

Polinomios ciclotómicos y semigrupos numéricos

**Investigación y desarrollo de
software**

Andrés Herrera Poyatos

Tutor: Pedro A. García Sánchez

Matemáticas:

- ① *Cyclotomic polynomials at roots of unity*, Bartłomiej Bzdęga, Andrés Herrera-Poyatos and Pieter Moree, accepted by Acta Arithmetica, [arXiv:1611.06783](#).
- ② *Coefficients and higher order derivatives of cyclotomic polynomials: old and new*, Andrés Herrera-Poyatos and Pieter Moree, [arXiv:1805.05207](#).
- ③ *Isolated factorizations and their applications in simplicial affine semigroups*, Pedro A. García-Sánchez and Andrés Herrera-Poyatos, [arXiv:1804.00885](#).
- ④ *Exponent sequences of cyclotomic numerical semigroups*, Alexandru Ciolan, Pedro A. García-Sánchez, Andrés Herrera-Poyatos and Pieter Moree, on preparation.

Informática:

- ① Algoritmos para detectar polinomios de Kronecker.
- ② Herramientas para de visualización de grafos asociados a semigrupos numéricos: dot-numericalsgps and FrancyMonoids.

Definición (semigrupo numérico)

Un semigrupo numérico S es un submonoide aditivo de $\mathbb{N} = \{0, 1, 2, \dots\}$ tal que $\mathbb{N} \setminus S$ es finito.

Ejemplo

$$S = \langle 3, 5 \rangle = \{3a + 5b : a, b \in \mathbb{N}\} = \{0, 3, 5, 6, 8, \rightarrow\}$$

0	1	2	3	4	5	6	7	8	9
1	0	0	1	0	1	1	0	1	1	...	1

Proposición

- Todo semigrupo numérico tiene un único sistema de generadores minimal, que es finito. Su cardinal se denomina **dimensión de inmersión de S** .
- $S = \langle n_1, \dots, n_e \rangle \subseteq \mathbb{N}$ es un semigrupo numérico si, y solo si, $\gcd(n_1, \dots, n_e) = 1$.

Definición (Serie de Hilbert y polinomio del semigrupo)

Serie de Hilbert:
$$H_S(x) = \sum_{s \in S} x^s = \frac{1}{1-x} - \sum_{g \notin S} x^g$$

Polinomio del semigrupo:

$$P_S(x) = (1-x)H_S(x) = 1 + (x-1) \sum_{g \notin S} x^g$$

¡Algunas propiedades del semigrupo se caracterizan mediante propiedades de P_S !

Ejemplo: S es simétrico si, y solo si, P_S es un palíndromo.

Ejemplo ($S = \langle 3, 5 \rangle = \{0, 3, 5, 6, 8, \rightarrow\}$)

$$H_S(x) = \frac{1}{1-x} - x - x^2 - x^4 - x^7 = \frac{1-x^{15}}{(1-x^3)(1-x^5)}$$

$$P_S(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8 = \frac{(1-x)(1-x^{15})}{(1-x^3)(1-x^5)} = \Phi_{15}(x)$$

Definición (Polinomios ciclotómicos)

Sea ζ_n una raíz n -ésima primitiva de la unidad. El n -ésimo polinomio ciclotómico es

$$\Phi_n(x) = \prod_{1 \leq j \leq n, (j,n)=1} (x - \zeta_n^j).$$

- Φ_n es el polinomio mínimo de ζ_n en \mathbb{Q} ;
- Φ_n es mónico con coeficientes enteros.

Definición (Polinomios de Kronecker)

Un polinomio $p \in \mathbb{Z}[x]$ es de Kronecker si todas sus raíces están en el círculo unidad, $\{z \in \mathbb{C} : |z| \leq 1\}$.

Lema (Kronecker)

Un polinomio $p \in \mathbb{Z}[x]$ es de Kronecker si, y solo si, factoriza como producto de un monomio y polinomios ciclotómicos.

Cyclotomic numerical semigroups

A. Ciolan, P.A. García-Sánchez, and P. Moree
SIAM J. Discrete Math. 30 (2016).

Definición (Semigrupos numéricos ciclotómicos)

Un semigrupo numérico S es ciclotómico si su polinomio es de Kronecker.

Definición (Intersecciones completas)

Un semigrupo numérico S es intersección completa si todas sus presentaciones minimales tienen $e(S) - 1$ relaciones.

