UNIVERSIDAD DE GRANADA

Polinomios ciclotómicos y semigrupos numéricos

Investigación y desarrollo de software

Andrés Herrera Poyatos

Tutor: Pedro A. García Sánchez

Trabajo de Fin de Grado

Doble Grado en Ingeniería Informática y Matemáticas

Facultad de Ciencias

E.T.S. Ingenierías Informática y de Telecomunicación

Granada, a 19 de Junio de 2018

Abstract

In this thesis we present novel research on cyclotomic polynomials and commutative monoids, which ranges from new theoretical results to new algorithms and software.

Regarding cyclotomic polynomials, we evaluate these polynomials and their derivatives at roots of unity and obtain some consequences. We also extend some of these results to Kronecker polynomials, these being products of cyclotomic polynomials and a monomial.

Concerning commutative monoids, we introduce the concept of isolated factorizations and we use our insight about these factorizations to characterize four families of simplicial affine semigroups in several ways. These results can be effectively applied to numerical semigroups, obtaining very interesting consequences. Indeed, we apply a considerable part of the mentioned work to cyclotomic numerical semigroups. We prove a conjecture of Ciolan, Moree and García-Sánchez that states that for every integer $k \geq 4$ there is a cyclotomic numerical semigroup with embedding dimension k that is not symmetric. Another conjecture of the same authors claims that cyclotomic numerical semigroups are complete intersections. We make partial progress towards proving this latter conjecture. Moreover, we relate the cyclotomic exponent sequence of a numerical semigroup with its minimal system of generators and its Betti elements.

Our work also has a relevant computer science part. We compare several algorithms to detect Kronecker polynomials from theoretical and empirical perspectives. One of these algorithms is a novel proposal of our own and turns out to be the best algorithm on average. The implementation of this algorithm has been included in the GAP package `numericalsgps`.

Finally, we present two packages to draw graphs associated to numerical semigroups, `numerical-sgps` and `FrancyMonoids`.

Keywords: cyclotomic polynomials, Kronecker polynomials, commutative monoids, minimal presentations, complete intersections, affine semigroups, numerical semigroups, GAP, DOT

Resumen

Este trabajo se enmarca dentro de la teoría de números, el álgebra conmutativa y la informática teórica. Concretamente, presentamos nuevos resultados sobre polinomios ciclotómicos y monoides conmutativos. Hemos desarrollado nuevos conceptos y herramientas dentro de este ámbito que nos han permitido abordar varios problemas abiertos. Además, hemos implementado múltiples algoritmos para trabajar con estos objetos matemáticos y hemos desarrollados dos paquetes para visualizar grafos y árboles asociados a semigrupos numéricos.

Marco teórico

Un semigrupo numérico es un submonoide aditivo de los números naturales (incluyendo a 0) cuyo complemento en $\mathbb{N}$ es finito [**?**, Capítulo 1]. El máximo del conjunto $\mathbb{Z} \setminus S$ es conocido como el *número de Frobenius de* S y es denotado por $\mathrm{F}(S)$. Cada semigrupo numérico admite un único sistema de generadores minimal, que es finito. La cardinalidad de este conjunto se denota por $\mathrm{e}(S)$ y se conoce como la *dimensión de inmersión de* S. Como los semigrupos numéricos son monoides conmutativos finitamente generados, también son finitamente presentados. Es más, cada presentación de S consta de, al menos, $\mathrm{e}(S) - 1$ relaciones. Un semigrupo numérico se dice que es intersección completa si su presentación minimal tiene exactamente tiene exactamente $\mathrm{e}(S) - 1$ relaciones.

A cada semigrupo numérico S se le puede asociar una serie, denominada serie de Hilbert (o función generatriz de S), que viene dada por

$$\mathrm{H}_S(x) = \sum_{s \in S} x^s$$

y que lo caracteriza de forma unívoca. Esta serie se puede determinar a partir del *polinomio del semigrupo numérico*, definido como $\mathrm{P}_S(x) = (1 - x)\mathrm{H}_S(x)$. Nótese que efectivamente P_S es un polinomio gracias a que $\mathbb{N} \setminus S$ es finito. El estudio de este polinomio es un aspecto importante de la teoría de semigrupos numéricos. Varias propiedades del semigrupo numérico se caracterizan en términos de propiedades del polinomio asociado. Por ejemplo, el polinomio es un palíndromo si, y solo si, el semigrupo numérico es simétrico [**?**]. En múltiples casos trabajar con estos polinomios no solo proporciona resultados teóricos interesantes sino que también presenta ventajas computacionales a la hora de desarrollar algoritmos.

