ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

ELABORACIÓN DE UNA MONOGRAFÍA SOBRE LA ELIMINACIÓN DE CUANTIFICADORES, DIRIGIDA A ESTUDIANTES DE LA CARRERA DE MATEMÁTICA DE LA ESPOCH

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

MATEMÁTICO

AUTOR:

DARÍO GONZALO MATEHU TUALONGO

Riobamba – Ecuador

2024

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

ELABORACIÓN DE UNA MONOGRAFÍA SOBRE LA ELIMINACIÓN DE CUANTIFICADORES, DIRIGIDA A ESTUDIANTES DE LA CARRERA DE MATEMÁTICA DE LA ESPOCH

Trabajo de Integración Curricular

Tipo: Proyecto de Investigación

Presentado para optar al grado académico de:

MATEMÁTICO

AUTOR: DARÍO GONZALO MATEHU TUALONGO

DIRECTOR: Dr. LEONIDAS ANTONIO CERDA ROMERO

Riobamba – Ecuador

2024

Yo, Darío Gonzalo Matehu Tualongo, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación, el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 13 de mayo de 2024

Darío Gonzalo Matehu Tualongo

175121325-5

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE CIENCIAS

CARRERA MATEMÁTICA

El Tribunal del Trabajo de Integración Curricular certifica que: El Trabajo de Integración Curricular; Tipo: Proyecto de Investigación. **ELABORACIÓN DE UNA MONOGRAFÍA SOBRE LA ELIMINACIÓN DE CUANTIFICADORES, DIRIGIDA A ESTUDIANTES DE LA CARRERA DE MATEMÁTICA DE LA ESPOCH**, realizado por el señor: **DARÍO GONZALO MATEHU TUALONGO**, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Integración Curricular, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Dra. Janneth del Rocío Morocho Yaucán **PRESIDENTE DEL TRIBUNAL**		2024-05-13
Dr. Leonidas Antonio Cerda Romero **DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2024-05-13
Dr. Ramón Antonio Abancín Espinosa **ASESOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**		2024-05-13

DEDICATORIA

A mis padres, Margarita del Rocío Tualongo y Gonzalo Matehu Gonzales, por su inagotable amor, apoyo, su dedicación y sacrificio han sido la base de mi formación y éxito académico, por inculcarme los valores del trabajo duro, la honestidad y la perseverancia. Sus consejos y respaldo constante han sido vitales en mi desarrollo personal y profesional. A mi hermano, Mateo Sebastián, cuya compañía y apoyo han sido una fuente constante de motivación y alegría. A mi familia en general, cuyo apoyo colectivo ha sido esencial para alcanzar este hito académico. Su fe en mí me ha dado la fortaleza para superar cada desafío. A todos ustedes, les dedico este trabajo con profunda gratitud y reconocimiento. Cada uno de ustedes ha jugado un papel esencial en mi vida, proporcionándome el apoyo, el amor y la inspiración necesarios para alcanzar esta meta. Sin ustedes, este logro no habría sido posible.

Darío

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas aquellas personas que han sido fundamentales para la culminación de esta tesis.

En primer lugar, a mi tutor, Leonidas Cerda, por su guía experta, paciencia y apoyo constante a lo largo de este proceso. Su dedicación y conocimientos han sido invaluables para la realización de este trabajo. A mis padres, Margarita Tualongo y Gonzalo Matehu, por su amor incondicional y su constante apoyo. Gracias por ser mi fuente de inspiración y por enseñarme el valor del esfuerzo y la perseverancia. A mi hermano, Mateo Sebastián, por su compañía y estímulo constante. Tu energía y apoyo han sido esenciales para mantenerme motivado. A mi amigo, Raúl Núñez, por su amistad y apoyo inquebrantable. Tu presencia y palabras de aliento han sido de gran ayuda durante este recorrido. Y finalmente, a toda mi familia, cuyo apoyo colectivo ha sido esencial para alcanzar este hito académico. Gracias por creer en mí y por estar siempre a mi lado. A todos ustedes, mi más profundo agradecimiento.

Darío

ÍNDICE DE CONTENIDO

ÍNDICE DE ANEXOS

RESUMEN

En la ESPOCH, no hay evidencia de la existencia de información sobre la eliminación de cuantificadores, lo cual dificulta a que estudiantes interesados en clasificar y construir estructuras matemáticas, puedan iniciar sus investigaciones. Por lo tanto, el objetivo de la presente investigación fue realizar un análisis de la teoría de eliminación de cuantificadores mediante la presentación de definiciones, ejemplos y demostración de teoremas, con el fin de elaborar una monografía que pueda servir como material bibliográfico para los estudiantes de la Carrera de Matemática de la ESPOCH, y a todas aquellas personas interesadas en comprender este tema. La metodología implementada tuvo un enfoque cualitativo y se utilizó un estudio descriptivo, con el fin de analizar y describir los tópicos más relevantes sobre eliminación de cuantificadores, y se aplicó un diseño de tipo documental, porque implicó un proceso basado en la búsqueda, recuperación y análisis crítico de contenidos relevantes. Mediante esta metodología se logró determinar que la técnica de eliminación de cuantificadores ayuda a simplificar utilizando en lógica matemática, teoría de modelos y teoría de la computación. Se pudó demostrar que ciertas teorías admiten eliminación de cuantificadores, haciendo más fácil demostrar que dichas teorías son decidibles, definibles y completas. En este contexto se concluye que la técnica de eliminación de cuantificadores sintentiza mucho el estudio de teorías que cuentan con propiedades tales como la decidibilidad, definibilidad y completitud.

Palabras clave: <MATEMÁTICA>, <LÓGICA>, <CUANTIFICADORES>, <TEORÍA DE MODELOS>, <MONOGRAFÍA>.

0723-DBRA-UT-2024

SUMARY/ABSTRACT

ESPOCH does not have any evidence on the existence of information regarding quantifier elimination, which impedes students interested in classifying and building mathematical structures to initiate their research. Therefore, the aim of this research was to perform an analysis on the theory of quantifier elimination by presenting definitions, examples and proof of theorems, in order to develop a monograph to be used as bibliographic material for students of Mathematics at ESPOCH, and all those students interested in understanding this topic. The methodology implemented had a qualitative approach and used a descriptive study to analyze and describe the most relevant topics on quantifier elimination. In addition, a documentary type design was applied, since it implied a process based on the search, recovery and critical analysis of relevant contents. By means of this methodology it was possible to determine that the quantifier elimination technique helpsin the simplification process mathematical logic, model theory and theory of computation. It was possible to evidence that certain theories admit quantifier elimination, making it easier to demonstrate that such theories are decidable, definable and complete. In this context it is concluded that the quantifier elimination technique greatly synthesizes the study of theories that have properties such as decidability, definability and completeness.

Keywords: <MATHEMATICS>, <LOGIC>, <QUANTIFIRS>, <MODEL THEORY>, <MONOGRAPH>.

Lic. Paul Rolando Armas Pesántez Mgs.

0603289877

INTRODUCCIÓN

La eliminación de cuantificadores es un tema de la lógica matemática y la teoría de modelos que tiene sus raíces en el siglo XIX y se ha desarrollado a lo largo del siglo XX. Los fundamentos de este campo se encuentran en los trabajos de matemáticos y lógicos como Gottlob Frege, Georg Cantor, David Hilbert y otros. El problema fundamental que aborda la eliminación de cuantificadores es cómo expresar afirmaciones matemáticas que involucran cuantificadores en términos de expresiones sin cuantificadores. Esto es relevante para la lógica y la matemática porque permite demostrar propiedades y relaciones entre objetos matemáticos de una manera más simple. Uno de los primeros pasos significativos en el estudio de la eliminación de cuantificadores fue el trabajo de Giuseppe Peano a fines del siglo XIX, que buscaba axiomatizar la aritmética y reducir las afirmaciones aritméticas a fórmulas lógicas más básicas.

El presente trabajo de investigacón se sumerge en el fascinante mundo de la eliminación de cuantificadores en el contexto de las teorías formales de primer orden. La idea fundamental detrás de este concepto es la capacidad de transformar cualquier fórmula de un lenguaje de primer orden, que haga uso de cuantificadores existenciales ($\exists$) o universales ($\forall$), en otra fórmula equivalente dentro de una teoría T específica, prescindiendo de dichos cuantificadores.
En términos más formales, la eliminación de cuantificadores se manifiesta como una propiedad deseable de una teoría T, demostrando que para cada fórmula de primer orden $\varphi(\vec{v})$ en el lenguaje de la teoría, existe, en el mismo lenguaje, una fórmula sin cuantificadores, representada por $\varphi'(\vec{v})$ y lógicamente a $\varphi(\vec{v})$. Esta propiedad está respaldada por la capacidad de la teoría para demostrar la equivalencia entre ambas fórmulas; es decir,

$$T \vdash \forall \vec{v}(\varphi(\vec{v}) \iff \varphi'(\vec{v})).$$

El interés en la eliminación de cuantificadores se enmarca en la búsqueda de una comprensión más profunda y eficiente de las teorías formales, permitiendo una representación más clara y manejable de sus propiedades. Este trabajo de investigación se embarca en explorar definiciones, teoremas y aplicaciones prácticas de la eliminación de cuantificadores, destacando su importancia en la lógica matemática y teoría de modelos. Además, este trabajo se presenta como un análisis académico para el entendimiento y la aplicación de la eliminación de cuantificadores, con el propósito de contribuir al conocimiento en lógica matemática y brindar una perspectiva integral a estudiantes, académicos y profesionales interesados en este campo de estudio.

CAPÍTULO I

1. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del Problema

La eliminación de cuantificadores presenta algunos desafíos debido a su abstracción matemática y su complejidad teórica. Para iniciar estudios sobre la técnica de eliminación de cuantificadores se requiere una comprensión profunda de la lógica matemática.
En la ESPOCH, no hay evidencia de la existencia de una monografía sobre la eliminación de cuantificadores, lo cual dificulta que estudiantes interesados en clasificar y construir estructuras matemáticas, puedan iniciar sus investigaciones.

1.2. Objetivos

1.2.1. *Objetivo General*

Analizar la teoría de eliminación de cuantificadores mediante la presentación de definiciones, ejemplos y demostración de teoremas con el fin de elaborar una monografía que pueda servir como material bibliográfico para los estudiantes de la Carrera de Matemática de la ESPOCH, y a todas aquellas personas interesadas en comprender este tema.

1.2.2. *Objetivos específicos*

- Aplicar técnicas de búsqueda de información que involucren la identificación de palabras clave, con el propósito de localizar fuentes bibliográficas relevantes sobre la eliminación de cuantificadores.
- Analizar la bibliografía hallada sobre eliminación de cuantificadores, mediante una lectura crítica, para seleccionar la bibliografía más relevante sobre la eliminación de cuantificadores.
- Determinar los contenidos más relevantes sobre la eliminación de cuantificadores, a través de un análisis crítico de contenidos, con el fin de resumir y sintetizar la información de manera más efectiva.
- Recopilar información precisa y detallada sobre la eliminación de cuantificadores, para posteriormente redactar una monografía que tendrá una estructura y metodología basada en "Monografía Guía"de (OBI, 2018).

- Redactar una monografía sobre eliminación de cuantificadores, utilizando el editor de texto LaTeX, con el fin de proporcionar un recurso completo y de alta calidad para los estudiantes de la carrera de matemática de la ESPOCH.

1.3. Justificación

La eliminación de cuantificadores es un tema fundamental en lógica matemática en general, y la teoría de modelos en particular. Este proyecto de titulación busca explorar a profundidad los resultados más relevantes en este campo, brindando una comprensión más sólida de las bases teóricas que sustentan importantes áreas de investigación. El presente Trabajo de Titulación pretende documentar y resaltar la teoría de eliminación de cuantificadores. Como producto final, se generará una monografía que servirá como referente y guía para los estudiantes de la carrera de matemática, facilitando su consulta en el futuro.

CAPÍTULO II

2. MARCO TEÓRICO

Dentro de la búsqueda selecta sobre la eliminación de cuantificadores se puede observar en varios libros (ver por ejemplo (David Marker, 2002), (Rene Cori y Daniel Lascar, 2006) y (María Manzano, 2006)) la mención de que el trabajo fundamental del matemático consiste en examinar estructuras, sugerir propiedades que puedan corresponder a éstas y preguntarse si dichas propiedades se satisfacen o no. Tras una lectura crítica, se puede observar la gran dificultad en entender el tema de eliminación de cuantificadores, ya que son temas muy abstractos y que se debe tener una amplia gama de conocimientos previos.

Las fórmulas lógicas que involucran cuantificadores añaden un nivel de complejidad que puede obstaculizar su análisis y manipulación. Los cuantificadores, ya sean universales o existenciales, introducen la idea de generalidad o existencia en las proposiciones lógicas, generando capas adicionales de abstracción y ambigüedad. Esto da lugar a desafíos que trascienden las fórmulas proposicionales más simples, ya que los cuantificadores tienen la capacidad de expresar relaciones entre variables y conjuntos de manera abstracta y amplia.

La dificultad tambien se presenta en la complejidad al acceso de información, pues la bibliografía escencial se encuentra en otros idiomas (inglés por lo general) lo que limita su estudio de una manera eficaz, ya que es un trabajo extra poder comprender la teoría en dicho idioma.

En (David Marker, 2002) la eliminación de cuantificadores se estudia en el capítulo 3, posterior al estudio de estructuras y teorías. La notación que utiliza es comprensiva y es muy similar a la de (Rene Cori y Daniel Lascar, 2006), lo cual ayuda a comprender mucho mejor la teoría, su análisis y estudio.

En (María Manzano, 2006) se trata la eliminación de cuantificadores en el capítulo 7, su estudio no es muy profundo; además, su notación es confusa y poco didáctica, lo que dificulta su entendimiento.

En (Annalisa Marcja y Carlo Toffalori, 2003) presenta la eliminación de cuantificadores en el capítulo 2, su notación es más comprensiva en comparación con (María Manzano, 2006), su estudio se basa en ejemplos y en algunas aplicaciones, las cuales serán analizadas en el transcurso de la redacción de la monografía que se realizará.

2.1. Elaboración de Monografía en Matemática

La elaboración de una monografá presenta un desafío significativo, por lo tanto, la planificación resulta crucial. Es fundamental que se inicie la redacción lo antes posible y se comunique con sus asesores ante cualquier dificultad que se presente.

Antes de iniciar el proceso de redacción de una monografía en Matemática se recomienda realizar una búsqueda exhaustiva de fuentes primarias y secundarias del tema que se va ha estudiar.

Según (OBI, 2018), en el ámbito de la Matemática, el título de la monografía tiene la capacidad de presentar de manera evidente el tema u objetivo del trabajo. Se aconseja que no sea excesivamente extenso y que cualquier aclaración necesaria se proporcione al inicio de la monografía. Además, se debe incluir una indicación clara de las áreas y técnicas matemáticas que se abordarán.

Al recopilar bibliografía especializada, se recomienda buscar fuentes que aborden tanto el tema de estudio como los obstáculos matemáticos específicos en relación con el tema que se está estudiando. La integración de estas técnicas fortalecen la argumentación y hacen que la monografía sea más accesible para las personas al que está dirigido.

La construcción de una monografía bien estructurada requiere no solo de una profunda indagación en la bibliografía especializada, sino también de la aplicación de herramientas y técnicas que mejoren la claridad y coherencia de los argumentos matemáticos.

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Descripción de enfoque, alcance, diseño, tipo, métodos, técnicas e instrumentos de investigación empleadas

El proyecto de investigación se centró en el análisis cualitativo, adoptando una perspectiva que implicó una selecta revisión bibliográfica sobre la eliminación de cuantificadores, utilizando como recurso libros cuidadosamente elegidos. En el marco de esta iniciativa, se llevó a cabo un estudio descriptivo, orientado a examinar detenidamente y describir con detalle los temas más relevantes relacionados con la eliminación de cuantificadores. Este enfoque se sustentó en la meticulosa elección de bibliografía destacada y especializada en la temática, con el propósito de asegurar una base sólida y comprensiva para el análisis.

El diseño que se aplicó es de tipo documental, porque implicó un proceso basado en la búsqueda, recuperación y análisis crítico de contenidos relevantes dentro del marco de una investigación cualitativa. En consecuencia, se aplicó mecanismos de búsqueda, recopilación, organización y análisis de la información relacionada con el tema en cuestión.

Dentro de está perspectiva, en está investigación se realizó las siguientes actividades.

i) Recopilación y organización de información relacionada con la eliminación de cuantificadores.

ii) Revisión del material bibliográfico recopilado en la etapa anterior. En está actividad, con el objetivo de identificar las mejores fuentes de consulta, el material bibliográfico se ordenó y clasificó, según los objetivos proporcionados en la investigación. Posteriormente, se analizó rigurosamente todas aquellas fuentes que son más significativas para la investigación.

iii) Redacción de la monografía con revisiones por capítulos específicamente, una vez comprendida la información seleccionada, se redactó los primeros borradores de cada capítulo correspondiente al tema de investigación, realizando revisiones en cada uno de ellos.

Los instrumentos que fueron utilizados en el trabajo de investigación abarcan tanto libros tradicionales como libros virtuales, bibliografía virtual y dispositivo electrónico (computadora), finalmente la monografía fue escrita con el editor de texto LaTeX, que es un sistema de composición tipográfica de alta calidad en la escritura para matemática.

CAPÍTULO IV

4. MARCO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Resultado derivado del trabajo de investigación

Como resultado derivado del trabajo de investigación, se obtuvo una monografía titulada "Dominando la lógica, una exploración de la eliminación de cuantificadores", las ideas y aportes que se estableció toman importancia y pueden ser consultadas por todas aquellas personas interesadas en estudiar la teoría investigada. Al analizar y comprender la informanción selecta, se realizó la redacción de los primeros borradores de cada capítulo correspondiente al tema de investigación, posterior se realizó la redacción de la monografía. La monografía está organizada en cinco capítulos:

- Capítulo 1: Lenguajes de primer orden y estructuras.
- Capítulo 2: Eliminación de cuantificadores.
- Capítulo 3: Ordenes lineales discretos y ordenes lineales densos.
- Capítulo 4: Campos algebraicamente cerrados
- Capítulo 5: Eliminación-pp de cuantificadores y módulos.

4.2. Procesamiento, análisis e interpretación de resultados

El interés por la eliminación de cuantificadores surgió antes del nacimiento oficial de la teoría de modelos, Lowenheim y Skolem presentaron procedimientos a principios del siglo XX que traducían fórmulas a una forma más simple, evitando los cuantificadores. Langford, en 1927, proporcionó ejemplos explícitos de eliminación de cuantificadores en algunas estructuras algebraicas concretas, específicamente en órdenes lineales discretos y densos. Los primeros resultados y los teoremas de Tarski enfatizaban la decibilidad como un objetivo clave.

La eliminación de cuantificadores se percibía como un paso hacia la decibilidad, con el tiempo, el énfasis en la decibilidad disminuyó es así que hubo un cambio hacia un creciente interés en la definibilidad como tema principal en la intersección entre Teoría de Modelos y la eliminación de cuantificadores. Es por ello que se destaca que la definibilidad se convirtió en el tema principal donde convergen la Teoría de Modelos y la eliminación de cuantificadores, no solo se trata de la decibilidad, sino también de cómo las estructuras pueden ser definidas de manera efectiva. También se observó que la Teoría de eliminación de cuantificadores es fundamental para establecer que las teorías son definibles y completas. Lo cual contempla el estudio de propiedades de una manera más sencilla y factible.