Teorema (Ciolan, García-Sánchez, Moree)

Sea S un semigrupo numérico.

- ① *Si S es intersección completa, entonces S es ciclotómico.*
- ② *Si S es ciclotómico, entonces es simétrico.*

Cyclotomic numerical semigroups

A. Ciolan, P.A. García-Sánchez, and P. Moree
SIAM J. Discrete Math. 30 (2016).

Definición (Semigrupos numéricos ciclotómicos)

Un semigrupo numérico S es ciclotómico si su polinomio es de Kronecker.

Teorema (Ciolan, García-Sánchez, Moree)

Sea S un semigrupo numérico.

- ① *Si S es intersección completa, entonces S es ciclotómico.*
- ② *Si S es ciclotómico, entonces es simétrico.*

Conjetura

- ① *Un semigrupo numérico es ciclotómico si, y solo si, es intersección completa.*
- ② *Para cada $k \geq 4$ existe un semigrupo numérico S_k simétrico con dimensión de inmersión k que no es ciclotómico.*

Cyclotomic polynomials at roots of unity

Bartłomiej Bzdęga, Andrés Herrera-Poyatos and Pieter Moree
Acta Arithmetica (2018), [arXiv:1611.06783](#)

Problema

Evaluar Φ_n en las raíces de la unidad.

Lema (Evaluación en 1)

$$\Phi_n(1) = \begin{cases} 0 & \text{si } n = 1; \\ p & \text{si } n = p^k \text{ para algún primo } p; \\ 1 & \text{en caso contrario.} \end{cases}$$

Lema (Evaluación en -1)

$$\Phi_n(-1) = \begin{cases} -2 & \text{si } n = 1; \\ 0 & \text{si } n = 2; \\ p & \text{si } n = 2p^k \text{ para algún primo } p; \\ 1 & \text{en caso contrario.} \end{cases}$$

Cyclotomic polynomials at roots of unity

Bartłomiej Bzdęga, Andrés Herrera-Poyatos and Pieter Moree
Acta Arithmetica (2018), [arXiv:1611.06783](#)

Teorema (Evaluación de Φ_n en raíces de la unidad)

Sean $n, m > 1$ enteros coprimos y ξ_m una raíz m -ésima primitiva de la unidad. Entonces

$$\Phi_n(\xi_m) = \exp \left(\sum_{\chi \in \widehat{\mathbb{Z}_m^\times}} \hat{f}(\chi) \chi(n) \prod_{p|n} (1 - \bar{\chi}(p)) \right),$$

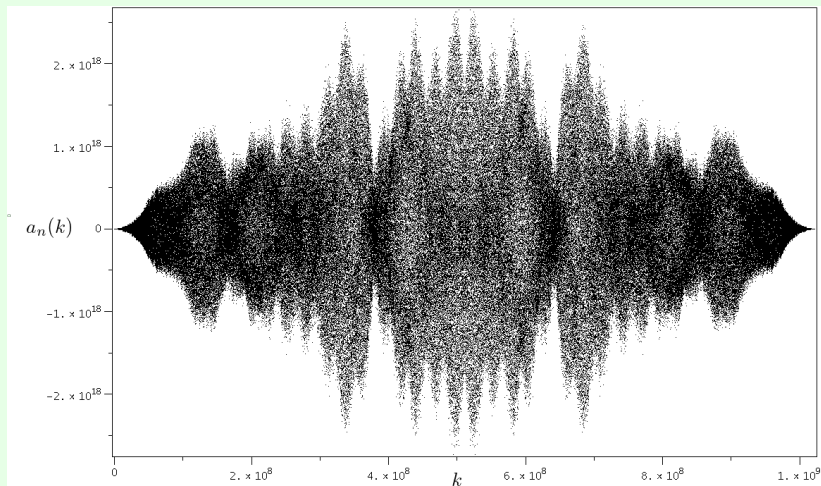
donde $f(k) = \log(1 - \xi_m^k)$.

Teorema (Originalmente demostrado por Vaughan, 1975)

Existen infinitos enteros positivos n tales que

$$\log \log H(\Phi_n) > \log(2) \frac{\log n}{\log \log n}.$$

Ejemplo ($n = 3234846615 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$)



Si el número de factores primos distintos de n es grande aparecen patrones complejos que no sabemos explicar.

