) \bmod 2 \\ \mathbf{uvu} & \text{si } (a,b) = (1,0) \bmod 2 \\ \mathbf{uuv} & \text{si } (a,b) = (1,1) \bmod 2 \end{cases} \tag{5}$$

(Una demostración completa de esta observación podría proceder por inducción y aquí la omitimos. Tal demostración, para el primer caso en (5) es inmediata. Los otros tres se seguirían de uno cualquiera de ellos por mera simetría.)

Así pues, las relaciones (3)–(5) caracterizan por completo los tipos de las tríadas pitagóricas generadas mediante los métodos clásicos presentados.

3 Semiautómata de operadores

3.1 Recordatorio de nociones básicas

Con el fin de aclarar notación y terminología, recordamos nociones básicas [1, 3, 4].

Un *semiautómata* es una estructura (Q, A, t) donde Q es un conjunto (no-vacío) de *estados*, A es uno finito de *símbolos* (es decir, es un *alfabeto*) y $t : Q \times A \to Q$ es una función de *transición*. Una relación $q = t(p, a)$ se interpreta como que "si el semiautómata está actualmente en el estado p y arriba el símbolo a entonces se pasa al estado q", o en aras de la síntesis: "de p con a se pasa a q". Mediante A^* denotamos al conjunto de *palabras* (es decir, secuencias de longitud finita) sobre A. La *palabra vacía* `nil` es la unidad del semigrupo A^* con la operación de concatenación. La función de transición puede ampliarse a $t^* : Q \times A^* \to Q$ de manera recursiva: $\forall p \in Q$:

$$[t^*(p, \texttt{nil}) = p \;\; \& \;\; \forall \alpha \in A^*,\, a \in A: \; t^*(p, \alpha a) = t(t^*(p, \alpha), a)]\,.$$

Así pues, $t^*(p, \alpha)$ es el estado al que se llega cuando se aplica la palabra α partiendo de p. Un estado $q \in Q$ es *alcanzable* desde un estado $p \in Q$ si existe una palabra $\alpha \in A^*$ tal que $q = t^*(p, \alpha)$. El semiautómata es *conexo* si para cualesquiera dos estados en él se tiene que existe un estado, que puede ser uno de ellos, tal que desde este último se alcanzan aquellos dos.

Un *autómata* es un semiautómata finito (es decir, su conjunto de estados es finito) en el que se ha distinguido un estado *inicial* y un conjunto de estados *finales*, o sea, es una estructura $\mathrm{Aut} = (Q, A, t, q, F)$, donde (Q, A, t) es un semiautómata finito, $q_0 \in Q$ es el estado inicial y $F \subset Q$ es el conjunto de estados finales. El *lenguaje reconocido* por el autómata consta de las palabras que hacen pasar el estado inicial a uno cualquiera de los finales: $L(\mathrm{Aut}) = \{\alpha \in A^* | \; t^*(p, \alpha) \in F\}$.

Por otro lado, una *gráfica dirigida* es una estructura (N, A) donde N es un conjunto (no-vacío) de *nodos* y $A \subset N \times N$ es un conjunto de *aristas*. Se dice que una arista $uv = (u, v) \in A$ *sale* de u y *entra* a v. El *grado interior* de un nodo es el número de aristas que salen de él y el *grado exterior* es el número de aristas que entran a él. La gráfica está *etiquetada (por aristas)*, mediante un conjunto E, si se da una función $e : A \to E$ que a cada arista uv le asocia una *etiqueta* $e(uv) \in E$.

A un semiautómata $S = (Q, A, t)$ se le asocia la gráfica dirigida etiquetada G_S siguiente:

Nodos Cada estado $q \in Q$ es un nodo.

Aristas Para cualesquiera $p, q \in Q$ y $a \in A$ si acaso $q = t(p, a)$ entonces la pareja ordenada pq se considera una arista con etiqueta a (en este caso, puede haber aristas múltiples: una arista uv se repite tantas veces como haya símbolos a tales que $v = t(u, a)$).