El proyecto de invetigación generó una monografía que está estructurada en 5 capítulos, los cuales son organizados de acuerdo a la necesidad de comprensión y de la complejidad de los temas. Por ende el primer capítulo consta de preliminares y un estudio de la lógica, donde se abordaron temas tales como, lenguajes de primer orden, estructuras y teorías. El segundo capítulo es el tema central y primordial, pues se estudia la teoría de eliminación de cuantificadores, donde se estudia las definiciones así como también un lema fundamental para reducir fórmulas y establecer cómo una teoría admite eliminación de cuantificadores. Los capítulos tercero, cuarto y quinto estan dedicados a ilustrar varios ejemplos clave de eliminación de cuantificadores, empezando por los más antiguos (los resultados de Langford sobre los órdenes lineales discrétos o densos) hasta llegar a los que probablemente sean los más clásicos y célebres (los procedimientos de eliminación de Tarski para los campos reales y complejos). Se trató también otros conjuntos de eliminaciones (en particular, la eliminación de pp-fórmulas para módulos sobre un anillo dado).

Para obtener información más detallada sobre la monografía, se recomienda consultar el Anexo A.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Luego de culminar el trabajo de investigación se pueden ver algunas conclusiones:

1. La aplicación de técnicas de búsqueda de información que incluyan la identificación de palabras clave fue esencial para localizar fuentes bibliográficas pertinentes sobre la eliminación de cuantificadores. Al utilizar palabras clave específicas relacionadas con el tema, se optimizó la búsqueda y se aumentó las probabilidades de encontrar información relevante. Este enfoque permitió centrarse en el estudio directamente relacionada con la eliminación de cuantificadores en lugar de explorar ampliamente temas no pertinentes.

2. El análisis crítico de la bibliografía sobre eliminación de cuantificadores ha llevado a la identificación y selección de las fuentes más relevantes y valiosas para la investigación. Este proceso no solo contribuyó a la calidad y solidez del estudio, sino que también orientó la investigación hacia áreas específicas de interés y relevancia en el ámbito de la eliminación de cuantificadores.

3. El proceso de determinar los contenidos más relevantes implicó una evaluación crítica, selección cuidadosa y síntesis eficiente de la información relacionada con la eliminación de cuantificadores.

4. La combinación de una recopilación detallada de información sobre la eliminación de cuantificadores y la implementación de la metodología del libro "Monografía Guía"de (OBI, 2018) estableció un sólido fundamento para la redacción de la monografía académica estructurada y metodológicamente respaldada.

5. La elaboración de una monografía sobre la eliminación de cuantificadores representará un valioso recurso para los estudiantes de la carrera de matemática en la ESPOCH. La monografía se presenta como un documento completo y de alta calidad que servirá como guía integral para comprender y aplicar los procedimientos relacionados con la eliminación de cuantificadores en el contexto de la Teoría de Modelos.

5.2. Recomendaciones

Como recomendación final, se sugiere profundizar en otras teorías y algoritmos que complementen y enriquezcan la comprensión de la eliminación de cuantificadores. De igual modo se sugiere lo siguiente:

1. Aplicar técnicas de búsqueda de información que incluyan la identificación de palabras clave, ya que este enfoque ayudó a optimizar la búsqueda y aumentó las probabilidad de encontrar información relevante.

2. Realizar un análisis crítico de la bibliografía de los temas de investigación para identificar y seleccionar las fuentes más relevantes. Este proceso contribuirá a la calidad y solidez del estudio, además de orientar la investigación hacia áreas específicas de interés y relevancia.

3. Llevar a cabo una evaluación crítica, una selección selecta y una síntesis de la información. Esto permitirá determinar los contenidos más importantes.

4. Seguir el enfoque presentado en el texto "Monografía Guía"de (OBI, 2018), para la redacción de la monogafía. De esta forma se tiene un sólido fundamento metodológico para la escritura de una monografía de matemática.

5. Utilizar el editor de texto LaTeX para la elaboración de la monografía. Ya que este software se caracteríza por generar documentos de alta calidad, sobre todo en ambientes que manejan gran catidad de fórmulas matemáticas.

Bibliografía

1. **CHANG Chen & KEISLER H. Jerome.***Model Theory.* Third edition. New York, USA: Elsevier Science Pubilisher B.V. 1990. págs. 49-60.

2. **CORI, Rene & LASCAR, Daniel**. *Mathematical Logic.* University of London: Editorial Oxford, 2006. págs. 112-135.

3. **HODGES Wilfrid**. *Model Theory.* Universyty of London: Editorial Board 1993. págs. 66-75.

4. **MANZANO María**. *Model Theory*. New York, USA: Editorial Oxford, 2006. págs. 203-218.

5. **MARKER David**. *Model Theory An Introduction*. University of Illinois, Chicago, USA: Editorial Board, 2002. págs. 71-104

6. **MIJAJLOVIC Zarko**. *An introduction to model theory.*, University of Novi Sad Institute of Mathematics, Yugoslavia: University of Novi Sad, 1987. págs. 3-24.

   OBI.

7. *Monografía Guía*. Ginebra, Suiza: Organización del Bachillerato Internacional, 2018. págs. 303-307.

8. **TENT Katrin & ZIEGLER Martin**. *A Course in Model Theory.* Department of Mathematics, Cornell University, Ithaca: Editorial Board 2012. págs. 27-37.

9. **TOFFALORI, Carlo & MARCJA, Annalisa**. *A Guide To Classical and Modern Model Theory.* University of Flrence, Italy: Editorial Kluwer Academic Publishers, 2003. págs. 5-75.

ANEXOS

ANEXO A: DOMINANDO LA LÓGICA: UNA EXPLORACIÓN DE LA ELIMINACIÓN DE CUANTIFICADORES.

DOMINANDO LA LÓGICA:

UNA EXPLORACIÓN DE LA ELIMINACIÓN DE CUANTIFICADORES

DARIO MATEHU

Resumen

En la ESPOCH, no hay evidencia de la existencia de información sobre la eliminación de cuantificadores, lo cual dificulta que estudiantes interesados en clasificar y construir estructuras matemáticas, puedan iniciar sus investigaciones, por lo tanto, el objetivo de la presente investigación fue realizar un análisis de la teoría de eliminación de cuantificadores mediante la presentación de definiciones, ejemplos y demostración de teoremas con el fin de haber elaborado una monografía que pueda servir como material bibliográfico para los estudiantes de la Carrera de Matemática de la ESPOCH, y a todas aquellas personas interesadas en comprender este tema. La metodología implementada tuvo un enfoque cualitativo y se utilizó un estudio descriptivo, con el fin de analizar y describir los tópicos más relevantes sobre eliminación de cuantificadores, y se aplicó un diseño de tipo documental, porque implicó un proceso basado en la búsqueda, recuperación y análisis crítico de contenidos relevantes. Mediante esta metodología se logró determinar que la técnica de eliminación de cuantificadores ayuda a simplificar utilizando en lógica matemática, teoría de modelos y teoría de la computación. Se pudó demostrar que ciertas teorías admiten eliminación de cuantificadores, haciendo más fácil demostrar que dichas teorías son decidibles, definibles y completas. En este contexto se concluye que la técnica de eliminación de cuantificadores sintentiza mucho el estudio de teorías que cuentan con propiedades tales como la decidibilidad, definibilidad y completitud.

Abstract

ESPOCH does not have any evidence on the existence of information regarding quantifier elimination, which impedes students interested in classifying and building mathematical structures to initiate their research. Therefore, the aim of this research was to perform an analysis on the theory of quantifier elimination by presenting definitions, examples and proof of theorems, in order to develop a monograph to be used as bibliographic material for students of Mathematics at ESPOCH, and all those students interested in understanding this topic. The methodology implemented had a qualitative approach and used a descriptive study to analyze and describe the most relevant topics on quantifier elimination. In addition, a documentary type design was applied, since it implied a process based on the search, recovery and critical analysis of relevant contents. By means of this methodology it was possible to determine that the quantifier elimination technique helpsin the simplification process mathematical logic, model theory and theory of computation. It was possible to evidence that certain theories admit quantifier elimination, making it easier to demonstrate that such theories are decidable, definable and complete. In this context it is concluded that the quantifier elimination technique greatly synthesizes the study of theories that have properties such as decidability, definability and completeness.

Introducción

La lógica matemática y la teoría de modelos se han beneficiado significativamente de la evolución de conceptos y técnicas que permiten abordar de manera más eficiente y profunda la expresión de proposiciones cuantificadas. Entre estas, la eliminación de cuantificadores ha emergido como un área fundamental que desempeña un papel crucial en la simplificación y comprensión de enunciados matemáticos complejos. La capacidad de encontrar fórmulas que involucran cuantificadores universales y existenciales, a fórmulas sin dichos cuantificadores han revolucionado la resolución de problemas y la demostración de teoremas.

Esta monografía se sumerge en el mundo de la eliminación de cuantificadores, explorando técnicas y herramientas utilizadas para transformar afirmaciones lógicas cuantificadas en fórmulas equivalentes sin cuantificadores.

Se examinará la relación entre la eliminación de cuantificadores y la teoría de orden lineal discreto, que proporciona herramientas para entender las estructuras ordenadas discretas y sus propiedades fundamentales. Además, exploraremos su conexión con la teoría de orden lineal denso, ofreciendo perspectivas adicionales para la resolución de problemas cuantificativos en entornos más amplios. También se estudiará la aplicación de la eliminación de cuantificadores en campos algebraicamente cerrados, destacando cómo esta técnica ha permitido simplificar y clarificar los enunciados en este contexto específico. Se abordará las pp-fórmulas, profundizando en su relevancia y aplicación en la eliminación de cuantificadores, ofreciendo así una visión más completa y detallada de los elementos que componen este intrigante campo de estudio.

Índice general

1. Lenguajes de primer orden y estructuras

1.1 Lenguaje de primer Orden

El trabajo fundamental del matemático es examinar estructuras, sugerir propiedades que podrían pertenecer a ellas y preguntar si estas propiedades se satisfacen o no [4].

En la lógica matemática, los lenguajes de primer orden juegan un papel fundamental en el análisis y la descripción de diversas estructuras matemáticas. Aunque en esta sección nos detendremos en explicar detalladamente cada uno de estos conceptos, proporcionaremos una primera comprensión de los mismos.

En términos generales, podríamos afirmar que una estructura matemática consiste en un conjunto (sobre el cual hay interés de estudio) equipado con una serie de funciones, relaciones y elementos destacados. Después, se elige un lenguaje adecuado mediante el cual se analice el comportamiento de dichas funciones, relaciones y elementos destacados en el conjunto bajo estudio.

Un ejemplo de estructura bastante simple podría ser $(\mathbb{N},+,0,1)$, que está formada por el conjunto de números naturales y la función de suma, junto con 0 y 1 como elementos destacados. Para estudiar esta estructura, se selecciona un lenguaje apropiado que incluya el símbolo de una función binaria (para la suma) y otros dos símbolos para las constantes 0 y 1. Gracias a la elección de este lenguaje, es posible formular enunciados como:

$$\forall x(x = 0 \lor \exists y(x = y + 1)),$$

que puede interpretarse como la afirmación de que "todo número natural diferente de 0 es el sucesor de otro número natural".

Este pequeño ejemplo resalta tanto el interés como la utilidad de los lenguajes al describir propiedades de las estructuras matemáticas. A partir de aquí, introduciremos algunas definiciones básicas.

No habrá un alfabeto único sino más bien un alfabeto apropiado, llamado **lenguaje**, para cada tipo de estructura bajo consideración. Por estructura entendemos un conjunto M no vacío, provisto de lo siguiente:

Un cierto número de elementos distinguidos; para cada entero positivo p, un cierto número de relaciones de $p - lugar$ en M; y para cada entero positivo p, un cierto número de funciones de M^P a M.

Obviamente, no usaríamos el mismo lenguaje para hablar, por ejemplo, de grupos y de conjuntos ordenados.

Definición 1.1 — Lenguaje de primer orden.

Un lenguaje de primer orden es un conjunto L de símbolos compuesto por dos partes:

a) La primera parte, comun a todos los lenguajes, consiste por un lado de un conjunto infinito numerable.

$$\mathscr{V} = \{v_0, v_1, ..., v_n, ...\}$$

de elementos llamados **símbolos de variables**.

Por otro lado los siguientes símbolos

a_1) Los paréntesis: $), ($ y

los símbolos para los conectores: $\wedge, \vee, \Rightarrow, \iff$, además

el símbolo de negación: $\neg$

a_2) Dos nuevos símbolos que son:

$\forall$ **para todo**, el cuantificador universal; y

$\exists$ **existe por lo menos uno**, el cuantificador existencial.

Cada uno de estos cuantificadores se llama el dual de otro.

b) Segunda parte: Puede variar de un lenguaje a otro.

Es la unión de un conjunto $\mathscr{C}$ y de dos sucesiones de conjuntos $(\mathscr{F}_n)_{n\in\mathbb{N}^*}$ y $(\mathscr{R}_n)_{n\in\mathbb{N}^*}$ disjuntas por pares y toda disjunta de $\mathscr{C}$.

Los elementos de $\mathscr{C}$ se llaman **símbolos constantes**.

b_1) Para cada entero $n \geq 1$, los elementos de $\mathscr{F}_n$ se denominan $n - lugar$(o $n - ario$) o de aridad n, o con n argumentos. Símbolos de funciones (o funcionales). Y los elementos de $\mathscr{R}_n$ se llaman de aridad n, símbolos de relación (o predicados).

Se dice unario, binario y ternario respectivamente, $1 - ario$, $2 - ario$, $3 - ario$

b_2) Considere el símbolo $\simeq$ llamado **símbolo igualdad**.

En un lenguaje de primer orden, es un elemento de $\mathscr{R}_2$, *i.e.* un símbolo de relación binaria.

El lenguaje que contiene este símbolo se denomina lenguaje con igualdad.

Así, tener un lenguaje de primer orden, L es definir las dos sucesiones $(\mathscr{R}_n)_{n\in\mathbb{N}^*}$ y

$(\mathscr{F}_n)_{n\in\mathbb{N}^*}$ y considerar el conjunto

$$\mathscr{L} = \mathscr{V} \cup \{),(,\neg,\wedge,\vee,\Rightarrow,\iff,\forall,\exists\} \cup \mathscr{C} \cup (\mathscr{F}_n)_{n\in\mathbb{N}^*} \cup (\mathscr{R}_n)_{n\in\mathbb{N}^*}$$

Los símbolos para las constantes, las funciones y relaciones son llamadas

símbolos no lógicos.

▪ **Ejemplo 1.1** Consideremos el lenguaje $\mathscr{L} = \{R,c,f,g\}$ donde R es un símbolo de relación binaria, c es un símbolo constante, y f,g son dos símbolos de función unarios.

▪ **Ejemplo 1.2** Consideremos el lenguaje $\mathscr{L} = \{f,g,c_1,c_2\}$ donde f es un símbolo de función binaria y g un símbolo de función ternario, c_1 y c_2 son símbolos constante.

Conjunto de términos

Definición 1.2 — Conjunto de términos,definición desde arriba.

El conjunto $\mathscr{T}(\mathscr{L})$ de

términos del lenguaje es el subconjunto más pequeño $\mathscr{W}(\mathscr{L})$ que

a) Contiene las variables y los símbolos constantes, es decir $\mathscr{V} \cup \mathscr{C}$

b) Es cerrado bajo la operación

$$(m_1,m_2,...,m_n) \longmapsto fm_1m_2...m_n$$

para todo entero positivo $m \geq 1$ y cada elemento $f \in \mathscr{F}_n$.

En otras palabras, los términos son palabras que se pueden obtener aplicando las siguientes reglas, un número finito de veces.

- Los símbolos de variables y constantes son términos.
- Si $m \in \mathbf{N}^*$, si f es un símbolo de función $n-ario$ de $\mathscr{L}$, y si $t_1,t_2,...,t_n$ son

términos, entonces la palabra

$$ft_1, t_2, \ldots, t_n$$

es un término.

Definición 1.3 — Conjunto de términos, definición desde abajo.

$$\mathscr{T}_0(\mathscr{L}) = \mathscr{V} \cup \mathscr{C}$$

Para cada entero $k \geq 1$, fijemos

$$\mathscr{T}_{n+1} = \mathscr{T}_k(\mathscr{L}) \cup \bigcup_{n \in \mathbf{N}^*} \{ft_1 t_2 \ldots t_n : f \in \mathscr{F}_n, t_1 \in \mathscr{T}_k(\mathscr{L}), t_2 \in \mathscr{T}_k(\mathscr{L}) \ldots, t_n \in \mathscr{T}_k(\mathscr{L})\}$$

■ **Ejemplo 1.3** Sea el lenguaje $\mathscr{L} = \{0, 1, +, \cdot\}$ donde $+$ y $\cdot$ son símbolos de función binarios y $0, 1$ constantes entonces sea el término $+1 + 1 \cdot 01$.

Definición 1.4 — Altura de un término.

La altura de un térmio $t \in\in \mathscr{T}(\mathscr{L})$ es el menor entero k tal que $t \in \mathscr{T}_k(\mathscr{L})$

■ **Ejemplo 1.4** Sea $\mathscr{L}$ un lenguaje que tiene un símbolo constante c, un símbolo de función unario f y un símbolo de función g ternario. Considere la palabra

$$W = ggffv_0gv_2v_0cfcffgfcgv_2fv_0ffcfcfc$$

su altura es $h[W] = 7$

Definición 1.5 — Fórmulas atómicas.

Una palabra $W \in \mathscr{W}(\mathscr{L})$ es una fórmula atómica si y sólo si existe un número natural

$n \in \mathbb{N}^*$, un símbolo de relación $n-ario$ R, y un término $t_1, \ldots t_n$, del lenguaje L tal que

$$W = Rt_1t_2 \ldots t_n$$

En el caso donde L es un lenguaje con igualdad y t, u son términos arbitrarios en $\mathscr{T}(L\mathscr{L})$, se escribe

$$t \simeq u$$

para la fórmula atómica $\simeq tu$

Denotaremos el conjunto de fórmulas atómicas del lenguaje L por $At(\mathscr{L})$.

■ **Ejemplo 1.5** Sea $\mathscr{L} = \{v_0, v_1, R\}$ donde v_0,v_1 son símbolos de variables y R símbolo de relación binaria. Entonces la fórmula atómica es:

$$F = Rv_0v_1$$

Definición 1.6 — Conjunto de fórmulas.

El conjunto $\mathscr{F}(\mathscr{L})$ de fórmulas del lenguaje (de primer orden) $\mathscr{L}$ es el subconjunto más pequeño de $\mathscr{W}(\mathscr{L})$ que

a) Contiene todas las fórmulas atómicas.

b) Siempre que contenga dos palabras V y W también contiene las palabras

$$\neg W, (V \alpha W) \qquad \text{donde} \quad \alpha \in \{\wedge, \vee, \rightarrow, \longleftrightarrow\}$$

y, para todo número natural n, las palabras $\forall v_n W$ y $\exists v_n W$.

