Ecuaciones Diofantinas Determinantales.

Carlos E. Valencia O.
Departamento de Matemáticas, Cinvestav-IPN

Ciudad de México, 24 de Julio del 2023.

Un punto de contacto entre tres areas de las matemática:

1. Algebra lineal.
2. Ecuaciones Diofantinas.
3. Combinatoria.

Bosquejo

Un punto de contacto entre tres areas de las matemática:

1. Algebra Lineal
   - Eigenvalores-Eigenvectores.
   - El radio espectral.
   - M-matrices.
   - M-matrices casi no-singulares.
2. Ecuaciones Diofantinas
   - El décimo problema de Hilbert.
   - La matriz Laplaciana.
   - Que es una Estructura Aritmética?
3. La combinatoria de las estructuras aritméticas del camino.
   - Caracterización usando la subdivisión de aristas.
   - Estructuras aritméticas y triangulaciones del polígono.
4. El algoritmo ilustrado

Eigenvalores-Eigenvectores.

Empecemos con una de las primeras cosas que nos enseñan en la licenciatura y con la que todos estamos familiarizados.

Sea M una matrix cuadrada de tamaño n, con entradas en un campo (digamos los reales $\mathbb{R}$ o los complejos $\mathbb{C}$).

Definición

Un escalar λ, es un eigenvalor de M, si existe un vector $\mathbf{r}$

$$M\mathbf{r} = \lambda\mathbf{r}.$$

Esto es, $(\lambda, \mathbf{r})$ es una pareja eigenvalor-eigenvector si y sólo si

$$(\lambda I_n - M)\mathbf{r} = \mathbf{0}.$$

El espectro de M.

Definición

El espectro de M es la sucesión $\Lambda_M = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n)$ de eigenvalores de M.

Sabemos que Λ_M es el conjunto de soluciones del polinomio

$$p_M(t) = \det(tI_n - M) \in \mathbb{C}[t].$$

El espectro de una matriz es muy importante y ha sido muy estudiado.

Definición

Las raices de $p_M(t)$ pueden estar repetidas y al número de veces que una raiz aparece se le llama su multiplicidad algebraica.

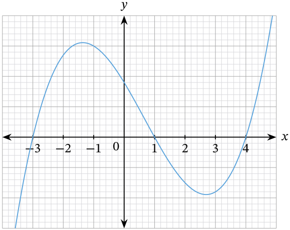
Por lo general no prestamos mucha atención a los eigenvectores.

Radio espectral.

Definición

El radio espectral $\rho(M)$ de M es su eigenvalor maximo λ_1.

$$p_M(t) = (t-4)(t-1)(t+3) \Rightarrow \Lambda_M = \{-3, 1, 4\} y \rho(M) = 4.$$



$$\begin{aligned} p_M(t+4) &= ((t+4)-4)((t+4)-1)((t+4)+3) \\ &= t(t+3)(t+7) = t^3 + 10t^2 + 21t \end{aligned}$$

$$\begin{aligned} p_M(-(t+3)) &= ((-t-3)-4)((-t-3)-1)((-t-3)+3) \\ &= (-t-7)(-t-4)(-t) = -(t^3 + 10t^2 + 21t) \end{aligned}$$

M-matrices.

Una Z-matriz es una matriz tal que $M_{i,j} \leq 0 \ \forall \ 1 \leq i \neq j \leq n$.

Definición

Una Z-matriz A es una M-matriz si existe una matriz no negativa N y $\alpha \geq |\rho(N)|$ tal que

$$M = \alpha I_n - N.$$

Teorema

Una Z-matriz A es una M-matriz si y sólo si todos sus menores principales son no-negativos.

M-matrices casi no-singulares.

Definición

Una matriz es M-matrix casi no-singular si es una Z-matrix, todos sus menores principales propios son positivos y su determinante es no-negativo.

Teorema

Si M es una matriz no-negativa, entonces M es una M-matriz casi non-singular con $\det(M) = 0$ si y soló si M es irreducible y existe $\mathbf{r} > \mathbf{0}$ tal que $M\mathbf{r}^t = \mathbf{0}^t$.

Cuándo una Z-matriz es una M-matriz?