Coefficients and higher order derivatives of cyclotomic polynomials: old and new

Andrés Herrera-Poyatos and Pieter Moree

arXiv:1805.05207

Teorema (Lehmer, 1966)

Sean $k \geq 1$ y $n \geq 2$ enteros. Entonces

$$(\log \Phi_n)^{(k)}(1) = \sum_{j=1}^k \frac{B_j^+ s(k, j)}{j} J_j(n).$$

Teorema

$$\frac{\Phi_n^{(k)}(1)}{\Phi_n(1)} = \mathcal{B}_k \left(\sum_{j=1}^1 \frac{B_j^+ s(1, j)}{j} J_j(n), \dots, \sum_{j=1}^k \frac{B_j^+ s(k, j)}{j} J_j(n) \right).$$

Coefficients and higher order derivatives of cyclotomic polynomials: old and new

Andrés Herrera-Poyatos and Pieter Moree

arXiv:1805.05207

Teorema

Sea f un polinomio de Kronecker con $f(0) \neq 0$ y $f(1) \neq 0$. Escribimos $f = \prod_{\mathcal{D}} \Phi_d^{e_d}$. Para cada entero $k \geq 2$ se tiene

$$\sum_{j=1}^k \left\{ \begin{matrix} k \\ j \end{matrix} \right\} (\log f)^{(j)}(1) = \frac{B_k^+}{k} \sum_{d \in \mathcal{D}} e_d J_k(d).$$

Teorema

Para cada $k \geq 4$ el semigrupo numérico

$$S_k = \{0, k, k+1, k+2, \rightarrow\} \setminus \{2k-1\}$$

es simétrico, tiene dimensión de inmersión k y no es ciclotómico.

Isolated factorizations and their applications in simplicial affine semigroups

Pedro A. García-Sánchez and Andrés Herrera-Poyatos

arXiv:1804.00885

Sea S un semigrupo numérico y $A = \{n_1, \dots, n_e\}$ un sistema de generadores minimal de A . Definimos $\varphi: \mathbb{N}^e \rightarrow S$ como

$$\varphi(x_1, \dots, x_e) = x_1 n_1 + \dots + x_e n_e.$$

Definición (factorizaciones aisladas)

- Las factorizaciones de $s \in S$ son los elementos de $Z(s) = \varphi^{-1}(s)$.
- $x \in Z(s)$ es aislada si $\langle x, y \rangle = 0$ para todo $y \in Z(s) \setminus \{x\}$.

Aplicación: Análisis de nuevas familias de semigrupos numéricos

Único elemento de Betti \subset Betti divisible \subset Betti ordenado

\subset Intersección completa con solo un elemento Betti minimal

$\subset \alpha$ -rectangular \subset Libre \subset Intersección completa.

Exponent sequences of cyclotomic numerical semigroups

Alexandru Ciolan, Pedro A. García-Sánchez, Andrés
Herrera-Poyatos and Pieter Moree

Definición (Secuencia de exponentes ciclotómicos)

Sea S un semigrupo numérico ciclotómico. Existe una secuencia $\{f_d\}$ con soporte finito tal que

$$P_S(x) = \prod_{d=1}^{\infty} (1 - x^d)^{f_d},$$

Esta secuencia se denomina secuencia de exponentes ciclotómicos de S .

- ① $\Omega_+ = \{d \in \mathbb{N} : f_d > 0\};$
- ② $\Omega_- = \{d \in \mathbb{N} : f_d < 0\}.$

Teorema

Ω_- es un sistema de generadores de S y $\Omega_+ \setminus \{1\} \subset S$.

Exponent sequences of cyclotomic numerical semigroups

Alexandru Ciolan, Pedro A. García-Sánchez, Andrés
Herrera-Poyatos and Pieter Moree

Teorema

$\Lambda \subseteq \Omega \setminus (A \cup \{1\})$ con:

- ① Λ está totalmente ordenado con respecto a \leq_S , el orden del semigrupo;
- ② si $\alpha \in \Lambda$ y $s \in \Omega \setminus (A \cup \{1\})$ con $s \leq_S \alpha$, entonces $s \in \Lambda$.

Entonces $\Lambda \subseteq \text{Betti}(S) \cap \Omega_+$.

Teorema

Sea A un sistema de generadores minimal de S .