Dadas dos fórmulas F y G en $\mathscr{F}(\mathscr{L})$ las fórmulas $\neg F, (F \wedge G), (F \vee G)$ se llaman respectivamente, la negación de la fórmula F, la conjunción de las fórmulas F y G y la disjunción de las fórmulas F y G.

Toda fórmula es una palabra, el recíproco no es cierto.

■ **Ejemplo 1.6** Sea $\mathscr{L} = \{v_0, v_1, , v_2, c, f, R\}$ donde v_0,v_1 son símbolos de variables, R símbolo de relación binaria, f símbolo de función unario. Entonces la fórmula es:

$$F = \forall v_0(\exists v_1 \forall v_0(Rv_1v_0 \to \neg v_0 \simeq v_3) \wedge \forall v_2(\exists v_2(Rv_1v_2 \vee fv_0 \simeq c) \wedge v_2 \simeq v_2))$$

Variables libres, variables acotadas y fórmulas cerradas

Definición 1.7 — Ocurrencias libres y acotadas.

Dado un $k \in \mathbb{N}$ y una fórmula $F \in \mathscr{F}(\mathscr{L})$ las ocurrencias, si las hay, de las variables de v_k en la fórmula F pueden ser de dos clases: libres y acotadas.

Se procede por inducción

a) Si F es atómica, entonces las ocurrencias de v_k en F son libres.

b) Si $F = \neg G$, las ocurrencias libres de v_k en F son las ocurrencias libres de v_k en G.

c) Si $F = (G\alpha H)$, donde $\alpha \in \{\vee, \wedge, \to, \longleftrightarrow\}$, las ocurrencias libres v_k en F son las ocurrencias libres de v_k en G y las ocurrencias libres de v_k en H

d) Si $F = \forall v_h G$ o si $\exists v_h G$ para $h \neq k$, las ocurrencias libres de v_k en F son las ocurrencias libres de v_k en G.

e) Si $F = \forall v_k G$ o si $\exists v_k G$ ninguna de las ocurrencias de v_k en F es libre.

Las ocurrencias de v_k en F que no son libres se llaman acotadas.

Veamos las siguientes notas

1. *Con respecto al paso de G a la fórmula $\forall v_k G$ se tiene que las variables v_k ha sido*

universalmente cuatificada.

2. *Con respecto al paso de G a la fórmula $\exists v_k G$ se tiene que las variables v_k ha sido universalmente cuatificada.*

Ejemplo 1.7

1. Sea $\mathscr{L} = \{v_0, v_1, v_2, c, f, R\}$ donde v_0,v_1 son símbolos de variables, R símbolo de relación binaria, f símbolo de función unario. Entonces la fórmula es:

   $$F = \forall v_0(\exists v_1 \forall v_0(Rv_1v_0 \to \neg v_0 \simeq v_3) \wedge \forall v_2(\exists v_2(Rv_1v_2 \vee fv_0 \simeq c) \wedge v_2 \simeq v_2))$$

   En F, todas las ocurrencias de v_0 y todas las ocurrencias de v_2 están acotadas; las dos primeras ocurrencias de v_1 están acotadas mientras que la tercera está libre; por último, la única ocurrencia de v_3 está libre.

2. El campo ordenado de los números reales está completamente axiomatizado por las siguientes propiedades:

   Axiomas de campo:

   a) $\forall v_1 \forall v_2 \forall v_3[(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$

   b) $\forall v_1(v_1 + 0 = v_1 \wedge v_1 = 0 + v_1)$

   c) $\forall v_1 \exists v_2(v_1 + v_2 = 0)$

   d) $\forall v_2(v_1 + v_2 = v_2 + v_1)$

   e) $\forall v_1 \forall v_2 \forall v_3[(v_1 \cdot v_2) \cdot v_3 = v_1 \cdot (v_2 \cdot v_3)]$

   f) $\forall v_1(v_1 \cdot 1) = v_1 \wedge v_1 = (1 \cdot v_1)$

   g) $\forall v_1(v_1 \neq 0) \to \exists v_2(v_1 \cdot v_2) = 1)$

   h) $\forall v_2(v_1 \cdot v_2) = v_2 \cdot v_1)$

   i) $\forall v_1 \forall v_2 \forall v_3(v_1(v_2 + v_3)) = v_1 \cdot v_2 + v_1 \cdot v_3)$

   Axiomas de orden:

j) $\forall v_1 \forall v_2 (v_1 < v_2 \vee v_1 = v_2 \vee v_2 < v_1)$

k) $\forall v_1 \forall v_2 \forall v_3 ((v_1 < v_2 \wedge v_2 < v_3)) \to v_1 < v_3$

l) $\forall v_1 \forall v_2 \forall v_3 (v_1 < v_2 \to v_1 + v_3 < v_2 + v_3)$

m) $\forall v_1 \forall v_2 \forall v_3 ((v_1 < v_2 \wedge v_3 > 0)) \to v_1 \cdot v_3 < v_2 \cdot v_3$

n) $\forall v_1 \forall v_2 \forall v_3 ((v_1 < v_2 \wedge v_3 < 0)) \to v_2 \cdot v_3 < v_1 \cdot v_3$

Completitud:

$\forall S \subseteq \mathbb{R}[\exists v_1 (v_1 \in S) \wedge \exists v_2 \forall v_1 (v_1 \in S \to v_1 < v_2) \to \exists v_3 \forall v_1 (\exists t (t \in S \wedge v_1 < t) \vee v_1 = v_3 \vee v_1 < v_3)]$

De estas propiedades, solamente la última (axioma de completitud) no parece ser expresable en primer orden porque cuantifica sobre subconjuntos de los reales, y utiliza el símbolo $\in$ que no estaba en el lenguaje de primer orden.

Definición 1.8 — Variables libres, Fórmula Cerrada.

1. Las variables libres en una fórmula $F \in \mathscr{F}(\mathscr{L})$ son aquellas variables que tienen al menos una ocurrencia libre en F.
2. Una fórmula cerrada: Es aquella en la que no hay variables libres.

Notación

Dado una fórmula $F \in \mathscr{F}(\mathscr{L})$ y números naturales distintos por pares $i, i_2, \ldots, i_n$, se usará la notación $F[v_i, v_{i_2}, \ldots, v_{i_n}]$, para identificar que las variables libres de la fórmula F están entre

$$v_i, v_{i_2}, \ldots, v_{i_n}$$

Como es el caso para los términos, se debe notar que cada fórmula $F \in \mathscr{F}(\mathscr{L})$, existe un *entero n tal que*

$$F = F(v_0, v_1, \ldots, v_n) = F(\vec{v}) \quad donde \quad \vec{v} = (v_0, v_1, \ldots, v_n)$$

Definición 1.9

Dada la fórmula $F = F(v_i, v_{i_2}, \ldots, v_{i_n})$ del lenguaje $\mathscr{L}$ en cada una de las variables $v_i, v_{i_2}, \ldots, v_{i_n}$ tiene al menos una ocurrencia libre, la fórmula

$$\forall v_i, \forall v_{i_2}, \ldots, \forall v_{i_n}$$

y todas las fórmulas similares obtenidas permutando el orden de las variables $v_i, v_{i_2}, \ldots, v_{i_n}$ son cuantificadas se denominan cierres universales de F.

Notación

Consideremos la ocurrencia en una fórmula de cuantificadores Q_v, donde Q denota $\forall$ o $\exists$, y v la variable que necesariamente sigue a Q en F.

$$Q_v \rightarrow \forall v G \qquad Q_v \rightarrow \exists v G$$

la palabra Q_v es seguida por una subfórmula G de F.

1.2 Estructuras

La palabra estructura en el contexto de la matemática se refiere comúnmente a un conjunto en el cual se definen un conjunto específico de funciones, relaciones (u operaciones internas), y a veces incluye elementos que son considerados como "distinguidos".

Un ejemplo de esto sería el campo ordenado de los números reales es la estructura

$$(\mathbb{R}, \leq, +, \cdot, 0, 1)$$

Una estructura en matemática es una conjunto donde se define un cierto número de funciones y relaciones, junto con elementos que se denominan distinguidos.

■ **Ejemplo 1.8** El campo ordenado de los número reales

$$(\mathbb{R}, \leq, +, \times, 0, 1)$$

El grupo aditivo de enteros es la estructura

$$(\mathbb{Z}, +, 0)$$

Modelos de un lenguaje

Consideremos un lenguaje de primer orden $\mathscr{L}$ que no es necesariamente un lenguaje con igualdad.

Definición 1.10 — Modelo.

Un modelo del lenguaje $\mathscr{L}$, o $\mathscr{L}-estructura$, es una estructura $\mathfrak{M}$ consistiendo de

a) Un conjunto M no vacío, llamado el dominio o el conjunto base o el conjunto **subyacente** de la estructura $\mathfrak{M}$.

b) Para cada símbolo constante c de $\mathscr{L}$ un elemento $c^{\mathfrak{M}}$ de M, llamado interpretación del símbolo c en el modelo $\mathfrak{M}$.

c) Para todo número natura $k \geq 1$ y para cada símbolo de función $k-ario$, f de $\mathscr{L}$, una aplicación $f^{\mathfrak{M}}$ de M^k en M (es decir, una operación $k-aria$ en el conjunto M, llamado interpretación del símbolo f en el modelo $\mathfrak{M}$.

d) Para todo número natura $k \geq 1$ y para cada símbolo de relación $k-ario$ R de $\mathscr{L}$, un subconjunto $R^{\mathfrak{M}}$ de M^k (es decir una relación $k-aria$ en el conjunto M)

llamado interpretación del símbolo R en el modelo $\mathfrak{M}$.

e) En el caso donde L es un lenguaje con igualdad, se dice que el modelo $\mathfrak{M}$ respeta la igualdad, si $\simeq^{\mathfrak{M}}$ la interpretación en $\mathfrak{M}$ de símbolo de iguadad en M.(Es decir es el conjunto $\{(a,b) \in M^2 : a = b\}$, tambien llamado la **diagonal de** M^2).

Veamos las siguientes notas:

1. *Se denotara los modelos por letras caligraficas $\mathfrak{M}, \mathfrak{N}, \ldots$ y para el conjunto base letra latina $M, N, ..$*
2. *La $\mathscr{L}-estructura$ $\mathfrak{M}$ se suele denotar:*

$$\mathfrak{M} = (M; (c^{\mathfrak{M}})_{c \in \mathscr{L}}, (f^{\mathfrak{M}})_{f \in \mathscr{L}}, (R^{\mathfrak{M}})_{R \in \mathscr{L}})$$

■ **Ejemplo 1.9** Sea el lenguaje $\mathscr{L} = \{R, f, c\}$ donde R es un símbolo de relación binario, f un símbolo de función unario y c una constante, podemos denotar el siguiente modelo

$$\mathfrak{N} = (\mathbb{R}, \leq, \cos, \pi).$$

Homomorfismos e isomorfismos

Consideremos en el lenguaje $\mathscr{L}$, sean $\mathfrak{M} = (M; \ldots)$ y $\mathfrak{N} = (N; \ldots)$ dos $\mathscr{L}-estructuras$ y sea φ una aplicacion de M a N.

Definición 1.11 — Homomorfismo.

La aplicacion φ es un homomorfismo de $\mathscr{L}-estructura$ de $\mathfrak{M}$ en $\mathfrak{N}$ si y solo si se cumple las siguientes condiciones

a) Para cada simbolo constante c de $\mathscr{L}$

$$\varphi(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$$

b) Para cada numero natural $n \geq 1$ para cada simbolo de funcion $n-ario$ f y para todos los elementos $a_1, a_2 \ldots a_n \in M$

$$\varphi(f^{\mathfrak{M}}(a_1, a_2 \ldots a_n)) = f^{\mathfrak{N}}(\varphi(a_1), \ldots, \varphi(a_n))$$

c) Para cada numero natural $k \geq 1$ para cada simbolo de relacion $k-ario$ R de L y para todos los elementos $a_1, a_2 \ldots a_n \in M$, si $(a_1, a_2 \ldots a_n) \in R^{\mathfrak{M}}$ entonces

$$(\varphi(a_1), \ldots, \varphi(a_n)) \in R^{\mathfrak{N}}$$

Asi, un homomorfismo de una $\mathscr{L}-estructura$ a otra es una aplicacion del conjunto base del primero en el conjunto base que respeta todas las relaciones, funciones y constantes de otras estructuras.

Decimos que φ es llamado **incrustación** de $\mathfrak{M}$ en $\mathfrak{N}$ si φ es inyectiva y por (c), $(\varphi(a_1), \ldots, \varphi(a_n)) \in R^{\mathfrak{N}}$ implica $(a_1, \ldots, a_n) \in R^{\mathfrak{M}}$ para todo $a_1, \ldots, a_n \in M$. Cuando hay alguna incrustación de $\mathfrak{M}$ en $\mathfrak{N}$, escribimos $\mathfrak{M} \subseteq \mathfrak{N}$

■ **Ejemplo 1.10**

1. La aplicación $n \longmapsto (-1)^n$ es un homomorfismo de la estructura $(\mathbb{Z}, 0, +)$ a la estructura $(\{-1, 1\}, 1, \cdot)$.
2. La aplicación $\begin{array}{ccc} 0 & \longmapsto & 0 \\ 1 & \longmapsto & 2 \end{array}$ es un homomorfismo de la estructura $(\mathbb{Z}_2, 0, +)$ a la estructura $(\mathbb{Z}_4, 0, +)$.

Definición 1.12 — Monomorfismo.

Un monomorfismo de $\mathscr{L}-estructura$ de $\mathfrak{M}$ en $\mathfrak{N}$ es un homomorfismo de $\mathfrak{M}$ en $\mathfrak{N}$ que tiene la siguiente propiedad

a) Para cada numero natural $k \geq 1$, para cada simbolo de relacion $k-ario$ R de $\mathscr{L}$ y para todos los elementos $a_1, a_2 \dots a_n \in M$,

$$(a_1, a_2 \dots a_n) \in R^{\mathfrak{M}} \quad \text{si y solo si} \quad (\varphi(a_1), \dots, \varphi(a_n)) \in R^{\mathfrak{N}}$$

Lema 1.2.1 Cada monomorfismo es inyectivo.

Demostración. Debemos recordar aquí que solo estamos considerando lenguajes con igualdad y modelos que respetan la igualdad.

Si φ es un monomorfismo de M en N, la propiedad de la definición 1.12 aplicada al símbolo de igualdad $\simeq$ muestra que para todos los elementos a y b de M, tenemos

$$(a, b) \in R^{\mathfrak{M}} \quad \text{si y solo si} \quad (\varphi(a), \varphi(b)) \in R^{\mathfrak{N}}$$

es decir que $a = b$ si y sólo si $\varphi(a) = \varphi(b)$. ■

Definición 1.13 — Isomorfismo.

Un isomorfismo de una $\mathscr{L}-estructura$ $\mathfrak{M}$ sobre otra $\mathscr{L}-estructura$ $\mathfrak{N}$ es un monomorfismo de $\mathfrak{M}$ en $\mathfrak{N}$ que es sobreyectiva.

Definición 1.14 — Automorfismo.

Un automorfismo de $\mathscr{L}-estructura$ $\mathfrak{M}$ es un isomorfismo de $\mathfrak{M}$ sobre $\mathfrak{M}$

Definición 1.15 — Estructuras isomorfas.

Si existe un isomorfismo entre dos estructuras, se dicen que son isomorfos.

Definición 1.16 — Satisfacción de las fórmulas de una estructura.

Consideremos $\mathfrak{M}$ una cierta $\mathscr{L}-$estructura y sea F una fórmula de $\mathfrak{M}$ con variables libres $\vec{v} = (v_{i_1}, \ldots, v_{i_m})$ y $\vec{a} = (a_{i_1}, \ldots, a_{i_m})$ elementos de M. Inductivamente definimos $\mathfrak{M} \models F(\vec{a})$ como sigue:

1. Si F es de la forma $t_1 = t_2$, entonces, $\mathfrak{M} \models F(\vec{a})$ si $t_1^{\mathfrak{M}}(\vec{a}) = t_2^{\mathfrak{M}}(\vec{a})$, con t_1, t_2 términos.
2. Si F es de la forma $R(t_1, \ldots, t_n)$, entonces,

   $\mathfrak{M} \models F(\vec{a})$ si $(t_1^{\mathfrak{M}}(\vec{a}), \ldots, t_n^{\mathfrak{M}}(\vec{a})) \in R^{\mathfrak{M}}$.
3. Si F es de la forma $\neg G$ entonces $\mathfrak{M} \models F(\vec{a})$ si $\mathfrak{M} \not\models G(\vec{a})$.
4. Si F es de la forma $G \wedge H$, entonces $\mathfrak{M} \models F(\vec{a})$ si $\mathfrak{M} \models G(\vec{a})$ y $\mathfrak{M} \models H(\vec{a})$.
5. Si F es de la forma $G \vee H$, entonces $\mathfrak{M} \models F(\vec{a})$ si $\mathfrak{M} \models G(\vec{a})$ o $\mathfrak{M} \models H(\vec{a})$.
6. Si F es de la forma $\exists v_j G(\vec{v}, v_j)$, entonces $\mathfrak{M} \models F(\vec{a})$ si existe un cierto $b \in M$ tal que $\mathfrak{M} \models G(\vec{a}, b)$.
7. Si F es de la forma $\forall v_j G(\vec{v}, v_j)$, entonces $\mathfrak{M} \models F(\vec{a})$ si$\mathfrak{M} \models G(\vec{a}, b)$ para todo $b \in M$.

En caso de que $\mathfrak{M} \models F(\vec{a})$, diremos que $\mathfrak{M}$ satisface $F(\vec{a})$ o que $F(\vec{a})$ es verdadero en $\mathfrak{M}$ o $\mathfrak{M}$ es un modelo de $F(\vec{a})$.

Definición 1.17 — Estructuras elementalmente equivalentes.

Dos $\mathscr{L}-$ estructuras $\mathfrak{M}$ y $\mathfrak{N}$ son elementalmente equivalentes ($\mathfrak{M} \equiv \mathfrak{N}$) si satisfacen las mismas $\mathscr{L}-$sentencias. Es decir

$$\mathfrak{M} \models F \iff \mathfrak{N} \models F \quad \text{para todas las sentencias} \quad F \in \mathscr{L}.$$

Nota. De aquí en adelante llamaremos sentencias a las fórmulas cerradas de un lenguaje es decir a las fórmulas que no contienen variables libres.

Definición 1.18 — Elemental.

Sea $\mathfrak{M}$ y $\mathfrak{N}$ dos $\mathscr{L}-$estructuras. Una incrustación φ de $\mathfrak{M}$ en $\mathfrak{N}$ se llama **elemental** si, para cada fórmula $F(\vec{v})$ en $\mathscr{L}$ y cada sucesión $\vec{a}$ en M, $\mathfrak{M} \models F(\vec{a})$ si y sólo si $\mathfrak{N} \models F(\varphi(\vec{a}))$.