Varias nociones de semiautomátas (tales como alcanzabilidad o conexidad) se reducen a correspondientes nociones de las respectivas gráficas dirigidas etiquetadas, y viceversa.

3.2 Semiautómata de estudio

Considérese las siguientes tres matrices

$$A_0 = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix} ,\quad A_1 = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix} ,\quad A_2 = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}. \tag{6}$$

Se tiene pues que si

$$I_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \;,\; I_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \;,\; I_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

entonces

$$A_1 = A_0 I_1 \;,\; A_2 = A_0 I_2.$$

Las inversas de las matrices A_i son

$$A_0^{-1} = \begin{bmatrix} 1 & 2 & -2 \\ 2 & 1 & -2 \\ -2 & -2 & 3 \end{bmatrix} \quad ,$$
$$A_1^{-1} = \begin{bmatrix} -1 & -2 & 2 \\ 2 & 1 & -2 \\ -2 & -2 & 3 \end{bmatrix} \quad , \tag{7}$$
$$A_2^{-1} = \begin{bmatrix} 1 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{bmatrix},$$

y valen las identidades

$$A_1^{-1} = I_1 A_0^{-1} \quad , \quad A_2^{-1} = I_2 A_0^{-1}.$$

Sea

$$\mathcal{A} = \{A_0, A_1, A_2, A_0^{-1}, A_1^{-1}, A_2^{-1}\} \subset \mathrm{GL}(\mathbb{R}^3) \tag{8}$$

el conjunto de matrices definidas en (6) y (7), cada una de las cuales determina una transformación lineal invertible en $\mathbb{R}^3$.

Cálculos directos muestran que valen las siguientes observaciones:

Observación 3.1. Para cada $A \in \mathcal{A}$ si $\mathbf{a} = [a\ b\ c]^T$ es una tríada pitagórica, entonces $A\mathbf{a}$ también es una tríada pitagórica.

Observación 3.2. Para cada $A \in \mathcal{A}$ si $\mathbf{a} = [a\ b\ c]^T$ es una tríada pitagórica con tipo $\tau(\mathbf{a})$, entonces $A\mathbf{a}$ posee el mismo tipo, $\tau(A\mathbf{a}) = \tau(\mathbf{a})$.

Observación 3.3. Si $i \neq j$ entonces $\left(A_j^{-1} A_i\right)^2 = Id_3$.

Sea $\langle \mathcal{A} \rangle < \mathrm{GL}(\mathbb{R}^3)$ el subgrupo generado por $\mathcal{A}$ en el grupo general lineal $\mathrm{GL}(\mathbb{R}^3)$. Una presentación de este subgrupo es pues:

Generadores $A_0, A_1, A_2, A_0^{-1}, A_1^{-1}, A_2^{-1}$.

Relatores [1] $\forall i :\quad A_i^{-1} A_i\ ,\quad A_i A_i^{-1}$
$\forall i \neq j :\quad A_j^{-1} A_i A_j^{-1} A_i\ ,\quad A_j A_i^{-1} A_j A_i^{-1}$

[1]Es convencional decir que una *relación* en un grupo es de la forma $\sigma = \tau$ donde σ y τ son palabras en un conjunto A de generadores, una relación se identifica entonces con un elemento de $A^* \times A^*$. Claramente, $\sigma = \tau$ es una relación si y sólo si la palabra $\sigma^{-1}\tau \in A^*$ coincide con la unidad del grupo. En tal caso, forzamos el lenguaje y decimos que $\sigma^{-1}\tau$ es un *relator*.

Naturalmente, todo elemento $g \in \langle\mathcal{A}\rangle$ se representa por alguna palabra $\sigma \in \mathcal{A}^*$.

Observación 3.4. A las palabras en $\mathcal{A}^*$ las escribimos, como es usual, de izquierda a derecha, mas en su aspecto semántico, como elementos del grupo $\mathrm{GL}(\mathbb{R}^3)$, actúan en ese orden, que es el reverso a la notación común en Algebra Lineal. Así, por ejemplo, un bigrama AB ha de interpretarse como la premultiplicación de la matriz A por la matriz B.