- ① S es Betti ordenado si, y solo si, S es ciclotómico y $\Omega^* \setminus (A \cup \{1\})$ está totalmente ordenado con respecto a \leq_S .
- ② S es Betti divisible si, y solo si, S es ciclotómico y $\Omega^* \setminus (A \cup \{1\})$ está totalmente ordenado con respecto a la divisibilidad de enteros.

Algoritmos para detectar polinomios de Kronecker

- Estudio del estado del arte.
- Desarrollo de nuevas propuestas.

Aplicaciones:

- ① Detección de semigrupos numéricos ciclotómicos.
- ② Detección de semigrupos numéricos intersecciones completas (si ciclotómico = intersección completa).



- Implementación en GAP.
- Licencia GPLv2.
- El mejor algoritmo se ha añadido al paquete `numericalsgps` de GAP.
gap-packages.github.io/numericalsgps/

Algoritmos para detectar polinomios de Kronecker

① Algoritmo propuesto por Pieter Moree.

- Basado en nuestro trabajo sobre polinomios de Kronecker.
- Complejidad: $O((\deg p)^6)$ en el peor caso.

② Algoritmo propuesto por David Boyd.

- Basado en secuencias de Sturm.
- Complejidad: $\theta((\deg p)^3)$.

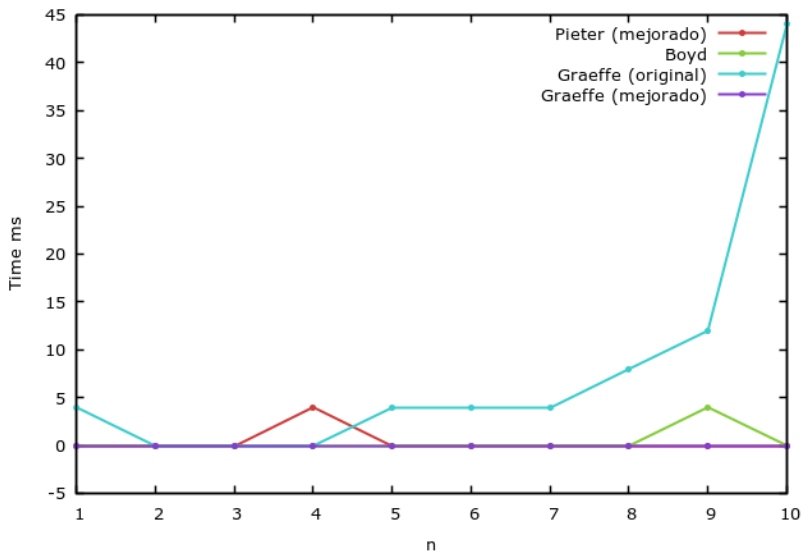
③ Algoritmo propuesto por Bradford and Davenport.

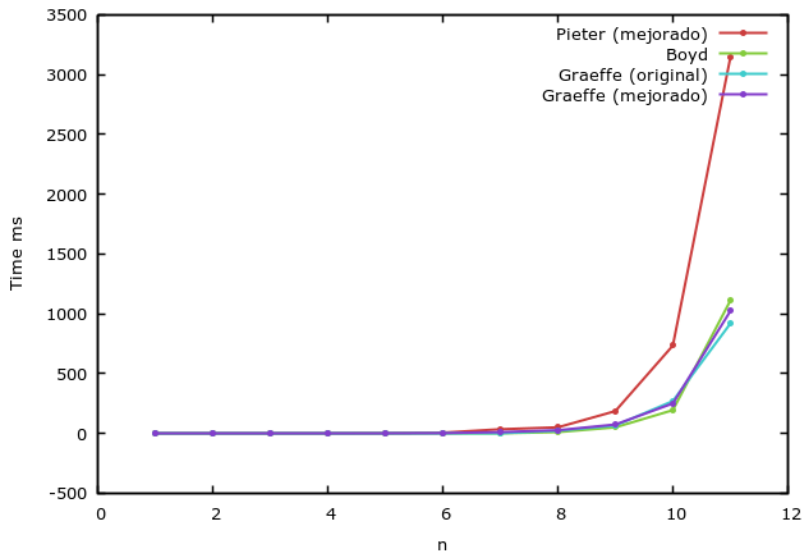
- Basado en el método de Graeffe.
- Complejidad: Difícil de analizar teóricamente.
 $O((\deg p)^4)$ en el peor caso.