Sea M una Z-matriz real y

$$f_M(\mathbf{x}) = \det(M + \operatorname{diag}(x_1, \ldots, x_n)) \in \mathbb{R}[x_1, \ldots, x_n].$$

Entonces M es una (no-singular M-matriz) M-matrix si y soló si los coeficientes del polinomio f_M son nonegativos (positivos).

Ademas, M es una M-matriz casi no-singular si y soló si todos los coeficientes, excepto tal vez el termino independiente del polinomio f_M, son positivos.

Cuándo una Z-matriz es una M-matriz?

Por ejemplo si

$$M = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & -1 & 2 \end{pmatrix},$$

entonces $f_M(\mathbf{x}) = x_1x_2x_3 + 2x_1x_2 + x_1x_3 + x_2x_3 + x_1 + 2x_2 + x_3$. Luego, M es una M-matriz casi no-singular, pero no no-singular.

Ecuaciones Diofantinas

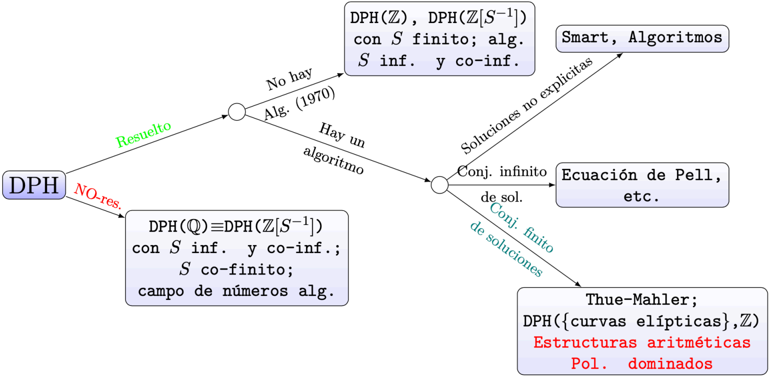
El décimo problema de Hilbert.

El décimo problema de Hilbert (DPH):

> *Dada una ecuación Diofantina cualquiera, existe un algoritmo que determine si está tiene o no solución?*

En 1970 Matiyasevich demostro que en general tal algoritmo NO existe.

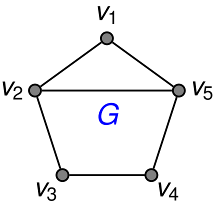
El siguiente diagrama esboza el trabajo hecho.



*The Algorithmic Resolution of Diophantine Equations

La matriz Laplaciana.

Sea el negativo de la matriz de adyacencia de una gráfica $G = (V, E)$.

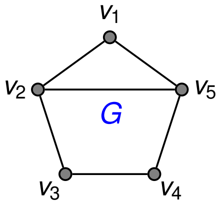


$$-A(G) = \begin{bmatrix} 0 & -1 & 0 & 0 & -1 \\ -1 & 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & -1 \\ -1 & -1 & 0 & -1 & 0 \end{bmatrix}$$

Esta es una matriz entera matrix, con sus entradas diagonales igual a cero y entradas non-positivas fuera de la diagonal.

La matriz Laplaciana.

Si ponemos el grado de cada vértice en su correspondiente entrada diagonal obtenemos la matriz Laplaciana de G.

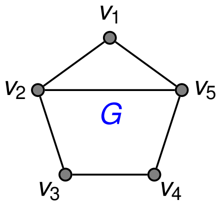


$$L(G) = \begin{bmatrix} 2 & -1 & 0 & 0 & -1 \\ -1 & 3 & -1 & 0 & -1 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & -1 & 0 & -1 & 3 \end{bmatrix}$$

Es singular de rango $n - 1$.

La matriz Laplaciana.

Si ponemos el grado de cada vértice en su correspondiente entrada diagonal obtenemos la matriz Laplaciana de G.



$$L(G) = \begin{bmatrix} 2 & -1 & 0 & 0 & -1 \\ -1 & 3 & -1 & 0 & -1 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & -1 & 0 & -1 & 3 \end{bmatrix}$$

Que mas podemos poner en la diagonal de tal manera que sea similar a la matriz Laplaciana?

Estructuras aritméticas de una gráfica.

Las estructuras aritméticas de una gráfica generalizan la matriz Laplaciana de una gráfica.