Por otro lado, los *polinomios ciclotómicos* son aquellos polinomios irreducibles de $\mathbb{Z}[x]$ tales que sus raíces son raíces de la unidad. El n-ésimo polinomio ciclotómico, Φ_n, es el polinomio mínimo de $\zeta_n = e^{2\pi i/n}$ sobre $\mathbb{Q}$. Por tanto, estos polinomios están relacionados con la teoría de cuerpos ciclotómicos, siéndo ésta un área importante de la teoría de números. Otro concepto relacionado con el de polinomio ciclotómico es el de polinomio de Kronecker [**?**]. Un polinomio de $\mathbb{Z}[x]$ se dice que es de Kronecker si sus raíces se encuentran en el disco unidad $\{z \in \mathbb{C} : |z| \leq 1\}$. Un resultado famoso de Kronecker afirma que los polinomios de Kronecker factorizan como producto de un monomio y polinomios ciclotómicos.

Descripción de los problemas abordados. Investigación producida

Recientemente se ha planteado la siguiente cuestión, "clasificar todos los semigrupos numéricos tales que su polinomio es de Kronecker" [**?**]. A estos semigrupos numéricos se les denomina ciclotómicos y son uno de los objetos de estudio de este trabajo. En [**?**] los autores demostraron que si un semigrupo numérico es intersección completa, entonces es ciclotómico. Además, comprobaron computacionalmente el recíproco de esta afirmación para semigrupos numéricos con número de Frobenius menor o igual que 69. Este hecho les llevó a conjeturar que un semigrupo numérico es ciclotómico si, y solo si, es intersección completa.

Originalmente el objetivo de este trabajo era tratar de demostrar que los semigrupos numéricos ciclotómicos son intersecciones completas, así como desarrollar e implementar algoritmos para detectar semigrupos numéricos ciclotómicos. Como un efecto colateral de esta investigación, surgieron otros problemas relevantes y desarrollamos varias herramientas y resultados interesantes dentro de la teoría de polinomios ciclotómicos y monoides conmutativos. Estos resultados evolucionaron hasta el punto de escribir cuatro publicaciones distinta. Tres de estas publicaciones ya se han subido al arXiv [**?**, **?**, **?**] y una de ellas ya ha sido aceptada por una revista especializada en teoría de números, Acta Arithmetica [**?**].

El primer problema considerado en este trabajo consiste en evaluar polinomios ciclotómicos en raíces de la unidad, esto es, encontrar una expresión para $\Phi_n(\zeta_m^k)$ cuando sea posible. Nuestra aspiración era que resolviendo este problema podríamos encontrar varias condiciones necesarias para ser un polinomio de Kronecker. Algunas condiciones de esta índole ya habían sido utilizadas en [**?**]. Hemos publicado los resultados obtenidos en este problema en [**?**], y varían desde una fórmula genérica para $\Phi_n(\zeta_m^k)$ hasta una nueva demostración del teorema de Vaughan, que trata sobre el comportamiento asintótico de la altura de Φ_n.

Un problema relacionado con el anterior es el de determinar las derivadas logarítmicas de Φ_n en ± 1. Lehmer fue el primer autor en estudiar y calcular estas derivadas [**?**]. En este trabajo presentamos una demostración más corta de los resultados de Lehmer y los aplicamos para encontrar una familia de eucaciones lineales que tienen como solución a las derivadas logarítmicas de los polinomios de Kronecker. Los coeficientes de estas ecuaciones lineales son números de Stirling de segunda especie. Estas ecuaciones se pueden utilizar para detectar polinomios que no sean de Kroencker. Como aplicación, para cada entero $k \geq 4$ encontramos un semigrupo numérico simétrico S con $\mathrm{e}(S) = k$ y $\mathrm{F}(S) = 2k + 1$ que no es ciclotómico. Este resultado establece una conjetura de Ciolan et. al. [**?**, Conjetura 2]. Hemos publicado todos estos resultados en [**?**] junto con una recopilación de fórmulas para los coeficientes de los polinomios ciclotómicos.

Con respecto a la teoría de monoides conmutativos, introducimos el concepto de factorizaciones aisladas y proporcionamos múltiples propiedades de estas factorizaciones. Estos resultados nos permiten caracterizar varias familias de semigrupos afines y son particularmente interesantes al aplicarse a semigrupos numéricos. Una de estas aplicaciones es el estudio de los semigrupos numéricos Betti ordenados y Betti divisibles, conceptos que hemos introducido nosotros en nuestro trabajo. Estos semigrupos resultan ser intersecciones completas y son una generalización de los semigrupos numéricos con un único elemento de Betti [**?**]. Hemos publicado estos resultados en [**?**].