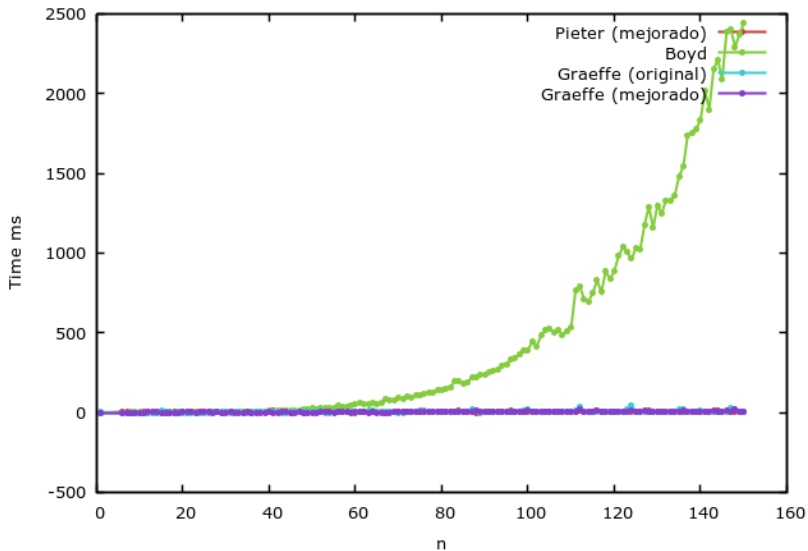
④ Nueva propuesta basada en el algoritmo de Bradford y Davenport.

- Complejidad: $O((\deg p)^3)$ en el peor caso.
- Es el mejor tanto en la teoría como en la práctica.

Para medir la complejidad, suponemos que los coeficientes están acotados.

Kronecker algorithms on $x^{2^n} + 2$ 

Kronecker algorithms on $x^{2^n}-1$ 

Kronecker algorithms on $1-x+x^n-x^{2n-1}+x^{2n}$ 

Herramientas de visualización para semigrupos numéricos

Motivación: visualizar grafos asociados a semigrupos numéricos

① dot-numericalsgps

- Genera código DOT
- El código DOT se visualiza mediante graphviz o similar
- Se ha añadido a la última versión de numericalsgps:
gap-packages.github.io/numericalsgps/doc/chap14.html

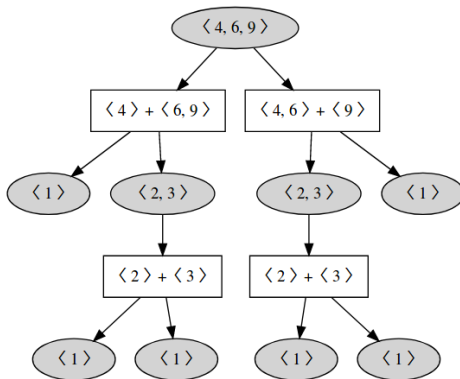
② FrancyMonoids

- Genera diagramas interactivos de 3djs
- Utiliza el paquete de GAP Francy:
<https://github.com/mcmartins/francy>
- Se encuentra en la organización de paquetes de GAP en GitHub:
<https://gap-packages.github.io/FrancyMonoids/>

- Ambos paquetes se pueden usar con jupyter
- Tienen licencia GPLv2

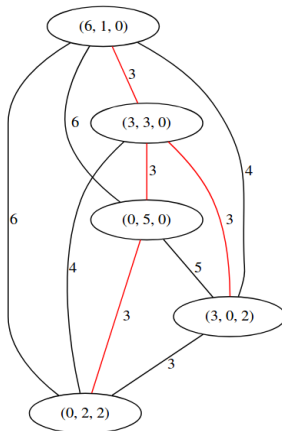
dot-numericalsgps

```
LoadPackage("numericalsgps");
S := NumericalSemigroup(4,6,9);
DotSplash(DotTreeOfGluingsOfNumericalSemigroup(S, 4));
```