Definition

Dada una gráfica conexa $G=(V,E)$, una *estructura aritmética* de G es un par $(\mathbf{d},\mathbf{r})\in\mathbb{N}_+^V\times\mathbb{N}_+^V$ tal que $\gcd(\mathbf{r}_v\mid v\in V)=1$ y

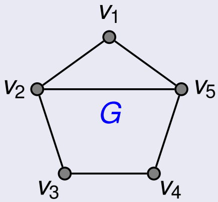
$$L(G,\mathbf{d})\mathbf{r}^t=\mathbf{0}^t,$$

donde $L(G,\mathbf{d})=\operatorname{diag}(\mathbf{d})-A(G)$ es llamada una matriz *pseudo-Laplaciana*.

Un ejemplo no-canonico.

Considere G con $\mathbf{d} = (4, 2, 5, 1, 3)$ y $\mathbf{r} = (1, 2, 1, 3, 2)$.

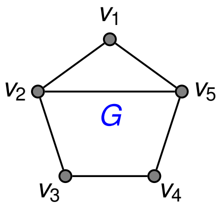
Ejemplo



$$L(G, \mathbf{d})\mathbf{r} = \begin{bmatrix} 4 & -1 & 0 & 0 & -1 \\ -1 & 2 & -1 & 0 & -1 \\ 0 & -1 & 5 & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ -1 & -1 & 0 & -1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 1 \\ 3 \\ 2 \end{bmatrix} = \mathbf{0}.$$

La matriz Laplaciana generalizada.

Si ponemos una variable de cada entrada diagonal obtenemos la matriz Laplaciana generalizada de G.



$$L(G) = \begin{bmatrix} x_1 & -1 & 0 & 0 & -1 \\ -1 & x_2 & -1 & 0 & -1 \\ 0 & -1 & x_3 & -1 & 0 \\ 0 & 0 & -1 & x_4 & -1 \\ -1 & -1 & 0 & -1 & x_5 \end{bmatrix}$$

Entonces una estructura aritmética es una solución de la ecuación Diofantina

$$\det(L(G, X)) = 0.$$

No toda solucion es una estructura aritmética

Todo $\mathbf{d}$ es una solución de la ecuación Diofantina $\mathrm{det}(L(G, X))$. Sin embargo, el converso no es cierto. Sea P_5, $\mathbf{d} = (1, 1, *, 1, 1)$ y $\mathbf{r} = (1, 1, 0, -1, -1)$.

$$L(G, \mathbf{d})\mathbf{r} = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ -1 & 1 & -1 & 0 & 0 \\ 0 & -1 & * & -1 & 0 \\ 0 & 0 & -1 & 1 & -1 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ -1 \\ -1 \end{bmatrix} = \mathbf{0}.$$

El par $(\mathbf{d}, \mathbf{r})$ no es una estructura aritmética. Sin embargo $\mathbf{d}$ es una solución de la ecuación Diofantina asociada a G.

El decimo problema de Hilbert.

Existe un algoritmo que encuentre todas las estructuras aritméticas?

Existe un algoritmo que encuentre todas las soluciones de una ecuación Diofantina determinantal?

M-matrices casi no-singulares y estructuras aritméticas de matrices.

El concepto de estructura aritmética se puede generalizar en el ambito de M-matrices.

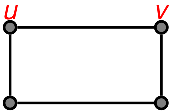
El concepto de M-matriz entera casi no-singular es equivalente al concepto de estructura aritmética.

Las soluciones de una ecuación Diofantina determinantal generalizan el concepto de eigenvalor-eigenvector.

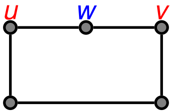
La combinatoria de las estructuras aritméticas del camino.

La subdivisión de una arista.

Dada una arista $e = uv$ de una gráfica G, la subdivisión de e en G es la gráfica $\widetilde{G}$ obtenida por remplazar la arista uv con el camino uwv donde w es un nuevo vértice.



$\Longrightarrow$



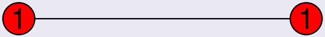
La complejidad de una estructura aritmética de una gráfica puede ser manejable para la subdivisión de una arista.

El **r** vector de una subdivisión de una arista.

El camino con n vértices P_n puede ser obtenido a partir de una arista por sucesivas subdivisiones.