Se tiene que el subgrupo $\langle\mathcal{A}\rangle$ admite *formas normales.*

Observación 3.5 (Formas normales)**.** Todo elemento $g \in \langle\mathcal{A}\rangle$ se representa de manera única por una palabra $\Sigma(g) \in \mathcal{A}^*$ tal que:

- $\Sigma(g)$ es mínimal, en el orden lexicográfico de $\mathcal{A}^*$ determinado por el orden de $\mathcal{A}$ presentado en la ecuación (8), entre todas las palabras que representen a g,
- ninguna partícula de la forma AA^{-1}, con $A \in \mathcal{A}$, ocurre en $\Sigma(g)$ y
- si alguna partícula de la forma $A_iA_j^{-1}$ ocurre en $\Sigma(g)$, entonces necesariamente $i < j$.

Una demostración de esta observación consiste en un procedimiento para derivar la forma normal de una palabra a partir de esa palabra. A grandes rasgos, éste es:

> *Dada la palabra inicial, de izquierda a derecha elimínese todo bigrama de la forma CC^{-1}, cada vez que se tenga $A_iA_j^{-1}$ con $i > j$, remplácese por $A_jA_i^{-1}$ y reiníciese el proceso.*

La palabra vacía `nil` está en forma normal, las 6 mónadas, $C \in \mathcal{A}$, están en forma normal y lo están también los $30 = 6^2 - 6 = 6(6-1)$ bigramas en $\mathcal{A}$ que no son de la forma CC^{-1}, con $C \in \mathcal{A}$.

Sea $\mathcal{F} \subset \mathcal{A}^*$ el lenguaje consistente de formas normales de acuerdo con la observación previa: $\mathcal{F} = \{\Sigma(g)|\ g \in \langle\mathcal{A}\rangle\}$. Entonces $\mathcal{F}$ puede ser dotado de una estructura de semiautómata mediante la función de transición

$$t : \mathcal{F} \times \mathcal{A} \to \mathcal{F}\ ,\ t : (v, C) \mapsto t(v, C) = \Sigma(v \cdot C),$$

donde $\cdot$ denota la mera concatenación de símbolos. Evidentemente, $\mathcal{F}$ es un semiautómata infinito y, de hecho, las transiciones se calculan como concatenaciones de acuerdo a la siguiente:

Regla de dos últimos símbolos. Si $\upsilon = \upsilon_0 AB \in \mathcal{F}$, con $\upsilon_0 \in \mathcal{F}$, $AB \in \{A_i A_j^{-1}, A_i^{-1} A_j\}$, $i \neq j$, entonces para cada $C \in \mathcal{A}$,

$$t(\upsilon, C) = \begin{cases} \upsilon_0 A & \text{si } C = B^{-1} \\ \upsilon_0 B^{-1} & \text{si } C = A \\ \upsilon_0 ABC & \text{si } C \notin \{A, B^{-1}\} \end{cases}$$

Vale, de manera inmediata:

$$\forall \upsilon_0, \upsilon_1 \in \mathcal{F}\,,\ C \in \mathcal{A}\ \left[\upsilon_1 = t(\upsilon_0, C) \iff \upsilon_0 = t(\upsilon_1, C^{-1})\right]. \tag{9}$$

Con esta construcción, $\mathcal{F}$ adquiere también una estructura de *gráfica dirigida*:

Nodos. Las palabras $\upsilon \in \mathcal{F}$ en forma normal.

Aristas. Si $\upsilon_1 = t(\upsilon_0, C)$ entonces la pareja ordenada (υ_0, υ_1) es una arista, y se le etiqueta con el símbolo C.

Por tanto, de acuerdo con (9), se tiene una arista, etiquetada con el símbolo C, de una palabra υ_0 a otra υ_1 cuando y sólo cuando se tenga la arista inversa de υ_1 a υ_0, etiquetada con C^{-1}.

Observación 3.6. Todo nodo $\upsilon \in \mathcal{F}$ representa un único elemento, $s(\upsilon) \in \langle \mathcal{A} \rangle$, en el grupo $\langle \mathcal{A} \rangle < \mathrm{GL}(3)$.