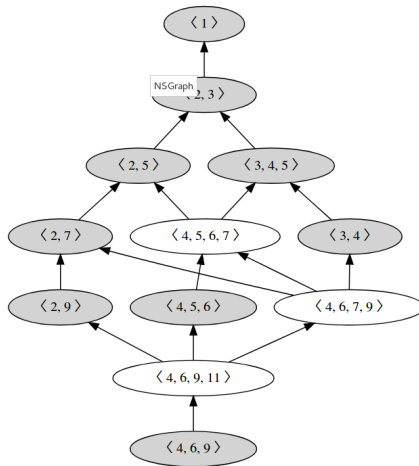
dot-numericalsgps

```
LoadPackage("numericalsgps");  
S := NumericalSemigroup(4,6,9);  
f:=FactorizationsElementWRTNumericalSemigroup(30,S);  
JupyterSplashDot(DotFactorizationGraph(f));
```



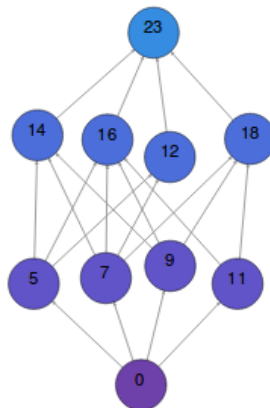
dot-numericalsgps

```
LoadPackage("numericalsgps");  
S := NumericalSemigroup(4,6,9);  
JupyterSplashDot(DotOverSemigroupsNumericalSemigroup(S));
```



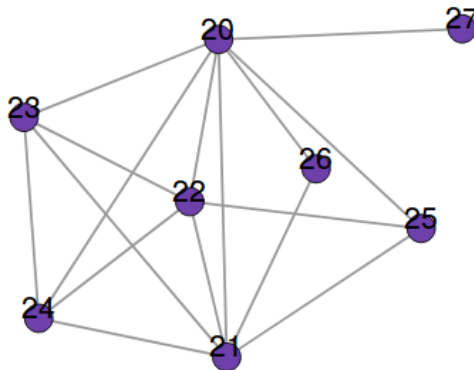
FrancyMonoids

```
LoadPackage("numericalsgps");  
LoadPackage("FrancyMonoids");  
s:=NumericalSemigroup(5,7,9,11);  
DrawHasseDiagramOfNumericalSemigroup(s,ApéryList(s,10));
```



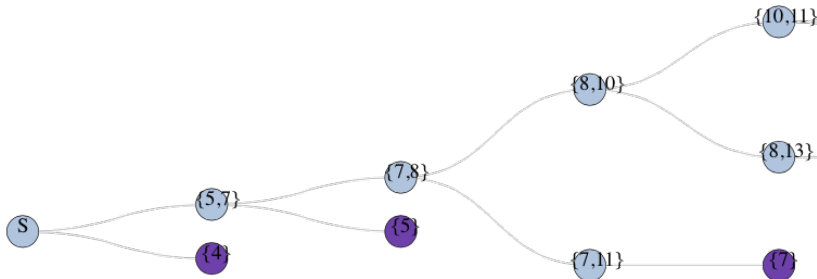
FrancyMonoids

```
LoadPackage("numericalsgps");  
LoadPackage("FrancyMonoids");  
s:=NumericalSemigroup(20,21,22,23,24,25,26,27,28);  
DrawRosalesGraph(67,s);
```



FrancyMonoids

```
LoadPackage("numericalsgps");
LoadPackage("FrancyMonoids");
s:=NumericalSemigroup(3,4,5);
gens:=s->Difference(MinimalGenerators(s),
                    [Multiplicity(s)]);
DrawTreeOfSonsOfNumericalSemigroup(s,5,gens);
```



Trabajo en proceso

① Secuencias de exponentes ciclotómicos

- Eliminar la hipótesis de que S sea ciclotómico en los resultados acerca de Ω_- y Ω_+ .
- Aplicación a semigrupos numéricos ciclotómicos con altura y profundidad fija.
- Estudio de la longitud de un semigrupo numérico ciclotómico.

② Semigrupos simpliciales afines:

- Generalizar el concepto de semigrupo numérico β -rectangular y γ -rectangular.
- Estudio de los semigrupos c^* -rectangulares, \bar{c} -rectangulares y c -rectangulares.

③ Semigrupos numéricos intersecciones completas:

- Nuevas caracterizaciones en terminos de $Betti(S)$.

④ Algoritmos para detectar polinomios de Kronecker:

- Publicar nuestro estudio y nuestras propuestas.

⑤ Librerías `numericalsgps-dot` y `FrancyMonoids`:

- Desarrollo de nuevas funciones.

¡Gracias por su atención!

Andrés Herrera Poyatos
andreshp9@gmail.com