Los resultados desarrollados sobre factorizaciones aisladas nos han permitido avanzar en la clasificación de los semigrupos numéricos ciclotómicos. Concretamente, nos han permitido obtener información a partir las secuencias de exponentes ciclotómicos de semigrupos numéricos ciclotómicos. Estas secuencias resultan estar muy relacionadas con los sistemas minimales de generadores y los elementos de Betti de estos semigrupos. Como consecuencia de estos avances, hemos caracterizado los semigrupos numéricos Betti ordenados y Betti divisibles en términos de sus secuencias de exponentes ciclotómicos. En particular, hemos demostrado que bajo ciertas hipótesis en la secuencia de exponentes ciclotómicos de un semigrupo numérico ciclotómico, este semigrupo es intersección completa. En el momento de terminar este trabajo seguimos trabajando en esta temática y esperamos conseguir más resultados pronto.

Si el conjunto de semigrupos numéricos ciclotómicos coincide con el de intersecciones completas, entonces para determinar si un semigrupo numérico es intersección completa o no bastaría comprobar si su polinomio es de Kronecker. Por lo tanto, buscar algoritmos eficientes para determinar si un polinomio es de Kronecker o no es un problema interesante. Hemos buscado algoritmos para este problema exhaustivamente en la literatura especializada. En este trabajo exponemos los frutos de esta búsqueda además de otras propuestas que nos han sugerido algunos investigadores de renombre en teoría de números. Ademas, hemos determinado la complejidad algorítmica de estos algoritmos y hemos mejorado algunos de ellos.

Desarrollo de software

Hemos implementado cada uno de los algoritmos para detectar polinomios de Kronecker que se han considerado. Este software se puede encontrar en GitHub [**?**] y está licenciado mediante GPLv2 (GNU general public license, versión 2). Hemos escrito el código en GAP, un sistema para el álgebra computacional discreta [**?**].

El mejor algoritmo de los anteriores se ha añadido al paquede de GAP `numericalsgps` [**?**], que también tiene una licencia GPLv2. Este paquete nos permite realizar operaciones con semigrupos numéricos en GAP. Además, se distribuye con la instalación por defecto de GAP y es el segundo paquete más citado de GAP según swMATH.

Durante el desarrollo de los resultados matemáticos que involucran semigrupos numéricos, surgió la necesidad de visualizar varios grafos y árboles que aparecen en este contexto. Esto motivó que desarrollasemos dos librerías de software que dibujan grafos y árboles asociados a semigrupos numéricos.

- `dot-numericalsgps` [**?**]. Esta librería contiene múltiples funciones para generar código DOT a partir de salidas del paquete `numericalsgps`. DOT es un lenguaje para la descripción de grafos [**?**] que puede ser renderizado por Graphviz [**?**] y otras librerías para la visualización de grafos. El código de `dot-numericalsgps` está disponible en GitHub [**?**] y está licenciado bajo GPLv2. Este código ha sido incluido en la última versión de `numericalsgps`, véase [**?**, manual, capítulo 14]. La versión actual del paquete de GAP `JupyterKernel` contiene una función para dibujar grafos descritos en DOT [**?**] . Por lo tanto, nuestras funciones se pueden utilzar en un notebook de jupyter con GAP [**?**].

- `FrancyMonois` [**?**]. Este paquete muestra objetos relacionados con monoides mediante `francy`, un entorno para desarrollar gráficos interactivos en GAP [**?**]. `FrancyMonoids` se encuentra en el repositorio oficial de GAP en GitHub [**?**]. La principal ventaja de usar este paquete es que los gráficos generados son interactivos, lo que puede ser particularmente útil para una página web o un notebook de jupyter.

Acknowledgements

The development of this thesis would have not been possible without the guidance and help of my advisor, Pedro A. García-Sánchez, and our collaborator, Pieter Moree. I would like to thank them for their support, encouragement and advice, as well as the countless hours that they have spent on these projects.

Completing my Bachelor's degree would have been much more difficult if it not were for the support and encouragement of my family and my girlfriend. I am very grateful to all of them and, in particular, my parents, Mercedes and Francisco, who have made everything that they could for me. I am sorry that, during the last months, I have devoted more time to this thesis than to you.

Last but not least, I would like to dedicate this thesis to my grandmother, who died this year. During my first and second years as a Bachelor's student, she always cooked for me when I had to stay the whole day at the university. Her marvelous dishes definitely helped me to stay active during these busy days and perform better at my exams. A part of she will always be with me.