Observación 3.7. Todo nodo en $\mathcal{F}$ tiene como grados interior y exterior al número 6.

Observación 3.8. Todo nodo en el semiautómata $\mathcal{F}$ es alcanzable desde el nodo `nil`, y se tiene, evidentemente, $\forall \upsilon \in \mathcal{F} :\ \upsilon = t^*(\mathtt{nil}, \upsilon)$. En otras palabras, la gráfica $\mathcal{F}$ es conexa.

Definimos de manera recursiva la operación *revirtiendo por inversos* $\mathrm{revi} : \mathcal{A}^* \to \mathcal{A}^*$ como sigue:

$$\mathrm{revi}\,(\mathtt{nil}) = \mathtt{nil}\ \&\ \left[\forall \sigma \in \mathcal{A}^*, C \in \mathcal{A} :\ \mathrm{revi}\,(\sigma C) = C^{-1}\mathrm{revi}\,(\sigma)\right].$$

Para cada $\upsilon_0 \in \mathcal{F}$, sea $\mathcal{F}(\upsilon_0)$ el (casi-)autómata cuyo semiautómata es $\mathcal{F}$ y cuyo *estado inicial* es el nodo υ_0. Lo seguiremos llamando semiautómata.

Proposición 3.9. *Para cualesquiera dos palabras $\upsilon_0, \upsilon_1 \in \mathcal{F}$, los semiautómatas $\mathcal{F}(\upsilon_0)$ y $\mathcal{F}(\upsilon_1)$ son conexos, en el sentido de que para cualquier nodo $\upsilon \in \mathcal{F}$ existen sendas palabras $\sigma_0, \sigma_1 \in \mathcal{F}$ tales que*

$$t^*(\upsilon_0, \sigma_0) = \upsilon = t^*(\upsilon_1, \sigma_1).$$

En efecto, en $\mathcal{F}(\upsilon_0)$ se tiene que para todo nodo $\upsilon \in \mathcal{F}$ la palabra en forma normal que conecta a υ_0 con υ es $\sigma_0 = \Sigma(\mathrm{revi}\,(\upsilon_0) \cdot \upsilon)$. $\square$

Cada palabra $\upsilon \in \mathcal{F}$ determina una transformación lineal $T_\upsilon \in \mathrm{GL}(3)$ y ésta es tal que si $\mathbf{a} = [a\,b\,c] \in (\mathbb{Z}-\{0\})^3$ es una tríada pitagórica, entonces $T_\upsilon\mathbf{a}$ también lo es, y, de acuerdo con la Observación 3.2, ésta ha de ser del mismo tipo que $\mathbf{a}$.

Sea $\mathcal{T} \subset (\mathbb{Z}-\{0\})^3$ la colección de tríadas pitagóricas. $\mathcal{T}$ puede ser dotado de una estructura natural de semiautómata sobre el alfabeto $\mathcal{A}$ mediante la función de transición

$$t_{\mathcal{T}} : \mathcal{T} \times \mathcal{A} \to \mathcal{T}\ ,\ (\mathbf{a}, C) \mapsto t_{\mathcal{T}}(\mathbf{a}, C) = C\mathbf{a}.$$

También adquiere una estructura de gráfica dirigida: los nodos son las tríadas pitagóricas y, toda vez que $\mathbf{b} = C\mathbf{a}$, entonces se tiende una arista de $\mathbf{a}$ hacia $\mathbf{b}$ con etiqueta C.

Debido a la Observación 3.2 esta última gráfica no es conexa y, de hecho, cada componente conexa está asociada al tipo de las tríadas en ella. Ya que los tipos son 5, y están enumerados en la expresión (1), visto como gráfica dirigida, $\mathcal{T}$ tiene exactamente 5 componentes conexas, cada una de las cuales queda determinada por su correspondiente primera tríada pitagórica, según (2). En efecto, al considerar una clase de equivalencia, se puede ver que posee una única tríada, que como vector en $\mathbb{R}^3$ es de mínima norma euclidiana, y ésta ha de ser una de las enlistadas en (2). Enumeremos a las clases de equivalencia como $\mathcal{T}_0$, $\mathcal{T}_1$, $\mathcal{T}_2$, $\mathcal{T}_3$ y $\mathcal{T}_4$, con correspondientes tríadas primeras $\mathbf{a}_0$, $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$ y $\mathbf{a}_4$, según (2).