Teorema 1.1 Sea $\mathfrak{M}$ y $\mathfrak{N}$ dos $\mathscr{L}-$estructuras, sea φ una función de M en N. Entonces las siguientes proposiciones son equivalentes:

(i) φ es una incrustación de $\mathfrak{M}$ en $\mathfrak{N}$;

(ii) Para cada fórmula libre de cuantificadores $F(\vec{v})$ en $\mathscr{L}$ y para toda sucesión $\vec{a}$ en M,

$$\mathfrak{M} \models F(\vec{a}) \iff \mathfrak{N} \models F(\varphi(\vec{a}));$$

(iii) Para cada fórmula atomica $G(\vec{v})$ en $\mathscr{L}$ y para cada sucesión $\vec{a}$ en M,

$$\mathfrak{M} \models G(\vec{a}) \iff \mathfrak{N} \models G(\varphi(\vec{a})).$$

La demostración es de manera directa utilizando la definición de incrustación, término, fórmula (atómica o sin cuantificador).

Teorema de compacidad

Teorema 1.2 Sea $\mathscr{S}$ un conjunto infinito de sentencias de un lenguaje $\mathscr{L}$. Supongamos que cada subconjunto finito de $\mathscr{S}$ tiene un modelo. Entonces $\mathscr{S}$ tiene un modelo.

Conjuntos definibles

Definición 1.19 — Conjuntos definibles.

Sea $\mathfrak{M}$ una cierta $\mathscr{L}-$estructura de dominio M.

Decimos que un conjunto $X \subseteq M^n$ es definible si y sólo si existe una fórmula $F(v_1, \ldots, v_n, w_1, \ldots, w_m)$ y $\vec{b} \in M^m$ tal que $X = \{\vec{a} \in M^n : \mathfrak{M} \models F(\vec{a}, \vec{b})\}$. En este caso decimos que $F(\vec{v}, \vec{b})$ define X en M.

■ **Ejemplo 1.11** Sea el lenguaje $\mathscr{L} = \{c_1, c_2, f, g\}$ donde c_1, c_2 son símbolos constantes y f, g símbolos de funciones binarias.

1. Sea $\mathfrak{M} = (\mathbb{N}, 0, 1, +, \cdot)$, el conjunto de los número primos es definible en $\mathfrak{M}$. Basta considerar

$$F(x) \equiv x \neq 1 \wedge \forall y \forall z (x = y \cdot z \rightarrow y = 1 \vee z = 1)$$

2. Sea $\mathfrak{M} = (\mathbb{Z}, 0, 1, +, \cdot)$ el anillo de los entero. Consideremos

$$X = \{(m, n) \in \mathbb{Z}^2 : m < n\}$$

El conjunto X es definible. En efecto, el Teorema de Lagrange nos garantiza que todo entero no negativo puede expresarse como a suma de cuatro cuadrados. De este modo, si consideramos $F[x, y]$ la fórmula

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2),$$

entonces podemos expresar X como

$$X = \{(m, n) \in \mathbb{Z}^2 : \mathfrak{M} \models F(x, y)\}$$

De aquí en adelante llamaremos ***sentencias*** *a las fórmulas cerradas de un lenguaje es decir a las fórmulas que no contienen variables libres.*

1.3 Teorías de primer orden

Definición 1.20 — Teoría de primer orden.

Una teoría de primer orden $\mathscr{T}$ consiste en un conjunto de fórmulas cerradas de un determinado lenguaje $\mathscr{L}$ (de primer orden). Dichas fórmulas son conocidas como los axiomas no lógicos (o simplemente axiomas) de la teoría $\mathscr{T}$.

Denotaremos al lenguaje de $\mathscr{T}$ como $\mathscr{L}(\mathscr{T})$ y diremos que $\mathscr{T}$ es una $\mathscr{L}-$teoría.

Definición 1.21 — Satisfacción de teorías de primer orden.

Dado un lenguaje $\mathscr{L}$ y una $\mathscr{L}-$teoría $\mathscr{T}$, decimos que una $\mathscr{L}-$estructura $\mathfrak{M}$ es un modelo de $\mathscr{T}$, que escribiremos como $\mathfrak{M} \models T$, si se verifica que $M \models \varphi$, para toda sentencias φ perteneciente a los axiomas no lógicos de $\mathscr{T}$. Decimos que una teoría $\mathscr{T}$ es satisfacible si posee, al menos, un modelo.

1.4 Teorias completas

Definición 1.22 — Teoría consistente.

Una teoría $\mathscr{T}$ es llamada consistente si existe un modelo $\mathfrak{M}$ tal que $\mathfrak{M} \models \mathscr{T}$

Definición 1.23 — Teoría completa.

Se dice que una teoría (consistente) $\mathscr{T}$ de $\mathscr{L}$ es completa si, para cada sentencia φ de $\mathscr{L}$, o bien $\varphi \in \mathscr{T}$ o $\neg\varphi \in \mathscr{T}$.

De hecho, se observa fácilmente sobre la base de la definición de verdad en la lógica de primer orden que, dada una estructura $\mathfrak{M}$ en un lenguaje $\mathscr{L}$, para cada $\mathscr{L}-$sentencia φ, o bien φ es verdadera en $\mathfrak{M}$ o bien $\neg\varphi$.

Definición 1.24 — Modelo completo.

Una teoría $\mathscr{T}$ es modelo completo si cada incrustación del modelo de $\mathscr{T}$ es elemental.

2. Eliminación de cuantificadores

2.1 Conjuntos de eliminación

Sea $\mathscr{L}$ un lenguaje. Puede ocurrir que dos $\mathscr{L}-$fórmulas diferentes F y G admitan el mismo significado en una estructura $\mathfrak{M}$ de $\mathscr{L}$, o en una clase de $\mathscr{L}-$estructuras , por ejemplo entre los modelos de una determinada $\mathscr{L}-$teoría $\mathscr{T}$.

Por ejemplo, en el campo ordenado de los reales (e incluso en todo campo real cerrado), la fórmula $F(v) = v \geq 0$ (siendo no negativa) es lo mismo que $G[v] = \exists w(v = w^2)$ (siendo un cuadrado). Del mismo modo, en el dominio ordenado de los números enteros, $F(v) = v \geq 0$ (ser positivo) tiene la misma interpretación que $G(v) = \exists w_1 \exists w_2 \exists w_3 \exists w_4 (v = \sum_{1 \leq i \leq 4} w_i^2)$ (siendo la suma de cuatro cuadrados): se trata de un célebre teorema de Lagrange.

Definición 2.1 — Equivalencia de fórmulas en la teoría $\mathscr{T}$.

Diremos que dos fórmulas $F(\vec{v})$ y $G(\vec{v})$ son equivalentes con respecto a $\mathscr{T}$, y escribiremos $F(\vec{v}) \sim_{\mathscr{T}} G(\vec{v})$, cuando

$$\forall \vec{v}(F(\vec{v}) \longleftrightarrow G(\vec{v})) \in \mathscr{T}$$

equivalente cuando

$$F(\mathfrak{M}^n) = G(\mathfrak{M}^n)$$

para todos los modelos $\mathfrak{M}$ de $\mathscr{T}$.

La noción de conjunto de eliminación surge de forma bastante natural en este punto. Es por eso que el siguiente paso será definir uno de los conceptos clave de esta sección. Además, este es un concepto que surge de manera natural tras conocer la idea de equivalencia entre fórmulas.

Definición 2.2 — Conjunto de eliminación.

Un conjunto de eliminación para $\mathscr{T}$ es un conjunto $\mathscr{F}$ de $\mathscr{L}-$fórmulas tal que cada fórmula $F(\vec{v})$ es $\mathscr{T}-$equivalente a una combinación booleana adecuada de fórmulas de $\mathscr{F}$.

Es evidente que el conjunto de todas las $\mathscr{L}$-fórmulas es un conjunto de eliminación para $\mathscr{T}$. Pero, por supuesto, éste no es un caso interesante, y razonablemente esperamos conjuntos más sencillos $\mathscr{F}$. En particular, cuando el conjunto de fórmulas atómicas en $\mathscr{L}$ es un conjunto de eliminación para $\mathscr{T}$, decimos que $\mathscr{T}$ tiene el cuantificador eliminación en $\mathscr{L}$.

Definición 2.3 — Eliminación de cuantificadores.

Sea $\mathscr{T}$ una teoría en el lenguaje $\mathscr{L}$. $\mathscr{T}$ tiene la eliminación de cuantificadores en $\mathscr{L}$ si y sólo si cada fórmula $F(\vec{v})$ en $\mathscr{L}$ es equivalente en $\mathscr{T}$ a una $\mathscr{L}-$fórmula libre de cuantificadores $G(\vec{v})$.

Ejemplo 2.1 Consideremos la fórmula $F(a,b,c) := \exists x(ax^2+bx+c=0)$ es equivalente a la fórmula $a \neq 0$. O en una teoría $\mathscr{T} = \mathscr{T}h(\mathbb{R},+,\cdot,0,1,<)$ la fóruma $F(a,b,c)$ es equivalentea la fórmula $b^2-4ac>0$

Es fácil ver que cada $\mathscr{T}$ consigue la eliminación de cuantificadores, aplicandose a un lenguaje adecuado que sea una extensión de $\mathscr{L}$. Para ello, podemos suponer que $\mathscr{L} = \mathscr{L}_0$ y $\mathscr{T} = \mathscr{T}_0$.

A continuación, podemos ampliar $\mathscr{L}$ a un lenguaje $\mathscr{L}_1$ que contenga un símbolo de relación $n-$ario R para cada fórmula $F(\vec{v})$ de $\mathscr{L}_0$, donde n es la longitud de la variable cuantificada $\vec{v}$. Finalmente, podemos aplicar el procedimiento $\mathscr{T}$ a fórmulas de $\mathscr{L}_\infty$, reemplazando cada cuantificación v con la relación R correspondiente.

$$\forall \vec{v}(F(\vec{v}) \leftrightarrow R(\vec{v})),$$

para cada $F(\vec{v})$ y obtener una nueva teoría $\mathscr{T}_1$, está claro que las fórmulas atómicas de $\mathscr{L}_1$ forman un conjunto de eliminación en $\mathscr{T}_1$ para las fórmulas en $\mathscr{L}_0$. Repitiendo este procedimiento contablemente muchas veces, uno define eventualmente un lenguaje $\mathscr{L}' \supseteq L$ y una teoría $\mathscr{T}'$ de $\mathscr{L}'$ extendiendo "naturalmente" $\mathscr{T}$ y teniendo la eliminación de cuantificadores en $\mathscr{L}'$.

Desgraciadamente, este procedimiento tiene un sabor bastante artificial y abstracto. De hecho, lo que nos gustaría obtener, dada una teoría $\mathscr{T}$ en un lenguaje $\mathscr{L}$, es mostrar que $\mathscr{T}$ tiene la eliminación de cuantificadores directamente en $\mathscr{L}$ o, de otro modo, determinar una extensión más pequeña $\mathscr{L}' \supseteq L$, posiblemente sugerida por el análisis algebraico de los modelos de $\mathscr{T}$, donde $\mathscr{T}$ (o, más exactamente, su extensión natural a $\mathscr{L}'$) tiene la eliminación de cuantificadores, o también un conjunto de fórmulas razonablemente simple, en $\mathscr{L}'$. De hecho, hay buenas razones para creer que tal lenguaje $\mathscr{L}'$ es, en cierto modo, "el" lenguaje propio de $\mathscr{T}$.

¿Cuáles son las principales ventajas de un conjunto de eliminación, en particular de la eliminación de cuantificadores?

La eliminación de cuantificadores es una técnica utilizada en lógica matemática y teoría de la computación para simplificar y analizar expresiones lógicas que contienen cuantificadores. El objetivo es transformar una fórmula cuantificada en una fórmula equivalente sin cuantificadores. A continuación, se presentan algunas de las principales ventajas de un conjunto de eliminación, centrándose en la eliminación de cuantificadores:

Ejemplo 2.2

1. La principal (al menos desde un punto de vista histórico) es la decidibilidad. En realidad, los primeros y más célebres resultados de eliminación de cuantificadores están relacionados con el tema de la decidibilidad.

   Expliquemos por qué.

   Recordemos que una teoría $\mathscr{T}$ es decidible si existe un algoritmo que compruebe en un número finito de pasos, para cada sentencia α en el lenguaje $\mathscr{L}$ de $\mathscr{T}$, si α está o no en T.

   Supongamos ahora que $\mathscr{F}$ es un conjunto de eliminación para $\mathscr{T}$ y que se dispone de lo siguiente:

   - Un procedimiento eficaz que traduzca cualquier sentencia del lenguaje $\mathscr{L}$, en una combinación booleana $\mathscr{T}$-equivalente de sentencias en $\mathscr{F}$.
   - Un algoritmo que, para cada combinación booleana de sentencias de $\mathscr{F}$, concluya si está o no en $\mathscr{T}$.

   Entonces, claramente, $\mathscr{T}$ es decidible, y en realidad hemos obtenido un algoritmo de decisión (aplicando sucesivamente los dos procedimientos anteriores).

2. Otra aplicación notable de la eliminación de cuantificadores se refiere a la

definibilidad. De hecho, si $\mathscr{F}$ es un conjunto de eliminación para $\mathscr{T}$, entonces los conjuntos definibles de un modelo $\mathfrak{M}$ de $\mathscr{T}$ se reducen a

$$F(\mathfrak{M}^n,\vec{x}) = \{\vec{y} : \mathfrak{M} \models F(\vec{y},\vec{x})\}$$

donde $F(\vec{v},\vec{w})$ es una combinación booleana finita de fórmulas de $\mathscr{F}$ y $x \in M$ en particular, si $\mathscr{T}$ tiene la eliminación del cuantificador en $\mathscr{L}$, entonces los conjuntos definibles de $\mathfrak{M}$ en $\mathscr{T}$ son sólo los de la forma

$$F(\mathfrak{M}^n,\vec{x})$$

donde $F(\vec{v},\vec{w})$ es una fórmula libre de cuantificador y $\vec{x} \in M$.

3. También es fundamental para estudiar la completitud del modelo. Supongamos que $\mathscr{T}$ admite eliminación de cuantificadores en $\mathscr{L}$.

   Afirmamos que, en este caso, toda incrustación entre modelos de $\mathscr{T}$ es elemental, es decir $\mathscr{T}$ es modelo completo. De hecho, $\mathfrak{M}$ y $\mathfrak{N}$ son modelos de $\mathscr{T}$, φ es una incrustación de $\mathfrak{M}$ en $\mathfrak{N}$.

   Dada una fórmula $F(\vec{v})$ en $\mathscr{L}$, sea $G(\vec{v})$ una fórmula libre de cuantificadores equivalente a $F(\vec{v})$ en $\mathscr{L}$. Sea $\vec{a}$ en M. Como φ es una incrustación,

$$\mathfrak{M} \models G(\vec{a}) \iff \mathfrak{N} \models G(\varphi(\vec{a}))$$

   como

$$\forall\vec{v}(F(\vec{v}) \iff G(\vec{v})) \in \mathscr{T},$$

$$\mathfrak{M} \models F(\vec{a}) \iff \mathfrak{N} \models F(\varphi(\vec{a}))$$

   Por lo tanto φ es elemental.

Las fórmulas sin cuantificadores son las más simples que existen. Si podemos entender bien los conjuntos que se pueden definir con fórmulas simples, entonces también podremos entender todos los conjuntos que se pueden definir, sin importar lo complejos que sean.

2.2 Reducción a fórmulas sencillas

Ya conocemos, aunque de forma genérica, algunas de las virtudes que poseen las teorías con eliminación de cuantificadores. ***¿Cómo sabemos si una teoría $\mathscr{T}$ tiene eliminación de cuantificadores en un determinado lenguaje $\mathscr{L}$?***

Para responder a esto, deberíamos estudiar si, dada una fórmula $F(\vec{v})$ de $\mathscr{L}$ cualquiera, existe otra $\mathscr{L}$-fórmula $G(\vec{v})$ sin cuantificadores cumpliéndose que

$$F(\vec{v}) \sim_{\mathscr{T}} G(\vec{v}).$$

Esto puede parecer una tarea imposible, pues la diversidad de las fórmulas de un lenguaje puede ser extremadamente grande. Sin embargo, introduciremos un resultado que nos permitirá reducir el estudio de la eliminación de cuantificadores a una serie de fórmulas muy concretas.

Lema 2.2.1 Sea $\mathscr{T}$ una determinanda $\mathscr{L}-$teoría. Para demostrar que $\mathscr{T}$ admite eliminación de cuantificadores sobre $\mathscr{L}$, es suficiente con demostrar que las fórmulas de la forma

$$\exists w \left(\bigwedge_{i \leq r} \alpha_i(\vec{v}, w) \right),$$

son equivalentes a una fórmula libre, donde cada $\alpha_i(\vec{v}, w)$ es una fórmula atómica o su negación y w es una variable que aparece en $\alpha_i(\vec{v}, w)$, para todo $i < r$.

Demostración. Sea $F(\vec{v})$ una fórmula genérica con cuantificadores. Podemos suponer por tanto que será de la forma

$$Q_1 w_1 \dots Q_m w_m \alpha(\vec{v}, \vec{w}),$$

donde $\vec{w} = (w_1, \dots, w_m)$, Q_j denota un cuantificador(ya sea el existencial $\exists$ o el universal $\forall$) para $1 \leq j \leq m$ y $\alpha(\vec{v}, \vec{w})$ es una fórmula libre. Incluso más, aplicando un algoritmo de reescritura en forma normal disyuntiva si fuese necesario, podemos suponer que $\alpha(\vec{v},\vec{w})$ es una disyunción de conjunciones de fórmulas atómicas y negaciones de atómicas.

Se consistirá en eliminar, en primer lugar, el cuantificador Q_m y, posteriormente, repetir el proceso hasta alcanzar el resultado deseado. Es decir, eliminar por completo la cadena de cuantificadores.

Sin pérdida de generalidad, podemos suponer que $Q_m = \exists$. De este modo, para obtener un procedimiento de eliminación de cuantificadores, nos podemos reducir al caso

$$\exists w \alpha(\vec{v},w),$$

donde α es una disyunción de conjunciones de fórmulas atómicas y negaciones.

Ahora bien, puesto el cuantificador existencial verifica las propiedades de distributividad en relación a la disyunción, tenemos que

$$\exists w(\beta \vee \gamma) \quad \text{es equivalante a} \quad (\exists w\beta) \vee (\exists w\gamma)$$

por tanto, también podemos suponer sin pérdida de generalidad que α es simplemente una conjunción de fórmulas atómicas y negaciones.

En resumen, para obtener un procedimiento de eliminación de cuantificadores para cualquier fórmula del lenguaje, podemos reducirnos al caso:

$$\exists w \left(\bigwedge_{i \leq r} \alpha_i(\vec{v},w) \right),$$

donde $\alpha_i(\vec{v},w)$ es una fórmula atómica o su negación. Tan solo nos resta justificar que podemos suponer que además de la variable w aparece en $\alpha_i(\vec{v},w)$ para todo $i \leq r$. Para ello, observemos que si $j \leq r$ es uno de los subíndices que no cumplen la condición anterior, entonces son equivalentes las fórmulas

$$1.\exists w\left(\bigwedge_{i\leq r}\alpha_i(\vec{v},w)\right) \quad \text{y} \quad 2.\alpha_j(\vec{v})\wedge\exists w\left(\bigwedge_{i\neq j}\alpha_i(\vec{v},w)\right),$$

siendo así únicamente necesario eliminar el cuantificador de la fórmula

$$\exists w\left(\bigwedge_{i\neq j}\alpha_i(\vec{v},w)\right)$$

En cualquier caso, se ha llegado a una fórmula de la forma que se buscaba. ■

3. Ordenes lineales discretos y densos

3.1 Ordenes lineales discretos

Comenzamos aquí el análisis de las teorías de cuantificadores eliminables.