Contents

Part I

Introduction

Chapter 1

Description

In this thesis we delve into two mathematical theories, the field of cyclotomic polynomials and the field of numerical semigroups, as well as other related topics. We develop new tools and concepts that we use to address some open problems on these fields. We also implement several algorithms to operate with these mathematical objects, and present two packages to visualize graphs and trees associated to numerical semigroups.

1.1 Theoretical framework

1.2 Description of the addressed problems. Produced research

1.3 Developed software

1.4 Structure of the thesis

This thesis is divided into two main parts.

a) **Mathematics**. This part contains the four publications that have been or are being developed on the fields of cyclotomic polynomials and commutative monoids.

- Cyclotomic polynomials at roots of unity, by Bartłomiej Bzdęga, Andrés Herrera-Poyatos and Pieter Moree, accepted in Acta Arithmetica, to appear. Avalaible on arXiv, arXiv:1611.06783.
- Coefficients and higher order derivatives of cyclotomic polynomials: old and new, by Andrés Herrera-Poyatos and Pieter Moree, available on arXiv, arXiv:1805.05207.
- Isolated factorizations and their applications in simplicial affine semigroups, by Pedro A. García-Sánchez and Andrés Herrera-Poyatos, available on arXiv, arXiv:1804.00885.
- Exponent sequences of cyclotomic numerical semigroups, by Alexandru Ciolan, Pedro A. García-Sánchez, Andrés Herrera-Poyatos and Pieter Moree. This publication is still being prepared for submission.

b) **Computer science**. This part deals with the algorithmic and coding aspect of the thesis. It is divided in two chapters.

- Algorithms to detect Kronecker polynomials. In this chapter we explain the three algorithms that we are aware of for detecting Kronecker polynomials. We present some improvements for these algorithms. We also compare them from theoretical and empirical perspectives.
- Visualization tools for numerical semigroups. We introduce our packages `dot-numericalsgps` and `FrancyMonoids` and provide some examples of their use.

1.5 Main bibliography

Chapter 2

Objectives and related courses

2.1 Objectives

2.2 Courses that are related to this thesis

The following list contains the courses of the double degree in mathematics and computer science that are taught at the University of Granada and are significantly related to this thesis.

a) **Mathematics**:

- Álgebra I
- Álgebra II
- Álgebra III
- Teoría de Números y Criptografía
- Álgebras, Grupos y Representaciones.

b) **Computer science**:

- Lógica y Métodos Discretos
- Algorítmica
- Estructuras de Datos
- Modelos Avanzados de Computación
- Fundamentos de Programación
- Metodología de la Programación

Part II

Mathematics

Part III

Computer Science

Part IV

Conclusion and future work

Chapter 3

Conclusion and future work

3.1 Conclusion

In this work we have obtained novel results in the fields of cyclotomic polynomials and commutative monoids. We have also developed new algorithms for detecting Kronecker polynomials after studying the literature available on this topic. Finally, we have presented two packages for drawing graphs associated to numerical semigroups.

The original objectives have been successfully achieved. Moreover, we have reached new objectives that were not initially considered when we proposed this thesis. Our focus was originally limited to cyclotomic numerical semigroups but, as a side effect of our research on this topic, we have produced a series of new results and tools that are interesting on their own. This has lead to the development of four separate publications, one of which have already been accepted by a peer-reviewed journal in number theory.

3.2 Future work

The publication on exponent sequences of cyclotomic numerical semigroups (Chapter **??**) is still a draft. We expect to generalize our results on cyclotomic exponent sequences to arbitrary numerical semigroups. That is, we are getting rid of the assumption of the finiteness of the exponent sequence. We hope that after these changes, Chapter **??** is ready to be separately published soon.

Our work on cyclotomic numerical semigroups generates expectation on a possible proof of the main conjecture of this area, which states that cyclotomic numerical semigroups are complete intersections. Nonetheless, our results only reach the surface of this conjecture, which is expected to be a very deep result. Relating a property of the polynomial of a numerical semigroup with the cardinality of its minimal presentation would be a very important advance in the theory of numerical semigroups.

The study of algorithms to detect Kronecker polynomials has been more productive than we expected. We were able to come up with new proposals that perform better than the current algorithms of the state of the art. We are going to work more on these proposals with the expectations of writing a journal publication on this topic.

Finally, the GAP packages `dot-numericalsgps` and `FrancyMonoid` will be continuously improved. We will add new functionality as new graphs and similar structures arise in the theory of numerical semigroups.