Ejemplo

Sea P_5 el camino con vértices etiquetados por $1, 2, 3, 4, 5$. Empecemos con la estructura aritmética canonica $\mathbf{d}_0 = (1, 1)$ de P_2

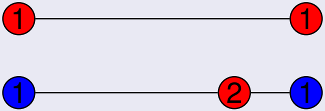


El r vector de una subdivisión de una arista.

El camino con n vértices P_n puede ser obtenido a partir de una arista por sucesivas subdivisiones.

Ejemplo

Sea P_5 el camino con vértices etiquetados por $1, 2, 3, 4, 5$. Empecemos con la estructura aritmética canonica $\mathbf{d}_0 = (1, 1)$ de P_2

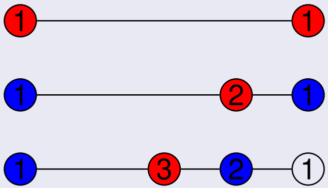


El **r** vector de una subdivisión de una arista.

El camino con n vértices P_n puede ser obtenido a partir de una arista por sucesivas subdivisiones.

Ejemplo

Sea P_5 el camino con vértices etiquetados por $1, 2, 3, 4, 5$. Empecemos con la estructura aritmética canonica $\mathbf{d}_0 = (1, 1)$ de P_2

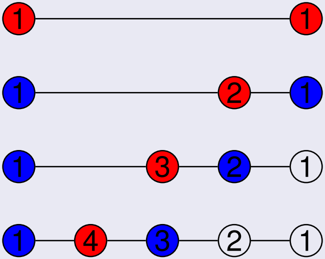


El **r** vector de una subdivisión de una arista.

El camino con n vértices P_n puede ser obtenido a partir de una arista por sucesivas subdivisiones.

Ejemplo

Sea P_5 el camino con vértices etiquetados por $1, 2, 3, 4, 5$. Empecemos con la estructura aritmética canonica $\mathbf{d}_0 = (1, 1)$ de P_2



Estructuras aritméticas del camino.

Teorema

Si $(\mathbf{d}, \mathbf{r})$ *es una estructuras aritmética de* P_n *para* $n \geq 3$ *y* $\mathbf{d} \neq (1, 2, \ldots, 2, 1)$, *entonces existe un vértice no terminal* v *de* P_n *tal que*

$$\mathbf{d}_v = 1 \textit{ and } \mathbf{d}_u > 1 \textit{ for all } u \in N_{P_n}(v).$$

Más aun, toda estructura aritmética $(\mathbf{d}, \mathbf{r})$ *of* P_n *diferente de la canonica puede ser obtenida a partir de una estructuras aritmética de* P_{n-1} *por subdividir una arista.*

$n=2$	$n=3$	$n=4$	$n=5$	
$(1,1)$	$(1,2,1)$ 1	$(1,3,2,1)$	$(1,4,3,2,1)$	
1	$(1,1,1)$ 1	$(1,2,3,1)$ 2	$(1,3,5,2,1)$	
	2	$(1,2,1,1)$	$(1,3,2,3,1)$	5
		$(1,1,2,1)$ 2	$(1,2,3,4,1)$	
		$(1,1,1,1)$ 1	$(1,2,5,3,1)$	
		5	$(1,3,2,1,1)$	
			$(1,2,3,1,1)$	
			$(1,2,1,2,1)$	5
			$(1,1,2,3,1)$	
			$(1,1,3,2,1)$	
			$(1,2,1,1,1)$	
			$(1,1,2,1,1)$	3
			$(1,1,1,2,1)$	
			$(1,1,1,1,1)$	1
			14	

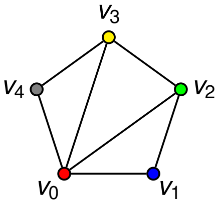
El número de estructuras aritméticas del camino.

Teorema

El número de estructuras aritméticas del camino P_{n+1} es igual al número de Catalan

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Estructuras aritméticas y triangulaciones del polígono.