Primero tratamos órdenes lineales infinitos. En consecuencia nuestro lenguaje básico es $\mathscr{L} = \{<\}$.

Más precisamente tratamos con:

- Teorías de los órdenes lineales discretos.
- Teorías de órdenes lineales densos.

Como ya se ha dicho, los resultados de la eliminación de cuantificadores en estos casos fueron mostrados por primera vez por Langford en 1927; Tarski prosiguió el análisis para obtener la decidibilidad y clasificar las teorías completas de órdenes totales infinitos discretos y densos.

Definición 3.1 — Órden lineal discreto.

Un (n infinito) orden lineal $\mathfrak{M} = (M, \leq)$ es discreto si y sólo si

i) $\forall a \in M$, si existe algún $a' \in M$ tal que $a < a'$, entonces existe un mínimo $b \in M$

para el cual $a < b$ (b se denomina sucesor de a y se denota $s(a)$);

- $\forall a \in M$, si hay algún $a' \in M$ tal que $a' < a$, entonces existe un máximo $b \in M$ para el que $b < a$ (b se llama predecesor de a; obviamente $a = s(b)$).

Ejemplo 3.1

1. La clase de órdenes lineales discretos con un mínimo, pero sin último elemento (como $(\mathbb{N}, \leq)$);
2. La clase de órdenes lineales discretos con un último elemento, pero no el menor (por ejemplo, N con respecto a la relación que invierte su orden habitual, es decir $(\{n \in \mathbb{N} | \frac{1}{n}\}, \leq)$;
3. La clase de los órdenes lineales discretos (infinitos) con un mínimo y un último elemento (como la unión disjunta de dos órdenes lineales discretos $(A, \leq)$, $(B, \leq)$, el primero en 1, el segundo en 2, con $a < b$ para todo
$a \in A$ y $b \in B$);
4. La clase de órdenes lineales discretos sin puntos finales (como $(\mathbb{Z}, \leq)$).

Cada una de estas clases es elemental. Además se puede demostrar que su teoría tiene la eliminación de cuantificadores en un lenguaje adecuado que extienda $\mathscr{L}$, y es completa incluso en $\mathscr{L}$. Aquí nos limitamos a demostrar, por simplicidad, estos resultados en el caso 1, es decir para órdenes lineales discretos con un mínimo pero sin último elemento.

Consideremos el lenguaje $\mathscr{L}' = \{\leq, 0, s\}$ donde 0 es una constante (que debe interpretarse como el menor elemento) y s es un símbolo de función $1 - ario$ (que debe interpretarse como la función que asigna cualquier elemento a su sucesor).

Es fácil escribir un conjunto de axiomas de primer orden para nuestra clase en $\mathscr{L}'$. Sea dLO^+ la teoría correspondiente. Por cierto, nótese que las fórmulas adecuadas en el lenguaje restringido $\mathscr{L}'$ definen el elemento mínimo y la función sucesora en cada modelo de dLO^+. Esto implica que los axiomas de dLO^+ pueden reescribirse también en $\mathscr{L}$, a costa de algunas complicaciones (y cuantificadores) más. Por ejemplo, expresar la existencia de un elemento mínimo requiere la $\mathscr{L}-$sentencia

$$\exists w \forall v(w \leq v),$$

en lugar de

$$\forall v(0 \leq v)$$

Pero momentáneamente preferimos tratar dLO^+ en $\mathscr{L}$. Observe que:

- $(\mathbb{N}, \leq, 0, s)$ es un modelo de dLO^+
- Si $\mathfrak{M}$ es otro modelo de dLO^+, entonces $\mathfrak{M}$ contiene una subestructura $(\{s^n(0^{\mathfrak{M}}) : n \in \mathbb{N}\}, \leq, 0^{\mathfrak{M}}, s^{\mathfrak{M}})$ isomorfa a un $(\mathbb{N}, \leq, 0, s)$, y además algunas copias más de $(\mathbb{Z}, \leq, s)$ (ya que $0^{\mathfrak{M}}$ es el único elemento sin ningún predecesor).

Teorema 3.1 dLO^+ tiene eliminación de cuantificadores en $\mathscr{L}'$.

Demostración. Tomemos una fórmula $F(\vec{v})$ en nuestro lenguaje $\mathscr{L}'$; buscamos una fórmula equivalente $G(\vec{v})$ sin cuantificadores.

Nuestro primer paso es demostrar que podemos suponer que $F(\vec{v})$ es de la forma

$$\exists w \left(\bigwedge_{i \leq r} \alpha_i(\vec{v}, w) \right)$$

donde cada $\alpha_i(\vec{v}, w)$ es una fórmula atómica, o su negación, y en realidad ocurre en $\alpha_i(\vec{v}, w)$ para cada $i \leq r$.

Queremos subrayar que este paso es bastante general, y no depende de nuestra lengua particular $\mathscr{L}'$. Veamos por qué. En primer lugar, podemos suponer tácitamente que $F(\vec{v})$ es de la forma

$$Q_1 w_1 \ldots Q_m w_m \alpha(\vec{v}, \vec{w})$$

donde las $Q_j's(1 \leq j \leq m)$ denotan cuantificadores $\forall$ o $\exists$, $\alpha(\vec{v}, \vec{w})$ es una fórmula libre de cuantificadores, e incluso una disyunción de conjunciones de fórmulas atómicas y negaciones (y $\vec{w}$ en abreviaturas $(w_1, \ldots, w_m)$, por supuesto). La estrategia en este punto es primero eliminar Q_m, y luego repetir el procedimiento y eliminar la cadena de cuantificadores por completo.

Recordemos que $\forall$ es equivalente a $\neg\exists\neg$ y por consiguiente, estamos de acuerdo en que basta con tratar el caso en que Q_m es $\exists$, es decir, con

$$\exists w \alpha(\vec{v}, w)$$

donde α es una disyunción de conjunciones de fórmulas atómicas o negaciones,
$w = w_m$ y $\vec{v}$ se amplía posiblemente para incluir $w_1, \ldots, w_{m-1}$. Como $\exists$ es distributivo con respecto a $\vee$, es decir, $\exists w(\alpha' \vee \alpha'')$es equivalente a $(\exists w \alpha') \vee (\exists w \alpha'')$, no hay pérdida de generalidad para nuestros propósitos en suponer que α es sólo una conjunción de fórmulas atómicas o negaciones.

En conclusión, se trata de

$$\exists w \left(\bigwedge_{i \leq r} \alpha_i(\vec{v}, w) \right)$$

donde cada $\alpha_i(\vec{v}, w)$ es una fórmula atómica, o su negación. También podemos suponer que w aparece realmente en $\alpha_i(\vec{v}, w)$ para cada $i \leq r$; de lo contrario, dejemos que $j \leq r$ niegue esta condición y observemos que nuestra fórmula

$$\exists w \left(\bigwedge_{i \leq r} \alpha_i(\vec{v}, w) \right)$$

es equivalente a

$$\alpha_j(\vec{v}) \wedge \exists w \bigwedge_{i \neq j} \alpha_i(\vec{v}, w)$$

en este punto basta con eliminar el cuantificador $\exists$ en la última parte de la fórmula

$$\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$$

Esto completa nuestro paso preliminar. Como ya se ha dicho, esto no depende de nuestro marco concreto. Trabajemos ahora con nuestra fórmula

$$\exists w \bigwedge_{i\leq r} \alpha_i(\vec{v}, w)$$

y nuestra lengua $\mathscr{L}'$. Nos preguntamos cuál es la forma de cualquier α_i. Un vistazo a $\mathscr{L}'$ muestra que α_i es $t = t'$, o $t < t'$, o la negación de una de estas fórmulas, donde t y t' son términos en $0, w, \vec{v}$(y w ocurre realmente en t o t'). Recordemos que $\neg(t \leq t')$ significa $t > t'$, y así sucesivamente.

Deduzca que α_i, es, sin pérdida de generalidad, o bien $t = t'$ o bien $t > t'$, con t y t' como antes.

Obsérvese que t y t' son de la forma $s^p(u)$ donde p es un entero no negativo y u varía entre $0, w, \vec{v}$. Recordemos ahora que s es inyectiva y deduzcamos que la fórmula que estamos examinando garantiza que existe una solución w para un conjunto finito de condiciones que dicen que w o un sucesor $s^q(w)$ (q un entero no negativo) es igual, o mayor, o menor que un término $s^p(u)$ donde p es, de nuevo, un entero no negativo y u varía entre $w, 0, \vec{v}$: como s es inyectiva, podemos suponer que, en cada una de estas ecuaciones e inecuaciones, s aparece sólo en un lado (a la izquierda, o a la derecha).

Nuestro objetivo es traducir esta fórmula en una equivalente que evite w y establezca simplemente condiciones libres de cuantificador sobre $\vec{v}$(y 0). Para obtenerla, proceda como sigue.

Trivialidades como $w = w$ o $w < s^p(w)$ para un p positivo pueden ser ignoradas y eliminadas (pueden ser enumeradas preliminarmente y por lo tanto son fácilmente reconocibles); si no ocurre nada más, entonces reemplace toda la fórmula por $0 = 0$. Por el contraio, cuando se cumple una condición que no puede ser satisfecha por ningún w, como $w = s^p(w)$, o $0 = s^p(w)$ para un p positivo (también estas condiciones pueden ser enumeradas preliminarmente), entonces reemplace nuestra fórmula por $\neg(0 = 0)$ (o con $\neg(v_1 = v_1)$) si se quiere y $\vec{v}$ no está vacío). En caso contrario, en cuanto encuentres una ecuación como $w = s^p(v_i)$, elimina w y $\exists$, y sustituye w por $s^p(v_i)$ en toda nuestra fórmula. Procede del mismo modo si se da una ecuación $w = s^p(0)$. Del mismo modo, cuando se cumple una condición $s^q(w) = v_i$, considere cualquier otra ocurrencia de w en la fórmula y, de nuevo utilizando la inyectividad de s, represéntela $s^{q'}(w)$ para un entero no negativo adecuado $q' \geq q$; por último, elimine w y $\exists$ y sustituya cada ocurrencia $s^{q'}(w)$ por $s^{q-q'}(v_i)$.

Por último, supongamos que sólo se producen disequaciones. Utilizando de nuevo la inyectividad de s, podemos suponer que todas ellas conciernen al mismo término $s^q(w)$ en w. Entonces nuestra fórmula afirma que $s^q(w)$ es menor que ciertos términos $t_0, \ldots, t_h$ en 0 y $\vec{v}$, y mayor que algunos otros términos $t_{h+1}, \ldots, t_k$.

Obtenemos un fórmula equivalente evitando w y su cuantificador de la siguiente manera. Enumerar (en una disyunción adecuada) todas las posibles ordenaciones de $t_0, \ldots, t_h$ en $\leq$ según las cuales $t_0, \ldots, t_h$ preceden a $t_{h+1}, \ldots, t_k$; para cada ordenación, que t, t' denotan respectivamente el mayor elemento entre $t_0, \ldots, t_h$ y el menor entre $t_{h+1}, \ldots, t_k$, añadimos $s(t) < t'$ (para dar a $s^q(w)$ el espacio adecuado). Con esto concluye el procedimiento de eliminación. ■

Corolario 3.1 dLO^+ es modelo completo (en $\mathscr{L}'$) y completo (tanto en $\mathscr{L}'$ como en $\mathscr{L}$).

Demostración. Claramente dLO^+ es modelo completo en $\mathscr{L}'$.

Además $(\mathbb{N}, \leq, 0, s) \models dLO^+$, y $(N, \leq, 0, s)$ es incrustable en cada modelo de dLO^+. Como dLO^+ es modelo completo, todas las incrustaciones correspondientes son elementales. Según esto, todos los modelos de dLO^+ son elementalmente equivalentes a $(\mathbb{N}, \leq, 0, s)$

y, por tanto, entre sí. Esto demuestra que dLO^+ es completo en $\mathscr{L}'$. Recordemos ahora que tanto el elemento mínimo como la función sucesora (es decir, las interpretaciones de los símbolos en $\mathscr{L}' - \mathscr{L}$) son $\emptyset-$definibles por $\mathscr{L}-$fórmulas en los modelos de dLO^+ . Entonces es fácil deducir que dLO^+ es completo en $\mathscr{L}$, también $\mathscr{L}'$ ■

Corolario 3.2 dLO^+ es decidible (en $\mathscr{L}'$ y en $\mathscr{L}$).

Demostración. Reduzca cualquier sentencia de $\mathscr{L}'$ a un estado equivalente libre de cuantificador. Se trata de una combinación booleana de fórmulas $s^m(0) \geq s^n(0)$ donde m y n son enteros no negativos, y dLO^+ puede comprobar fácilmente su pertenencia. Este procedimiento funciona incluso para $\mathscr{L}-$sentencias. ■

Corolario 3.3 Sea $\mathfrak{A} \models dLO^+$. Los subconjuntos de A definibles en $\mathfrak{A}$ (en $\mathscr{L}$ o en $\mathscr{L}'$) no son más que las uniones finitas de intervalos (abiertos o cerrados) en A (posiblemente teniendo $+\infty$ como extremo derecho).

Demostración. Sea $\varphi(v, \vec{w})$ una $\mathscr{L}'$-fórmula. Como dLO^+ tiene la eliminación de cuantificadores en $\mathscr{L}'$, podemos suponer que $\varphi(v, \vec{w})$ está libre de cuantificadores; debido al Teorema 3.1 (y su demostración), para cada $\vec{a}$ en A, $\varphi(\mathfrak{A}, \vec{a})$ es una unión de intersecciones de intervalos, y por tanto una unión de intervalos. ■

Con esto concluimos nuestro análisis de los órdenes lineales discretos con un penúltimo elemento. ¿Cómo tratar los otros tres casos de órdenes lineales discretos infinitos enumerados antes?. Se pueden tratar de forma similar para obtener la eliminación del cuantificador y, en consecuencia, la completitud. En particular, resulta que los cuatro casos agotan todas las posibles terminaciones de la teoría de los órdenes lineales discretos infinitos; en otras palabras, estas terminaciones se caracterizan completamente diciendo si los modelos correspondientes admiten o no un elemento menor y un elemento mayor.

En realidad, el caso sin puntos finales merece algunos comentarios más. De hecho, en este marco, el lenguaje ampliado L' no necesita ningún símbolo "constante" natural (simplemente porque faltan puntos finales), y toma el único símbolo de operación adicional s. En consecuencia, hablando con propiedad, la eliminación de cuantificadores falla en este lenguaje ampliado, porque no tenemos ninguna constante para construir oraciones atómicas. Por ejemplo, la sentencia (verdadera) $\exists w(w = w)$ no puede traducirse en una sentencia equivalente libre de cuantificadores; lo mismo ocurre con la sentencia (falsa) $\exists w(s(w) = w)$.

Por lo tanto, el enunciado correcto en este caso es sigue: un conjunto de eliminación para la teoría de los órdenes lineales discretos sin puntos finales es el conjunto de fórmulas atómicas más una sentencia única (como "no hay ningún elemento menor", o "no hay ningún elemento último"). No discutiremos aquí la prueba. De hecho, trataremos este caso en detalle al considerar los órdenes lineales densos en la siguiente sección. Por último, obsérvese que la decidibilidad puede demostrarse (en $\mathscr{L}$) en los 4 casos posibles. En consecuencia, la teoría (incompleta) dLO de infinitos órdenes lineales discretos también es decidible; de hecho, una sentencia φ de $\mathscr{L}$ pertenece a dLO si y sólo si está en cada una de sus 4 compleciones.

3.2 Órdenes lineales densas

Ahora nos ocuparemos de los órdenes lineales densos. El plan aquí es exactamente el mismo que en el caso discreto. Usamos el lenguaje $\mathscr{L} = \{\leq\}$ y distinguimos 4 casos posibles:

1. Hay un elemento menor, pero no un elemento último (al igual que entre los no racionales negativos con respecto al orden habitual);
2. Hay un último elemento, pero no un elemento menor (ahora los racionales no

positivos proporcionan un ejemplo);

3. Hay un elemento menor y un elemento último (fíjate en los racionales, o incluso en los reales, en el intervalo cerrado $[0,1]$);

4. No hay puntos finales (es el caso de $(\mathbb{Q}, \leq)$).

En 1, 2, 3 se muestra la eliminación de cuantificadores en un lenguaje con una o dos constantes adicionales para ser intepretadas en los puntos finales; 4 merece un tratamiento más específico, porque las fórmulas libres de cuantificador necesitan una sola $\mathscr{L}-$sentencia auxiliar para formar un conjunto de eliminación (incluso en $\mathscr{L}$): proporcionamos detalles completos más adelante. En todos estos casos es fácil deducir la completitud en $\mathscr{L}$. Esto implica que estas 4 clases agotan todas las posibles completaciones de la teoría de los órdenes lineales densos.

Sea $\mathscr{L} = \{\leq\}$ donde $\leq$ es un símbolo de relación binaria (que confundimos , por simplicidad, con su interpretación a continuación -una relación de orden-). En $\mathscr{L}$ consideramos la clase K de órdenes lineales. Se ve fácilmente que K es elemental, porque las propiedades que definen los órdenes lineales son sentencias de primer orden (y de hecho sentencias universales de primer orden) de L. Por ejemplo, la linealidad puede expresarse mediante

$$\forall v_0 \forall v_1 (v_0 \leq v_1 \vee v_1 \leq v_0).$$

El conjunto de las consecuencias lógicas de estas sentencias es la teoría de los órdenes lineales, está formado por las sentencias verdaderas en cada orden lineal.

Del mismo modo, la clase de órdenes lineales densos sin puntos finales es elemental; de hecho, la densidad se enuncia mediante

$$\forall v_0 \forall v_1 \exists v_2 (v_0 < v_1 \to v_0 < v_2 \wedge v_2 < v_1),$$

y falta de puntos finales por

$$\forall v_0 \exists v_1 (v_1 < v_0),$$

$$\forall v_0 \exists v_1 (v_0 < v_1)$$

($v_0 < v_1$ abreviado aqui $v_0 \leq v_1 \wedge \neg(v_0 = v_1)$)

El conjunto de las consecuencias lógicas de las sentencias citadas hasta ahora es la teoría de los órdenes lineales densos sin puntos finales; lo denotaremos por DLO^- .

Está formado por las sentencias verdaderas en cada orden lineal denso sin puntos finales. Recordemos que $(Q, \leq)$, $(R, \leq)$ son órdenes lineales densos sin extremos, y en consecuencia sus teorías incluyen DLO^- (y cabe preguntarse si en realidad son iguales a DLO^-).