Cada $\mathcal{T}_i$ es a su vez un semiautómata (con la misma tal estructura de $\mathcal{T}$) y en él se puede considerar a la tríada $\mathbf{a}_i$ como su estado inicial. Entonces $h_i : \mathcal{F} \to \mathcal{T}_i$, $\upsilon \mapsto h(\upsilon) = \mathbf{a}_i\upsilon$, determina un homomorfismo de semiautómatas: $h(\upsilon_0\upsilon_1) = h(\upsilon_0)\upsilon_1$ para cualesquiera dos palabras $\upsilon_0, \upsilon_1 \in \mathcal{F}$. No es un isomorfismo porque no es inyectiva: hay operadores distintos que pueden llevar hacia un mismo estado a dos estados distintos.

Con técnicas convencionales de autómatas finitos [1, 4], dadas dos tríadas pitagóricas $\mathbf{a}$, $\mathbf{b}$ se puede describir a todo el lenguaje de transformaciones en $\mathcal{F}$ que convierten $\mathbf{a}$ en $\mathbf{b}$ como una expresión regular en el alfabeto $\mathcal{A}$.

Finalmente, definamos en $\mathcal{T}$ la relación siguiente:

$$\mathbf{a} \sim \mathbf{b}\ \Leftrightarrow\ \exists \upsilon \in \mathcal{F} :\ \mathbf{b} = T_\upsilon\mathbf{a}.$$

Se tiene que ésta es una relación de equivalencia y por tanto $\mathcal{T}$ se parte como la unión disjunta de las clases de equivalencia resultantes. Estas son 5 y son exactamente $\mathcal{T}_0$, $\mathcal{T}_1$, $\mathcal{T}_2$, $\mathcal{T}_3$ y $\mathcal{T}_4$. De aquí resulta que al conmutar las dos primeras componentes en una tríada se sale de la correspondiente componente conexa, siempre según (2).

Observación 3.10. Si $(a,b,c) \in \mathcal{T}$ entonces $(b,a,c) \in \mathcal{T}$ y $(a,b,c) \not\sim (b,a,c)$.

Para concluir con esta presentación, formulamos la siguiente:

Observación 3.11. Siguiendo una enumeración de $\mathcal{F}$ se enumera efectivamente cada componente conexa $\mathcal{T}_i$ y dado que éstas son sólo 5, se enumera efectivamente todo el conjunto $\mathcal{T}$.

En resumen, por lo aquí visto resulta como conclusión final:

Proposición 3.12. *Toda tríada pitagórica se puede escribir como un producto de matrices en $\mathcal{A}$ aplicado a alguna de las cinco tríadas pitagóricas en (2).*

Guillermo Morales-Luna
Departamento de Computación
Cinvestav-IPN
Av. I. P. N. 2508,
Ciudad de México, 07300, México
gmorales@cs.cinvestav.mx

Referencias

[1] Ginsburg S., *Algebraic and automata-theoretic properties of formal languages.* Elsevier Science Inc. New York, NY, USA, 1975.

[2] Heule M. J. H., Kullmann O., y Marek V. W., Solving and verifying the boolean Pythagorean triples problem via cube-and-conquer. *CoRR*, abs/1605.00723, 2016.

[3] Holcombe M., *Algebraic Automata Theory.* Cambridge University Press, 1982. Cambridge Books Online.

[4] Sakarovitch J., *Elements of Automata Theory.* Cambridge University Press, New York, NY, USA, 2009.

[5] Weisstein E. W., Pythagorean triple. From MathWorld —A Wolfram Web Resource. Web page available from the address `http://mathworld.wolfram.com/PythagoreanTriple.html`. Visited on 02/06/16.