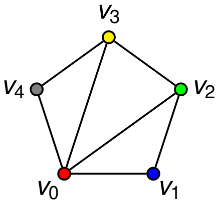


$\mapsto$

$$|\mathbf{d}'| = 3 \cdot 3$$

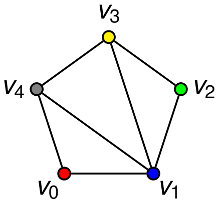
$$\mathbf{d}' = (3, \underbrace{1, 2, 2, 1}_{\mathbf{d}})$$

Estructuras aritméticas y triangulaciones del polígono.



$$\mapsto$$

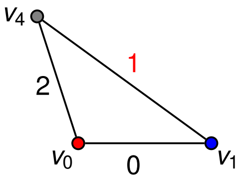
$$|\mathbf{d}'| = 3 \cdot 3$$
$$\mathbf{d}' = (3, \underbrace{1, 2, 2, 1}_{\mathbf{d}})$$



$$\mapsto$$

$$|\mathbf{d}'| = 3 \cdot 3$$
$$\mathbf{d}' = (1, \underbrace{3, 1, 2, 2}_{\mathbf{d}})$$

Estructuras aritméticas y triangulaciones del polígono.

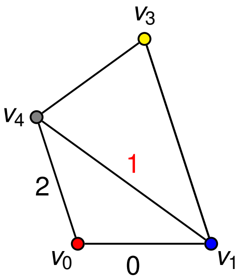


$(1,1,1)$

$\mapsto$

$()$

Estructuras aritméticas y triangulaciones del polígono.

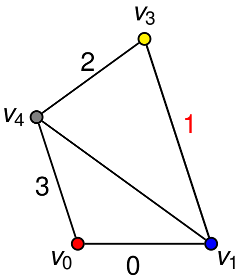


$(1, 2, 1, 2)$

$\mapsto$

(1)

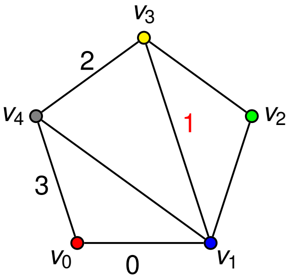
Estructuras aritméticas y triangulaciones del polígono.



$(1, 2, 1, 2)$

$\mapsto$ (1)

Estructuras aritméticas y triangulaciones del polígono.

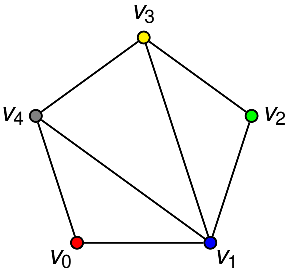


$(1, 3, 1, 2, 2)$

$\mapsto$

$(1, 1)$

Estructuras aritméticas y triangulaciones del polígono.

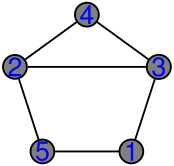


$(1, 3, 1, 2, 2)$ $\mapsto$ $(1, 1)$

El Algoritmo ilustrado.

El Algoritmo ilustrado

Considere la siguiente matriz pseudo-Laplaciana:

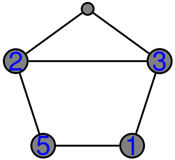


$$L = \begin{bmatrix} x_1+4 & -1 & 0 & 0 & -1 \\ -1 & x_2+2 & -1 & 0 & -1 \\ 0 & -1 & x_3+5 & -1 & 0 \\ 0 & 0 & -1 & x_4+1 & -1 \\ -1 & -1 & 0 & -1 & x_5+3 \end{bmatrix}$$

Sabemos que es una estructura aritmética ya que:

$$\det(L) = 6x_1 + 24x_2 + 6x_3 + 54x_4 + 7x_1x_2 + 3x_1x_3 + \cdots + x_1x_2x_3x_4x_5.$$

Considere la restricción $\mathbf{d}' = (2, 5, 1, 3)$

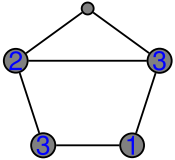


$$L = \begin{bmatrix} x_2 + 2 & -1 & 0 & -1 \\ -1 & x_3 + 5 & -1 & 0 \\ 0 & -1 & x_4 + 1 & -1 \\ -1 & 0 & -1 & x_5 + 3 \end{bmatrix}$$

Tenemos que

$$\det(L) = 6 + 7x_2 + 3x_3 + 22x_4 + 7x_5 + \cdots + x_2x_3x_4x_5.$$

Una estructura aritmética de $G \setminus v_1$ tal que $(2,3,1,3) \leq (2,5,1,3)$.