Teorema 3.2 Las fórmulas libres de cuantificador de $\mathscr{L}$ junto con una única sentencia de DLO^- (como $\exists v(v = v)$) son un conjunto de eliminación de DLO^-.

Demostración. Seguimos el mismo planteamiento que en el caso discreto. Pero ahora el símbolo sucesor no tiene sentido, nuestro lenguaje es más pequeño y, por tanto, nuestro escenario es más sencillo: los $\mathscr{L}-$términos son sólo variables (no surge ninguna constante porque no hay puntos finales). En consecuencia, lo que tenemos que hacer es eliminar el cuantificador en una fórmula

$$\exists w \alpha(\vec{v}, w)$$

donde $\alpha(\vec{v}, w)$ es una conjunción de condiciones que dicen que w es igual, o menor, o mayor que algún v en $\vec{v}$. Para obtenerlo, proceda como sigue. Ignoremos de nuevo trivialidades como $w = w$ (pueden enumerarse preliminarmente y reconocerse fácilmente); si no ocurre nada más, basta con sustituir nuestra fórmula por $\exists v(v = v)$.

Por el contrario, cuando se cumple una condición que no puede ser satisfecha por ninguna w, como $w < w$ (también estas afirmaciones negativas pueden ser enumeradas preliminarmente), sustituya nuestra fórmula por $\neg\exists v(v = v)$. En caso contrario, en cuanto se encuentre una ecuación $w = v_i$, suprima w y $\exists$, y sustituya w por v_i , en toda nuestra fórmula.

Por último, si sólo se producen inecuaciones y, por tanto, nuestra fórmula establece que w es menor que ciertas variables $(v_1, \dots, v_h$ sin pérdida de generalidad) y mayor que otras $(v_{h+1}, \dots, v_k)$, entonces obtenemos la fórmula sin cuantificador requerida de la siguiente manera.

Enumerar (en una disyunción adecuada) todas las posibles ordenaciones de $v_1, \dots, v_k$ en $\leq$ según las cuales $v_1, \dots, v_h$ preceden a $v_{h+1}, \dots, v_k$; para cada ordenación , que v, v' denotan respectivamente el elemento máximo entre $v_1, \dots, v_h$ y el menor entre $v_{h+1}, \dots, v_k$; $v < v'$ y la hipótesis de densidad son suficientes para garantizar que existe un w intermedio.

Cuando $h = 0$ o $h = k$, se utiliza la falta de puntos finales. Con esto concluye el procedimiento de eliminación. ■

Corolario 3.4 DLO^- es modelo completo y completo.

Demostración. La completitud del modelo es una consecuencia directa. La completitud puede deducirse como sigue, utilizando la completitud del modelo. Obsérvese primero que dos órdenes lineales densos cualesquiera sin extremos $(A, \leq)$ y $(B, \leq)$ se incrustan en una extensión común (por ejemplo, su suma $(A + B, \leq)$, donde $A + B$ es la unión disjunta de A y B, $\leq$ amplía los ordenamientos en A y B y, además, satisface $a < b$ para toda elección de $a \in A$ y $b \in B$). Como DLO^- es modelo completo, cada una de estas incrustaciones es elemental, en particular $(A, \leq)$ y $(B, \leq)$ son elementalmente equivalentes a su suma, y por tanto entre sí. ■

Corolario 3.5 Sea $A \models DLO^-$. Los subconjuntos A definibles en $\mathfrak{A}$ son solo las uniones finitas de intervalos (abiertos o cerrados), posiblemente con infinitos puntos finales.

Demostración. Proceda como para dLO^+. ■

4. Campos algebraicamente cerrados

4.1 Campos algebraicamente cerrados

Definición 4.1 — Campo algebraicamente cerrado.

Se dice que un campo $\mathscr{K}$ es algebraicamente cerrado si todo polinomio de grado positivo con coeficientes en $\mathscr{K}$:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad n > 0, \quad a_i \in \mathscr{K} \text{ con } 0 \leq i \leq n,$$

tiene al menos una raíz en $\mathscr{K}$.

■ **Ejemplo 4.1** $\mathbb{C}$ es un campo que verifica la condición de ser algebraicamente cerrado.

Definición 4.2 Se define la característica de un campo $\mathscr{K}$ como el menor entero positivo m tal que $1+1+\cdots+1 = 0$ (m veces). En caso de no existir tal m, se dice que la caracteristica de $\mathscr{K}$ es 0.

■ **Ejemplo 4.2** Tanto $\mathbb{R}$ como $\mathbb{C}$ son campos de carcaterística 0.

En cambio, para cada p primo, $\mathbb{Z}/p\mathbb{Z}$ es un campo (finito) de característica p.

Si un campo $\mathscr{K}$ tiene característica $n > 0$, entonces n es un número primo.

Tarski obtuvo sus célebres procedimientos de eliminación de cuantificadores para el campo complejo y el campo ordenado de los reales en los años treinta. Debido al parón provocado por la Guerra Mundial, no publicó sus resultados hasta 1948. Consideramos aquí el caso complejo, y aplazamos el real a la sección siguiente. Debemos subrayar que Tarski se ocupó de teorías de estructuras simples (el campo complejo, el campo ordenado de los reales) más que de clases axiomatizables (ACF, RCF). Pero un análisis cuidadoso de las pruebas identifica qué tipo de condiciones algebraicas son necesarias para garantizar el resultado de la eliminación del cuantificador: así uno se da cuenta de que lo que hace funcionar la maquinaria es simplemente ser algebraicamente cerrado en el caso complejo, y la propiedad del valor intermedio para los polinomios en el caso real.

Se trata de un resultado crucial, especialmente de cara a encontrar una axiomatización agradable para la teoría del campo complejo, o del campo ordenado de los reales. Como prometimos, aquí consideramos el caso complejo, pero preferimos un enfoque que trate toda la clase de campos algebraicamente cerrados.

Teorema 4.1 — Tarski.

La teoría *ACF* de campos algebraicamente cerrados tiene la eliminación de cuanlificadores en el lenguaje $\mathscr{L} = \{+, \cdot, -, {}^{\prime}, \infty\}$.

Demostración. Tomada una fórmula $\varphi(\vec{v}) \in \mathscr{L}$, buscamos una fórmula equivalente libre de cuantificador $\varphi'(\vec{v})$.

Como antes, podemos limitar nuestro análisis al caso en que $\varphi(\vec{v})$ es de la forma

$$\exists w \alpha(\vec{v}, w)$$

donde $\alpha(\vec{v}, w)$ es una conjunción finita de fórmulas atómicas y negaciones, todas ellas conteniendo w. En nuestro lenguaje, las fórmulas atómicas no son más que igualdades de términos, es decir, ecuaciones. Utilizando $-$, se puede expresar cada una de ellas como

$$p(\vec{v}, w) = 0$$

donde $p(\vec{y}, x)$ es un polinomio con coeficientes enteros.

En consecuencia $\varphi(\vec{v})$ es

$$\exists w \left(\bigwedge_{i \leq k} p_i(\vec{v}, w) = 0 \wedge \bigwedge_{j \leq h} \neg(q_j(\vec{v}, w) = 0) \right)$$

donde los $p_i's$ y los $q_j's$ son polinomios con coeficientes enteros, todos de grado positivo, n_i y m_j respectivamente, en x, por tanto respecto a w.

La teoría básica de campos nos dice que una secuencia de elementos en un campo excluye 0 si y sólo si su producto no es 0. En consecuencia, podemos suponer que a lo sumo se produce una inecuación en $\varphi(\vec{v}, w)$, digamos

$$\neg(q(\vec{v}, w) = 0)$$

donde $q(\vec{y}, x)$ es el producto de los polinomios $q_j(\vec{y}, x)$ cuando $j \leq h$, sea m el grado en x de $q(\vec{y}, x)$.

Llegados a este punto, cabe preguntarse si podemos reducir el número de ecuaciones de nuestra fórmula $\varphi(\vec{v}, w)$ para obtener como máximo una única ecuación.

Esto es cierto, y puede demostrarse utilizando de nuevo la teoría de campos pura (es decir, sin apelar al cierre algebraico), pero requiere algo más de sutileza. La idea es que, para un campo K dado y una secuencia $\vec{b}$ en K, las raíces comunes de los polinomios $p_i(\vec{b}, x)$ son sólo las raíces de su máximo común divisor, y que hay una fórmula libre de cuantificadores en $\vec{v}$, que define los coeficientes (en x) de este máximo común divisor, y es independiente de K y $\vec{b}$.

La primera afirmación está clara. Expliquemos los detalles de la segunda.

Consideremos $p_i(\vec{y},x)$ para $i \leq k$. Para cada i, escribamos $p_i(\vec{y},x)$ como un polinomio en x con coeficientes en $Z[\vec{y}]$

$$p_i(\vec{y},x) = \sum_{r \leq n_i} p_{i,r}(\vec{y})x^r.$$

Tomemos dos de estos polinomios, por ejemplo p_0 y p_1, y supongamos por simplicidad $n_0 \geq n_1$. Afirmamos que existe una fórmula libre de cuantificadores en $\vec{v}$ que produce, siempre que $p_1(\vec{v},x)$ no sea el polinomio nulo (en x), los coeficientes en x del cociente y el resto de la división de $p_0(\vec{v},x)$ por $p_1(\vec{v},x)$.

Para obtener esta fórmula, basta con seguir el procedimiento habitual de división de polinomios.

Se trata de un ejercicio tedioso pero sencillo. Por ejemplo, el primer paso consiste en escribir que

$$p_{1,n_1}(\vec{v}) = 0$$

o los coeficientes de $p_0(\vec{v},x)$ y $p_1(\vec{v},x)$ satisfacen

$$p_{1,n_1}(\vec{v})p_0(\vec{v},x) = p_{0,n_0}(\vec{v})p_1(\vec{v},x)x^{n_0-n_1} + P(\vec{v},x)$$

donde $P(\vec{v},x)$ es un polinomio de grado $< n_0$ en x, y, en este último caso, el cociente requerido admite

$$p_{0,n_0}(\vec{v})(p_{1,n_1}(\vec{v}))^{-1}x^{n_0-n_1}$$

como coeficiente de grado máximo.

En este punto, recordemos el algoritmo euclidiano de divisiones repetidas, que nos da el máximo común divisor (en x) de nuestros polinomios $p_i(\vec{y},x)(i \leq k)$ el último resto distinto de cero en una secuencia finita de divisiones sucesivas.

De nuevo, una fórmula adecuada libre de cuantificadores en $\vec{v}$ determina los coeficientes en x de nuestro máximo común divisor, siempre que los $p_i(\vec{v},x)'s$ $(i \leq k)$ no sean todos cero.

En conclusión, podemos suponer que nuestra fórmula $\varphi(\vec{v},w)$ tiene una de las tres formas siguientes:

1. $\exists w(p(\vec{v},w)=0)$,
2. $\exists w\neg(q(\vec{v},w)=0)$,
3. $\exists w(p(\vec{v},w)=0 \wedge \neg(q(\vec{v},w)=0))$

donde p y q son como antes.

Consideremos en primer lugar 1 . En cualquier campo, 1 equivale a decir que, si $\vec{v}$ elimina todos los coeficientes de $p(\vec{y},x)$ en x de grado positivo en x, entonces asigna el valor 0 también al término de grado 0 en x; esto puede escribirse como una fórmula adecuada libre de cuantificador en $\vec{v}$.

Consideremos ahora 2. En cualquier campo infinito, 2 equivale a decir que $\vec{v}$ no elimina los coeficientes del polinomio $p(\vec{y},x)$ en x. De nuevo, esta última afirmación puede expresarse mediante una fórmula libre de cuantificadores en $\vec{v}$. Finalmente tratemos con 3 . Afirmamos que, en cualquier campo algebraicamente cerrado, 3 es equivalente a la afirmación

$$(\star) \qquad\qquad p(\vec{v},x) \quad \text{no divide} \quad q(\vec{v},x)^n;$$

recordemos que n es el grado de $p(\vec{y},x)$ con respecto a x, y observemos que $(\star)$ puede expresarse como una fórmula sin cuantificador en $\vec{v}$ (basta con utilizar las observaciones anteriores sobre divisibilidad, y escribe que el resto de la división en $(\star)$ no es 0).

La dirección de izquierda a derecha es cierta en todo campo K: si, para una secuencia dada $\vec{b}$ en K, el eliminadro de $p(\vec{b},x)$ no está incluido en el eliminador de $q(\vec{b},x)$, entonces

$p(\vec{b},x)$ no puede dividir $q(\vec{b},x)$ y $(q(\vec{b},x))^n$. por el contrario, tome K y b como antes; suponga que toda raíz de $p(\vec{b},x)$ elimina también a para K algebraicamente cerrado, esto implica que todo factor lineal de $p(\vec{b},x)$ divide a $q(\vec{b},x)$ y, por tanto, que $p(\vec{b},x)$ divide a $q(\vec{b},x)^n$. Esto cumple nuestra prueba. ■

Comentemos ahora este resultado de eliminación del cuantificador y propongamos algunas consecuencias dignas de mención. En primer lugar , queremos destacar que la propiedad de eliminación de cuantificadores caracteriza a los campos algebraicamente cerrados entre los campos infinitos. De hecho, es un resultado profundo de Macintyre, McKenna y Van den Dries que un campo infinito cuya teoría elimina los cuantificadores en el lenguaje $\mathscr{L} = \{+,-,\cdot,0,1\}$ debe ser algebraicamente cerrado. Una consecuencia obvia de la eliminación de cuantificadores es la siguiente.

Corolario 4.1 ACF es un modelo completo.

Es evidente que el ACF no es completo. De hecho, para todo primo p, la sentencia $p = 0$ es verdadera en todo campo algebraicamente cerrado de característica p y falsa en todo campo algebraicamente cerrado de característica $\neq p$.

Corolario 4.2 Para todo $p = 0$ o primo, la teoría ACF_p es completa.

Demostración. Fijemos p. Existe un campo mínimo algebraicamente cerrado K_p de característica p: es el cierre algebraico del subcampo primo. K_p es incrustable en todo campo algebraicamente cerrado de la misma característica. Debido a la completitud del modelo de ACF_p, todas estas incrustaciones son elementales. En particular, todos los campos algebraicamente cerrados de característica p son elementalmente equivalentes a K_p y, en consecuencia, entre sí. ■

Como ya observamos en la sección 2.2, las teorías ACF_p agotan todas las posibles terminaciones de ACF en $\mathscr{L}$ cuando p abarca los primos y 0 (además, cada una de ellas tiene la eliminación del cuantificador en $\mathscr{L}$, simplemente porque extiende ACF). Una aplicación del teorema de la compacidad nos permite decir aún más. De hecho, hemos visto que la teoría del campo complejo es simplemente ACF_0, y por lo tanto está axiomatizada por ACF y, además, por las infinitas sentencias que afirman $\neg(p=0)$ para todo primo p. Sea σ una sentencia cualquiera de ACF_0. La compacidad nos dice que σ es una consecuencia de ACF y de un número finito de sentencias relativas a la característica. Por tanto, σ es cierta en todo campo algebraicamente cerrado de característica p para todos los $p's$ menos finitos. Así que hemos demostrado el siguiente resultado.

Teorema 4.2 Sea σ una sentencia del lenguaje $\mathscr{L}$. σ es verdadera en algún (equivalentemente todo) campo algebraicamente cerrado de característica 0 si y sólo si σ es verdadera en algún (equivalentemente todo) campo de característica p para todos menos un número finito de primos p.

Por lo tanto, lo que es cierto en el campo complejo (y en cualquier campo algebraicamente cerrado de característica 0) se cumple en los campos algebraicamente cerrados de característica p para casi todos los primos p. Veremos más adelante en esta sección una buena aplicación de este principio de transferencia de la teoría de modelos al álgebra. Tratemos ahora brevemente los problemas de decisión. Como ya se ha dicho, la decidibilidad se deduce de forma muy sencilla de la eliminación de cuantificadores.

Corolario 4.3 La teoría ACF de campos algebraicamente cerrados es decidible. ■

Demostración. Basta decidir si una sentencia dada σ de $\mathscr{L}$ libre de cuantificador está en ACF o no. Sin pérdida de generalidad, σ es una conjunción de disyunciones de sentencias atómicas y negaciones. Como una conjunción está en una teoría si y sólo si cada conjunción lo está, podemos escribir σ (hasta equivalencia, usando $-$) como

$$\left(\bigvee_i m_i = 0\right) \vee \left(\bigvee_j \neg(n_j = 0)\right).$$

donde $m_i's$ y $n_j's$ son enteros positivos. Así que nuestra sentencia sólo dice que la característica divide $\prod_i m_i$ o es coprima con algún n_j (o variantes adecuadas cuando no surge ninguna ecuación, o inecuación). Esto se puede comprobar fácilmente en el marco fijo. ■

Ocupémonos ahora de la definibilidad. Hemos visto en el capítulo 1 que, en cualquier campo K, los conjuntos construibles (en particular las variedades algebraicas) son definibles. El teorema 4.1 implica que, en campos algebraicamente cerrados, lo contrario también es cierto.

Corolario 4.4 En un campo algebraicamente cerrado K, para todo entero positivo n, un subconjunto de K^n es definible si y sólo si es construible.

Demostración. Basta demostrar que, si $X \subseteq K^n$ es definible, entonces X es constructible. Sea $\varphi(\vec{v}, \vec{w})$ una fórmula de $\mathscr{L}$ y $\vec{a}$ una secuencia en K que satisface

$$X = \varphi(K^n, \vec{a})$$

donde n es la longitud de $\vec{v}$. Utilizando la eliminación del cuantificador, podemos sustituir $\varphi(\vec{v}, \vec{w})$ por una fórmula equivalente que excluye los cuantificadores y, en consecuencia, es una combinación booleana finita de ecuaciones

$$q(\vec{v}, \vec{w}) = 0$$

donde $q(\vec{x}, \vec{y})$ es un polinomio con coeficientes en el subanillo generado por 1. Por lo tanto $X = \varphi(K^n, \vec{a})$ es la combinación booleana de las variedades algebraicas definidas por las fórmulas

$$q(\vec{v}, \vec{a}) = 0$$

y por tanto es un conjunto construible. ■

Obsérvese que en todo campo K los subconjuntos de K^n definibles mediante fórmulas libres de cuantificadores son construibles. La eliminación de cuantificadores garantiza que, cuando K es algebraicamente cerrado, no surge ningún otro conjunto definible. Consideremos ahora conjuntos definibles 1-arios en un campo algebraicamente cerrado K. En este marco restringido, se cumple la siguiente proposición.

Corolario 4.5 Sea K un campo algebraicamente cerrado, $X \subseteq K$ definible en K. Entonces X es finito o cofinito.

Demostración. Para cada $q(x,\vec{a}) \in K[x], q(v,\vec{a}) = 0$ define K si $q(x,\vec{a})$ es cero, y un conjunto finito en caso contrario. Una combinación booleana finita de conjuntos finitos o cofinitos sigue siendo finita o cofinita. ■

En realidad, podemos decir aún más. De hecho, en cualquier campo K (posiblemente no algebraicamente cerrado), un subconjunto X de K definible por una fórmula libre de cuantificador es o bien finito o cofinito. La eliminación del cuantificador extiende esta propiedad a subconjuntos arbitrarios 1-arios cuando K es algebraicamente cerrado.

Para concluir esta sección, queremos proponer una bonita aplicación de la Teoría de Modelos al Álgebra dentro de campos algebraicamente cerrados. Se trata del llamado Teorema de la inyectividad-implica-sobreyectividad. La compacidad, y la consecuente observación de que las sentencias verdaderas en el campo complejo son sólo las satisfechas por los campos algebraicamente cerrados de característica p para casi todos los primos p, se utilizan para deducir;

Teorema 4.3 Todo morfismo inyectivo f de una variedad algebraica V sobre el campo complejo hacia la propia V es sobreyectiva.

Demostración. Ya hemos notado que cualquier variedad algebraica es un conjunto definible, e incluso está definida por una conjunción finita de ecuaciones (posiblemente con parámetros). En particular, la fórmula

$$\bigwedge_{j \leq t} p_j(\vec{v},\vec{a}) = 0$$

sea K de esta forma (los $p_j's$ son polinomios con coeficientes enteros, y $\vec{a}$ denota una secuencia de parámetros complejos). Análogamente, un morfismo entre variedades es un mapa definido por una conjunción finita de ecuaciones. En consecuencia

$$\bigwedge_{i\leq s} q_i(\vec{v},\vec{w},\vec{a}) = 0$$

rendimiento f (los $q_i's$ son de nuevo polinomios con coeficientes enteros; podemos utilizar aquí libremente los mismos parámetros o que antes; si es necesario, ampliamos o para incluir nuevos números complejos).

En este punto es un ejercicio fácil escribir una sentencia de primer orden en el lenguaje $\mathscr{L}$ (sin parámetros) diciendo: para todo $\vec{z}$, si $\bigwedge_{i\leq s} q_i(\vec{v},\vec{w},\vec{z}) = 0$ define un morfismo desde la variedad dada por $\bigwedge_{j\leq t} p_j(\vec{v},\vec{z}) = 0$ hacia sí misma, y este morfismo es inyectivo, entonces es sobreyectivo.

Denotemos n, como de costumbre, la longitud de $\vec{v}$. Lo que tenemos que demostrar es que el campo complejo es un modelo de todas estas sentencias cuando los $p_j's$ y los $q_i's$ abarcan los polinomios con coeficientes enteros, equivalentemente que ACF_0 incluye estas sentencias. Utilizando la compacidad, podemos comprobar alternativamente lo que ocurre en ACF_p cuando p es un primo, y por tanto si las sentencias anteriores son ciertas en todo campo algebraicamente cerrado de característica p; como ACF_p es completo, basta con observar el comportamiento de un único modelo de ACF_p, por ejemplo del cierre algebraico $\overline{F}_p$ del campo F_p con P elementos: una respuesta positiva en $\overline{F}_p$ para p suficientemente numerosos implica una respuesta positiva para el campo complejo. Tomemos pues una variedad algebraica V sobre $\overline{F}_p$ y un morfismo inyectivo f de V a V sobre $\overline{F}_p$. Utilicemos el hecho algebraico de que $\overline{F}_p$, es localmente finito y representemos V como la unión de sus intersecciones con F^n donde F abarca los subcampos finitos de $\overline{F}_p$ (que contienen los parámetros que definen V y f). Recordemos el principio trivial de que toda función inyectiva de un conjunto finito a sí mismo es también sobreyectiva. Deduzcamos que la restricción de f a $V \cap F^n$ es sobreyectiva para todo F. Extendamos este resultado a f : f es sobreyectiva, como se requiere. ■

4.2 Otra vez Tarski: Campos cerrados reales

Definición 4.3 Sea el lenguaje $\mathscr{L} = \{0, 1, +, -, \cdot, \leq\}$ para un $\mathscr{K}$ campo ordenado. Consideremos las siguientes sentencias en $\mathscr{L}$

1. Los axiomas de campo,
2. Las que caracterizan los órdenes lineales,
3. La sentencia que dice que las sumas y los productos de elementos no negativos son no negativos.

$$\forall v_0 \forall v_1 (0 \leq v_0 \wedge 0 \leq v_1 \to 0 \leq v_0 + v_1 \wedge 0 \leq v_0 \cdot v_1).$$

4. Para todo n natural

$$\forall v_0 \forall v_1 \ldots \forall v_n \forall u \forall w \exists v (v_0 + v_1 \cdot u + \cdots + v_n \cdot u^n + u^{n+1} < 0 \wedge$$
$$\wedge 0 < v_0 + v_1 \cdot w + \cdots + v_n \cdot w^n + w^{n+1} \wedge u < w \to$$
$$\to u < v \wedge v < w \wedge v_0 + v_1 \cdot v + \cdots + v_n \cdot v^n + v^{n+1} = 0).$$

Las consecuencias lógicas de (1),(2),(3), (4) forman la teoría de los campos reales ordenados cerrados, denotado RCF.

En esta sección nos ocupamos del teorema de eliminación del cuantificador para campos cerrados reales. Se trata del principal resultado de Tarski en este marco, no sólo porque, como veremos, la demostración es más profunda y complicada que en el caso complejo, sino también porque el campo ordenado de los reales está intrínsecamente relacionado con la geometría. No es necesario recordar que, por ejemplo, en el plano euclídeo equipado con algunos ejes cartesianos fijos, cada punto es esencialmente un par ordenado de reales, cada línea recta es la variedad dada por un polinomio de grado 1 y 2 incógnitas sobre los reales, etc.

Por consiguiente, las afirmaciones sobre puntos, líneas, etc., se basan en el campo ordenado de los reales. En consecuencia, las afirmaciones sobre puntos, rectas, ... pueden traducirse fácilmente en afirmaciones sobre reales, sumas, multiplicaciones (a menudo de primer orden). En particular, un algoritmo de decisión sobre la teoría del campo ordenado de los reales (el álgebra elemental según la terminología de Tarski) debería funcionar también para la geometría euclidiana (de primer orden). En realidad, el procedimiento de eliminación de cuantificadores de Tarski se refería a los reales y no a la teoría RCF.

Pero, al igual que en el caso complejo, uno puede darse cuenta de que los ingredientes básicos de la prueba se refieren a campos cerrados reales arbitrarios. Así que enunciamos (y mostramos) el resultado en este entorno (aparentemente ampliado); pero deduciremos rápidamente que RCF es completa y, por tanto, igual a la teoría de $(\mathbb{R},+,-.\cdot,0,1,\leq)$. Seguimos el elegante enfoque de Cohen en lugar de la prueba original de Tarski.

Teorema 4.4 La teoría RCF de campos cerrados de carretes tiene la eliminación de cuantificadores en el lenguaje $\mathscr{L}=\{+,-,\cdot,0,1,\leq\}$.

Demostración. Procediendo como en el caso de campos algebraicamente cerrados, uno se da cuenta preliminarmente de que el meollo de la cuestión es eliminar el cuantificador $\exists$ en una fórmula

$$\exists w\alpha(w,\vec{v})$$

donde $\alpha(w,\vec{v})$ es la conjunción de a lo sumo una ecuación $p(w,\vec{v})=0$ y un conjunto finito (posiblemente vacío) de inecuaciones $q_i(w,\vec{v})>0$ (con $j\leq n$), donde $p(x,\vec{y})$ y $q_j(x,\vec{y})(j\leq m)$ son polinomios con coeficientes enteros.

Así pues, abramos un paréntesis (largo) y examinemos un polinomio arbitrario $f(x) = \sum_{i\leq t} f_i x^i$ con coeficientes en un campo real cerrado K. Se sabe que, si f_i no es 0 para todo $i \leq t$, entonces $f(x)$ tiene a lo sumo t raíces en el campo. Fijemos t.

Entonces se ve fácilmente que

1. a función que calcula, para cada polinomio $f(x)$ como antes, equivalentemente para cada secuencia no nula $(f_0,\ldots,f_t)$ en K^{t+1}, cuántas raíces admite $f(x)$ así como, para cada r y s con $1 \leq r \leq s < t$,
2. el conjunto de secuencias no nulas $(f_0,\ldots,f_t)$ en K^{t+1} tales que $f(x)$ tiene exactamente s raíces,
3. la función que convierte cualquier raíz no nula $(f_0,\ldots,f_t)$ en la raíz r-ésima de $f(x)$

son definibles en cualquier campo ordenado K de manera uniforme (independiente de K). Afirmamos que, dentro de campos reales cerrados, para cada t, estos objetos son definibles mediante fórmulas sin cuantificador, también de manera uniforme (independientemente del campo subyacente). Para ver esto, se utiliza la teoría de Sturm del recuento de raíces reales. Procedemos por inducción en t. El caso $t = 0$ está claro: el número de raíces es 0 si $f_0 \neq 0$, e indefinido en caso contrario; 2 y 3 son objetos vacíos. Así que supongamos $t > 0$y supongamos nuestra afirmación cierta para todo valor natural $< t$, para extenderla a t. La idea aquí es relacionar los ceros de $f(x)$ con las raíces de su derivada y el signo de $f(x)$ en estas raíces. De ahí que construyamos la derivada formal $f'(x)$ de $f(x)$ con respecto a x

$$f'(x) = \sum_{0\leq i\leq t} i f_i x^{i-1}$$

Preliminarmente, nótese que $f'(x) = 0$ si y sólo si $(f_1,\ldots,f_t) = (0,\ldots,0)$.

Excepto en este caso, la inducción nos proporciona fórmulas libres de cuantificadores que definen (con respecto a $(f_0,\ldots,f_t)$ a través de $(f_1, 2f_2,\ldots,tf_t)$)

1. la función contar, para cada secuencia $(f_0,\ldots,f_t)$ con $(f_1,\ldots,f_t) \neq (0,\ldots,0)$, cuán-

tas raíces admite $f'(x)$, y, para $1 \leq r \leq s < t$

2. el conjunto de las sucesiones $(f_0, \ldots, f_t)$ en K^{t+1} tales que $(f_1, \ldots, f_t)$ no es cero y $f'(x)$ tiene exactamente s raíces,
3. la función que convierte cualquier (adecuado) distinto de cero $(f_0, \ldots, f_t)$ en la raíz r-ésima de $f'(x)$.

Ahora ordena las raíces de $f'(x)$

$$\rho_1 < \cdots < \rho_s.$$

La propiedad del valor intermedio, que se cumple en todo campo real cerrado, garantiza que $f'(x)$ no puede cambiar de signo entre dos raíces sucesivas. ¿Podemos deducir que $f(x)$ es monótona (creciente o decreciente según el signo de $f'(x)$) en el mismo intervalo? Ciertamente sí en el caso del campo real: es un resultado bien conocido en análisis real elemental. Pero se puede hacer una demostración algebraica completa (aunque no trivial) para polinomios utilizando sólo los axiomas de RCF. En consecuencia, en todo campo real cerrado K, $f(x)$ es monótono (creciente o decreciente según el signo -positivo o negativo- de su derivada) en cada intervalo $(\rho_i, \rho_{i+1}), 1 \leq i < s$. Ahora mira $f(\rho_i)$ y $f(\rho_{i+1})$

(i) Si no son 0 y su signo es el mismo, entonces (ρ_i, ρ_{i+1}) no contienen cualquier raíz de $f(x)$ porque $f(x)$ es monótona en el intervalo (obsérvese que los casos en que exactamente uno entre ρ_i y ρ_{i+1} elimina a $f(x)$ pueden tratarse de forma similar).

- Si $f(\rho_i)$ y $f(\rho_{i+1})$ admiten signos opuestos, entonces (ρ_i, ρ_{i+1}) sí contiene una raíz de $f(x)$ por la propiedad del valor intermedio. La unicidad de esta raíz podría deducirse del Teorema de Rolle (dos raíces distintas de $f(x)$ $\rho_i < a < b < \rho_{i+1}$ determinar una nueva raíz intermedia de $f'(x)$, y esto es imposible). El análisis elemental garantiza que el Teorema de Rolle es cierto para los reales; pero, de nuevo, se puede dar una prueba algebraica alternativa y no trivial (para polinomios) que se cumple en todos los campos reales cerrados.

- Supongamos por fin $f(\rho_i) = f(\rho_{i+1}) = 0$. El argumento en 2 excluye de nuevo cualquier raíz intermedia adicional de $f(x)$.

Esta maquinaria nos permite contar las raíces en el intervalo $[\rho_1, \rho_s]$. Pero, ¿qué podemos decir en (∞, ρ_1) y $(\rho_s, +\infty)$?

Los mismos argumentos de antes garantizan que $f(X)$ es monótona, y en cada una de estas semirrectas aparece al menos una raíz. Pero nuestro escenario cambia cuando examinamos la existencia de esta raíz. En efecto, todo intervalo $(\rho_i, \rho_{i+1})(1 \leq i \leq s)$ es acotado, mientras que nuestras semirrectas son no. Sin embargo, el siguiente hecho algebraico nos ayuda.

Sea $f(x) = \sum_{i \leq t} f_i x^i$ como antes. Entonces $f(x)$ no tiene raíces fuera del intervalo $[-a, a]$ donde $a = 3t\,\text{máx}\{(|f_{t-i}f_t^{-1}| : 0 < i \leq t\} + 1$

(La prueba sólo utiliza los axiomas de los campos ordenados). Así, una posible raíz menor que ρ_1 debe estar en $[-a, \rho_1)$, y una posible raíz mayor que ρ_s debe pertenecer a $(\rho_s, a]$; además, la función de valor absoluto $||$ se puede definir de forma libre de cuantificadores, ya que, para cada $b \in K, |b|$ es b cuando $b \geq 0$ y $-b$ en caso contrario. Por tanto, nos encontramos en un marco acotado y podemos proceder como en los casos anteriores.

En conclusión, hemos proporcionado un procedimiento uniforme que cuenta, para cada no cero $(f_0, \ldots, f_t)$ en K, cuántas raíces admite $f(x)$. La función que calcula su número s está definida por una fórmula sin cuantificador (que comprueba esencialmente el signo de $f(x)$ en las raíces de su derivada y en $\pm a$). Del mismo modo, el conjunto de secuencias no nulas $(f_0, \ldots, f_t)$ en K para las que $f(x)$ tiene exactamente s raíces puede definirse comprobando estas relaciones de signo y formando una disyunción de primer orden adecuada para enumerar los casos en los que se produce s.

Por último, la función que produce, para cada $(f_0,\ldots,f_t)$ distinto de cero y $1 \leq r \leq s$, la raíz r-ésima de $f(x)$ se define fácilmente sobre la misma base. Con esto se cumple la prueba de la afirmación y termina nuestro paréntesis. Ahora volvemos a la eliminación del cuantificador. Recordemos que estamos considerando una fórmula

$$(a) \qquad \exists w(p(w,\vec{v}) = 0 \wedge \bigwedge_{j\leq m} q_j(w,\vec{v}) > 0)$$

o

$$(b) \qquad \exists w \bigwedge_{j\leq m} q_j(w,\vec{v}) > 0$$

donde$p(x,\vec{y})$ y $q_j(x,\vec{y})(j \leq m)$ son polinomios con coeficientes enteros. Cada uno de ellos se puede escribir como un polinomio con coeficientes en $\mathbb{Z}[\vec{y}]$ de la siguiente manera

$$p(x,\vec{y}) = \sum_{i\leq t} p_i(\vec{y})x^i,$$

$$q_j(x,\vec{y}) = \sum_{i\leq t_j} q_{j,i}(\vec{y})x^i.$$

(a) se reduce rápidamente a (b) porque su fórmula es equivalente a

$$(\bigwedge_{i\leq t} p_i(\vec{v} \wedge \exists w \bigwedge_{j\leq m} q_j(w,\vec{v}) > 0) \vee$$

$$\bigvee_{1\leq r\leq s\leq t} (\text{"}p(x,\vec{v}) \text{ tiene } s \text{ raíces"} \wedge$$

$$\wedge \text{ la } r\text{-ésima ráiz } \rho_r(\vec{v}) \text{ satistface } \bigwedge_{j\leq m} q_j(\rho_r(\vec{v}),\vec{v}) > 0\text{''}$$

donde esta última disyunción puede expresarse mediante una fórmula de primer orden sin cuantificador. Veamos (b). Para cada $j \leq m$ y para cada $s_j \leq t_j$, existen fórmulas libres de cuantificadores que definen, para cada campo real cerrado K, el conjunto de las sucesiones $\vec{b}$ tales que $q(x,\vec{b})$ tiene s_j raíces en x, y que enumeran estas raíces

$$\rho_{j,1}(\vec{b}) < \cdots < \rho_{j,s_j}(\vec{b}).$$

Se puede calcular el signo de $q_j(x,\vec{b})$ en los intervalos

$$(-\text{ínf}, \rho_{j,1}(\vec{b})),$$

$$(\rho_{j,i}(\vec{b}), \rho_{j,i+1}(\vec{b})) \quad (1 \leq i < s_j,$$

$$(\rho_{j,s_j}(\vec{b}, +\infty)$$

de manera uniforme (independiente de K y $\vec{b}$) observando el valor (de signo) de

$$q_j(\rho_{j,1}(\vec{b}) - 1, \vec{b})$$

$$q_j(\frac{\rho_{j,i}(\vec{b}) + (\rho_{j,i+1}(\vec{b})}{2}, \vec{b})$$

$$q_j(\rho_{j,s_j}(\vec{b}) + 1, \vec{b})$$

respectivamente. Enumerar todas las posibles ordenaciones de las raíces (en x) de las $q_j(x,\vec{b})'s$ cuando j se extiende sobre los números naturales $\leq m$, y dividir en cada caso K en un número finito de intervalos tales que las $q_j(x,\vec{b})'s$ tengan un signo constante (con respecto a x) en cada uno de ellos; comprobar estos signos (de la forma sugerida antes) y formar una disyunción adecuada escogiendo los intervalos donde todos estos signos son positivos. Este procedimiento es independiente de K y $\vec{b}$ y proporciona la fórmula sin cuantificador requerida. ■

Corolario 4.6 *RCF* es un modelo completo.

Corolario 4.7 *RCF* es completa en particular, *RCF* es la teoría del campo ordenado de los reales (así como de cada campo cerrado real).

Demostración. Existe un campo cerrado real mínimo ordenado, incrustado en cualquier modelo de *RCF*. Se trata del campo ordenado $\mathbb{R}_0$ de los números algebraicos reales. La completitud del modelo de *RCF* garantiza que todo campo real cerrado es una extensión elemental de $\mathbb{R}_0$. En particular, todos los campos reales cerrados son elementalmente equivalentes a $\mathbb{R}_0$ y, en consecuencia, entre sí. ■

Esta es la primera prueba de completitud que damos sobre la *RCF*; de hecho el criterio de Vaught's no se aplica porque la *RCF* no es categórica en ninguna potencia infinita.