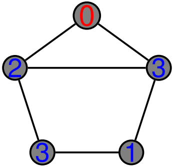


$$L = \begin{bmatrix} x_2+2 & -1 & 0 & -1 \\ -1 & x_3+3 & -1 & 0 \\ 0 & -1 & x_4+1 & -1 \\ -1 & 0 & -1 & x_5+3 \end{bmatrix}$$

Luego

$$\det(L) = 3x_2 + 3x_3 + 12x_4 + 3x_5 + \cdots + x_2x_3x_4x_5.$$

Una estructura aritmética de $G \setminus v_1$ tal que $(2, 3, 1, 3) \leq (2, 5, 1, 3)$.



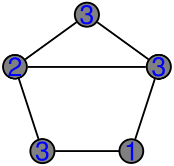
$$L = \begin{bmatrix} x_1 & -1 & 0 & 0 & -1 \\ -1 & x_2 + 2 & -1 & 0 & -1 \\ 0 & -1 & x_3 + 3 & -1 & 0 \\ 0 & 0 & -1 & x_4 + 1 & -1 \\ -1 & -1 & 0 & -1 & x_5 + 3 \end{bmatrix}$$

con

$$\det(L) = -12 - 2x_2 + 3x_1x_2 - 6x_3 + 3x_1x_3 - x_2x_3 + \cdots + x_2x_3x_4x_5.$$

El algoritmo

Hacer esto para todo vértice y obtenemos



$$L = \begin{bmatrix} x_1 + 3 & -1 & 0 & 0 & -1 \\ -1 & x_2 + 2 & -1 & 0 & -1 \\ 0 & -1 & x_3 + 3 & -1 & 0 \\ 0 & 0 & -1 & x_4 + 1 & -1 \\ -1 & -1 & 0 & -1 & x_5 + 3 \end{bmatrix}$$

con

$$\det(L) = -12 + 7x_2 + 3x_3 + 16x_4 + 7x_5 + \cdots + x_1 x_2 x_3 x_4 x_5.$$

El algoritmo

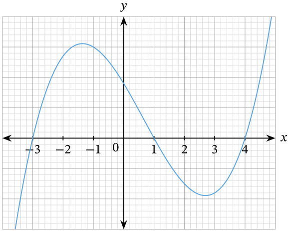
Entrada: Una matriz entera no-negativa con ceros en la diag.

1) Sean M_s las submatrices de M, borrar la col. y ren. s.
2) Compute $\mathcal{A}(M_s)$ para todo $s \in [n]$.
3) Sea $\mathbf{d} = \max_{s\in[n]}\mathbf{d}_s$ donde $\mathbf{d}_s \in \mathcal{A}(M_s)$.
4) Compute las EA $\mathbf{d}'$ de M tal que $\mathbf{d} \leq \mathbf{d}'$.

Salida: $\mathbf{d}$-structuras aritméticas de M.

Que pasa con las otras soluciones?

1. En general el conjunto de soluciones de una ecuación Diofantina determinantal es infinito.
2. La parte finita es formada por las estructuras aritmeticas y otras soluciones muy similares.
3. Hay un conjunto finito de familias infinitas de soluciones.
4. Muchas de las carateristicas de las soluciones pueden ser leidas en el polinomio $p_M(\mathbf{x}+\mathbf{d}) = \det((\mathbf{x}+\mathbf{d})I_n - M)$.



Bibliografia

- D. J. Lorenzini, Arithmetical graphs. Math. Ann. 285 (1989), no. 3, 481-501.
- H. Corrales y C. E. Valencia, Arithmetical structures of graphs, Linear Alg. and its App. 536 1 (2018), 120–151.
- Corrales, Valencia et al., Counting arithmetical structures on paths and cycles, Discrete Mathematics 341 10 (2018), 2949–2963.
- Ralihe R. Villagrán yC. E. Valencia, Algorithmic aspects of arithmetical structures, Linear Algebra and its Applications 640, 191–208, 2022.

Gracias por su atención!!!

http://www.math.cinvestav.mx/cvalencia