Hemos visto que los campos reales cerrados eliminan cuantificadores en su lenguaje $\mathscr{L} = \{+,-,\cdot,0,1,\leq\}$. Notablemente, están completamente caracterizados por esta propiedad: Macintyre, McKenna y Van den Dries demostraron que un campo orderado, cuya teoría tiene la eliminación de cuantificadores en $\mathscr{L}$, debe ser real cerrado. También observamos que *RCF* no conserva la eliminación del cuantificador en el lenguaje restringido $\mathscr{L}' = \{+,-,\cdot,0,1\}$ sin orden. En realidad se puede recordar que, incluso al comprobar la resolubilidad de la popular ecuación $ax^2+bx+c=0$ con grado 2 y 1 desconocido sobre los reales (o sobre cualquier campo real cerrado), se necesita una inecuación $b^2-4ac \geq 0$ para asegurar raíces, y de ahí eliminar $\exists$ en la fórmula $\exists w(v_2w^2+v_1w+v_0=0)$. Más formalmente, recordemos que, con respecto a la teoría del campo real, las fórmulas

$$\varphi(v) : v \geq 0$$

$$\varphi'(v) : \exists w(v = w^2)$$

son equivalentes. Como la *RCF* es completa y, por tanto, igual a la teoría del campo real, lo mismo ocurre en todo campo real cerrado. En consecuencia, la $\mathscr{L}$-fórmula (con el cuantificador $\exists$)

$$\varphi'(v) : \exists w(v = w^2)$$

define el conjunto de elementos no negativos en todo campo real cerrado. Sin embargo, no puede ser equivalente en *RCF* a ninguna $\mathscr{L}-$fórmula libre de cuantificador $\varphi''(v)$. De hecho $\varphi(\mathbb{R})$ es la semirrecta $[0,+\infty[$ de $\mathbb{R}$, y por tanto es infinita y coinfinita, mientras que $\varphi''(K)$ es finita o cofinita para todo campo K: véase la demostración del teorema 4.5. Ahora discutimos la decidibilidad: como ya se ha dicho, ésta era la principal consecuencia de la eliminación de los cuantificadores, según el sentir general en los años cuarenta.

Corolario 4.8 *RCF* es decidible.

Demostración. Debido a la eliminación del cuantificador, cada $\mathscr{L}-$sentencia σ es equivalente en *RCF* a una combinación booleana de sentencias $m = n$ o $m < n$ donde m y n son números enteros. Esta afirmación sin cuantificador puede comprobarse fácilmente en nuestro marco. ■

Examinemos ahora otra consecuencia notable de la eliminación de cuantificadores, a saber, la definibilidad. Recordemos que, en un campo ordenado K, todo conjunto semialgebraico (en otras palabras, toda combinación booleana finita de conjuntos de soluciones de inecuaciones

$$q(\vec{x}) \geq 0$$

con $q(\vec{x}) \in K[\vec{x}]$ es definible.

Corolario 4.9 En un campo ordenado real cerrado K, los conjuntos definibles son exactamente los semialgebraicos.

Demostración. Sea n un número entero positivo,$X \subseteq K^n$ un conjunto definible en K. Entonces hay una fórmula '$\varphi(\vec{v},\vec{w})$ de $\mathscr{L}$ y una secuenciañ $\vec{a} \in K$ tales que

$$X = \varphi(K^n,\vec{a})$$

Debido al teorema de eliminación del cuantificador de Tarski, podemos suponer que $\varphi(\vec{v},\vec{w})$ no tiene cuantificador y, por tanto, es una combinación booleana finita de inecuaciones

$$q(\vec{v},\vec{w} \geq 0$$

con $q(\vec{x},\vec{y} \in Z[\vec{x},\vec{y}]$. Por lo tanto, X es una combinación booleana finita de conjuntos de soluciones de las disecuaciones

$$q(\vec{v},\vec{a}) \geq 0$$

y por lo que es un conjunto semialgebraico. ■

■ **Ejemplo 4.3** Consideremos la siguiente afirmación: para una función semialgebraica f de $\mathbb{R}^{n+1} \to \mathbb{R}$, el conjunto A de las secuencias $\vec{x}$ en $\mathbb{R}^{n+1}$ tales que es semialgebraica.

Si se sustituye en todas partes semialgebraico por definible, esta proposición puede perder parte de su glamour (matemático). Pero, utilizando la lógica, se obtiene una breve demostración: A es definible mediante la fórmula

$$\varphi(\vec{v} : \exists w \forall \varepsilon(\varepsilon > 0 \to \exists r \forall y(y > r) \to$$

$$\to \exists z(f(\vec{v}, y) = z \wedge |z - w| < \varepsilon)))$$

(recuérdese que tanto f como el valor absoluto son definibles). Una aproximación directa mediante conjuntos semialgebraicos y proyecciones es más larga. En un campo real cerrado K, los subconjuntos definibles $X \subseteq K$ tienen una forma muy sencilla forma.

Corolario 4.10 Sea K un campo real cerrado y X un subconjunto definible de K. Entonces X es una unión de intervalos (cerrados o abiertos, posiblemente con extremos infinitos).

Demostración. Sea $q(x) \in K[x]$. Sabemos que $q(v) = 0$ define K si $q(x) = 0$ y un conjunto finito (es decir, el conjunto de las raíces $a_0 < \cdots < a_s$ de $q(x)$ en K) en caso contrario. Por otra parte, $q(v) > 0$ define $\emptyset$ si $q(x) = 0$; en caso contrario $q(v) > 0$ define la unión de algunos intervalos entre $]-\infty, a_0[,]a_0, a_1[, \ldots,]a_s, +\infty[$ (recuérdese que K satisface la propiedad de valor intermedio para polinomios). Por tanto, cualquier conjunto definible (equivalentemente, semialgebraico) $X \subseteq K$ es una combinación booleana finita de intervalos, y por tanto una unión finita de intervalos. ■

5. Eliminación-pp de cuantificadores y módulos

En esta sección nos ocupamos de los módulos (de izquierda) sobre un anillo (contable) **R** con identidad. Sea el lenguaje adecuado $\mathscr{L}_{\mathbb{R}}\{o,+,-,r(r\in\mathbb{R})\}$ para estas estructuras, axiomatizables mediante sentencias de primer orden en $\mathscr{L}_{\mathbb{R}}$.

Denotemos $\mathscr{T}_{\mathbf{R}}$ la teoría correspondiente. Un rápido vistazo a los axiomas de $\mathscr{T}_{\mathbf{R}}$ muestra que cada uno de ellos es una sentencia universal $\forall\vec{v}\alpha(\vec{v})$ donde $\alpha(\vec{v})$ es una fórmula atómica de $\mathscr{L}_{\mathbb{R}}$; esto confirma que la clase de los modelos de $\mathscr{T}_{\mathbf{R}}$ (a saber, de los **R**-módulos) es cerrada bajo subestructuras.

Ahora nos preguntamos si $\mathscr{T}_{\mathbf{R}}$ tiene eliminación de cuantificadores en $\mathscr{L}_{\mathbb{R}}$. Un ejemplo trivial muestra que esto es falso incluso en el caso simple en que **R** es el anillo $\mathbb{Z}$ de enteros. De hecho, basta considerar $\mathbb{Z}$ como un módulo sobre sí mismo. En $\mathbb{Z}$ la fórmula

$$\varphi(v) : \exists w(v=2w)$$

define el conjunto $2\mathbb{Z}$ de enteros pares. Por otro lado, toda fórmula atómica $\varphi'(v)$ en $\mathscr{L}_{\mathbb{Z}}$ es equivalente dentro de $\mathscr{T}_{\mathbb{Z}}$, y por tanto en la teoría del $\mathbb{Z}$-módulo, a

$$rv=0$$

para algún entero no negativo r. Esta fórmula define en $\mathbb{Z}\{0\}$ si $r \neq 0$ y $\mathbb{Z}$ en caso contrario. Ninguna combinación booleana de estos conjuntos puede ser igual a $2\mathbb{Z}$. Por lo tanto ninguna fórmula libre de cuantificador $\varphi'(v)$ de $\mathscr{L}_{\mathbb{Z}}$ es equivalente a $\varphi(V)$ en $Th(\mathbb{Z})$, y así en $\mathscr{T}_{\mathbb{Z}}$.

De ello se deduce que $\mathscr{T}_{\mathbb{Z}}$ no elimina los cuantificadores en $\mathscr{L}_{\mathbb{Z}}$. Sin embargo, observe que $\varphi(v)$ es una pp-fórmula típica en $\mathscr{L}_{\mathbb{Z}}$. De hecho, veremos que, para cualquier $\mathbb{R}$, las pp-fórmulas de $\mathscr{L}_{\mathbb{R}}$ son justo el único obstáculo a la eliminación de cuantificadores de $\mathscr{T}_{\mathbb{R}}$ en $\mathscr{L}_{\mathbb{R}}$. Veamos por qué. Tomemos cualquier anillo (contable) **R** con identidad. Recordemos que una pp-fórmula pp de $\mathscr{L}_{\mathbb{R}}$ es una fórmula existencial de la forma

$$\varphi(\vec{v} : \exists \vec{w}(A \cdot \vec{v} = B \cdot \vec{w})$$

donde A y B son matrices con coeficientes en **R** de tamaños adecuados, denota el producto habitual fila por columna entre matrices, y $\vec{v}$, $\vec{w}$ deben verse como vectores columna (con un número adecuado de filas). Así, cuando $\vec{w} = \emptyset$, las pp-fórmulas incluyen las fórmulas atómicas de

$$\mathscr{L}_{\mathbb{R}}$$

. Para cada pp-fórmula $\varphi(\vec{v})$ de $\mathscr{L}_{\mathbb{R}}$ y cada **R**-módulo $\mathfrak{M}$, $\varphi(\mathfrak{M}^n)$ es un subgrupo de $\mathfrak{M}^n$ (llamado subgrupo pp-definible), pero no es en general un submódulo. Añadamos aquí algunas observaciones más sobre las pp-fórmulas.

Veamos las siguientes notas:

1. *Si $\varphi(\vec{v}), \psi(\vec{v})$ son pp-fórmulas de $\mathscr{L}_{\mathbb{R}}$, entonces también $\varphi(\vec{v}) \wedge \psi(\vec{v})$ es (equivalente en $T_{\mathbf{R}}$) una pp-fórmula.*

2. *Sea $\varphi(\vec{v}, \vec{z})$ una pp-fórmula de $\mathscr{L}_{\mathbb{R}}$, $\varphi(\vec{v}, \vec{z}) : \exists \vec{w}(A^t(\vec{v}, \vec{z}) = B\vec{w})$.*

Entonces $\varphi(\vec{v},\vec{0})$ *es una pp-fórmula, y por tanto, para todo* $\mathbf{R}$*-módulo* $\mathfrak{M}$, $\varphi(\mathfrak{M}^n,\vec{0})$ *es un subgrupo pp-definible de* $\mathfrak{M}^n$*. Además, para cada* $\vec{a} \in M, \varphi(\mathfrak{M}^n,\vec{a}) = \emptyset$ *o* $\varphi(\mathfrak{M}^n,\vec{a})$ *es una clase* $\varphi(\mathfrak{M}^n,0)$ *en* M *(de hecho, dado* $\vec{b} \in \varphi(\mathfrak{M}^n,\vec{a})$*, es fácil comprobar* $\varphi(\mathfrak{M}^n,\vec{a}) = \varphi(\mathfrak{M}^n,0) + \vec{b}$*).*

3. *Sean* $\varphi(\vec{v}), \psi(\vec{v})$ *pp-fórmulas de* $\mathscr{L}_{\mathbb{R}}$ *con n variables libres, y sea k un número entero positivo. Es sencillo escribir una sentencia en* $\mathscr{L}_{\mathbb{R}}$ *que asegure que, en un* $\mathbf{R}$*-módulo* $\mathfrak{M}$ *dado el índice de* $\varphi(\mathfrak{M}^n) \cap \psi(\mathfrak{M}^n)$ *en* $\varphi(\mathfrak{M}^n)$ *es* $\geq k$ *en detalle esta sentencia dice*

$$\exists\vec{v}_0 \ldots \exists\vec{v}_{k-1} \left(\bigwedge_{i<k} \varphi(\vec{v}_i) \wedge \bigwedge_{i<j<k} \neg\psi(\vec{v}_i - \vec{v}_j) \right)$$

La denotaremos por $(\varphi : \psi) \geq k$*. Cualquier sentencia de esta forma se llama enunciado invariante (veremos más adelante la razón). Obsérvese que las combinaciones booleanas finitas de enunciados invariantes incluyen las sentencias que dicen:*

- *el índice de* $\varphi(\mathfrak{M}^n \cap \psi(\mathfrak{M}^n)$ *en* $\varphi(\mathfrak{M}^n)$ *es k ("*$= k$*" significa "* $\geq k$*" sino "* $\not\geq k+1$*"); denotaremos esta fórmula por* $(\varphi : \psi) = k$*;*
- *el índice de* $\varphi(\mathfrak{M}^n \cap \psi(\mathfrak{M}^n)$ *en* $\varphi(\mathfrak{M}^n)$ *es* $\leq k$ *("*$\leq k$*" significa* $\not\geq k+1$*; denotaremos esta fórmula por* $(\varphi, \psi) \leq k$*.*

Llegados a este punto podemos enunciar y demostrar el siguiente teorema fundamental (de pp-eliminación de cuantificadores para módulos).

Teorema 5.1 — Baur - Monk.

Sea $\mathbf{R}$ un anillo (contable) con identidad. Entonces las pp-fórmulas de $\mathscr{L}_{\mathbb{R}}$ junto con los enunciados invariantes forman un conjunto de eliminación para $\mathscr{T}_{\mathbf{R}}$ en $\mathscr{L}_{\mathbb{R}}$. Más precisamente: para cada fórmula $\alpha(\vec{v})$ de $\mathscr{L}_{\mathbb{R}}$, hay una combinación booleana β de enunciados invariantes y una combinación booleana $\gamma(\vec{v})$ de pp-fórmulas tales que

$$\forall\vec{v}(\alpha(\vec{v}) \iff \beta\wedge\gamma(\vec{v}))\in T_{\mathbf{R}}.$$

Se utilizará en está demostración el siguiente resultado de la teoría de grupos.

Lema 5.0.1 — B. H. Neumann.

Sea $\mathfrak{G}$ un grupo, $a, a_i \in G, H, H_i$ sean subgrupos de $\mathfrak{G}$ (donde i varia entre los naturales menores que algún N fijo), $aH \subseteq \bigcup\limits_{i<N} a_iH_i$. Sea I el conjuntos de los naturales $i<N$ para los cuales $|H : H\cap H_i| \leq N!$. Entonces $aH \subseteq \bigcup\limits_{i\in I} a_iH_i$.

Comencemos ahora la demostración del teorema.

Demostración. Procedemos por inducción sobre $\alpha(\vec{v})$. Si $\alpha(\vec{v})$ es una fórmula atómica, entonces $\alpha(\vec{v})$ es directamente una pp-fórmula. Los casos y $\neg$ y $\wedge$ son fáciles de manejar.

Supongamos entonces que $\alpha(\vec{v})$ es de la forma $\forall w\alpha'(w,\vec{v})$, donde la hipótesis de inducción garantiza que existe un enunciado invariante β' y una combinación booleana $\gamma'(w,\vec{v})$, de pp-fórmulas tales que

$$\forall w\forall\vec{v}(\alpha'(w,\vec{v}) \iff \beta'\wedge\gamma'(w,\vec{v}))\in\mathscr{T}_{\mathbb{R}}.$$

1^{era} reducción: sin pérdida de generalidad, $\alpha'(w,\vec{v})$ es una disyunción de pp-fórmulas o negaciones. En efecto, $\forall\vec{v}(\alpha(\vec{v}) \iff \beta'\wedge\forall w\gamma'(w,\vec{v}))\in\mathscr{T}_{\mathbb{R}}$. En consecuencia, podemos sustituir $\alpha'(w,\vec{v})$ por $\gamma'(w,\vec{v})$, que es una combinación booleana de pp-fórmulas y, por tanto, equivalente a una conjunción de disyunciones de pp-fórmulas o negaciones. Correspondientemente ponga $\alpha'(w,\vec{v}) : \bigwedge\limits_{j\leq s}\alpha'_j(w,\vec{v})$ donde, para cada, $j\leq s$, $\alpha'_j(w,\vec{v})$ es una disyunción de pp-fórmulas o negaciones.

$\forall w\alpha'(w,\vec{v})$ es equivalente en $T_{\mathbb{R}}$, a $\bigwedge_{j\leq s}\forall w\alpha_j' w,\vec{v})$. Entonces podemos manejar $\alpha_j'(w,\vec{v})$ (con $j\leq s$ en lugar de $\alpha'(w,\vec{v})$.

2^{da} reducción: $\alpha_j'(w,\vec{v})$ es de la forma $\theta(w,\vec{v})\to\bigvee_{i<N}$ donde N es a entero positivo, $\theta(w,\vec{v})$ y $\theta_i(w,\vec{v})$, (con $i<N$) son *pp*-fórmulas. De hecho $\alpha'(w,\vec{v})$ es una única disyunción de *pp*-fórmulas y negaciones. Pero sabemos que cualquier conjunción de *pp*-fórmulas es (equivalente en $\mathscr{T}_{\mathbb{R}}$ a) una *pp*-fórmula, y por tanto cualquier disyunción de negaciones de *pp*-fórmulas es la negación de una única *pp*-fórmula. Esto implica claramente nuestra afirmación. Resumamos la situación.

Queremos encontrar β y $\gamma(\vec{v})$ tales que, para cada **R**- módulo $\mathfrak{M}$ y cada secuencia $\vec{a}$ en M,

$$\theta(\mathfrak{M},\vec{a})\subseteq\bigcup_{i<N}\theta_i(\mathfrak{M},\vec{a}). \tag{5.1}$$

si y sólo si $\mathfrak{M}\models\beta\wedge\gamma(\vec{a})$. Sabemos que, dados $\mathfrak{M}$ y $\vec{a}$, o bien $\theta(\mathfrak{M}m\vec{a})=\emptyset$ o bien $\theta(\mathfrak{M},\vec{a})$ es una clase lateral del subgrupo *pp*-difinible $\theta(\mathfrak{M},\vec{0})$. Lo mismo puede decirse de $\theta_i(\mathfrak{M},\vec{a})$, para cada $i<N$. Por cierto, nótese que $\exists w\theta(w,\vec{v}),\exists w\theta_i(w,\vec{v})$(con $i<N$) son *pp*-fórmulas. 5.1 es cierta cuando $\vec{a}$ satisface $\neg\exists w\theta_i(w,\vec{v})$, o (la negación de una *pp*-fórmula) en $\mathfrak{M}$, y ciertamente falsa cuando $\vec{a}$ satisface

$$\exists w\theta_i(w,\vec{v})\wedge\bigvee_{i<N}\neg\exists w\theta_i(w,\vec{v})$$

en $\mathfrak{M}$. Por tanto, no hay pérdida de generalidad para nuestros propósitos en suponer $\theta(\mathfrak{M},\vec{a})\neq\emptyset$ y $\theta_i(\mathfrak{M},\vec{a})\neq\emptyset$ para todo $i<N$. Sea S el conjunto de los índices $i<N$ que satisfacen

$$|\theta(\mathfrak{M},\vec{0}):\theta(\mathfrak{M},\vec{0})\cap\theta_i(\mathfrak{M},\vec{0}|\leq N!.$$

Observa que S depende de $\mathfrak{M}$ (y de $\vec{a}$, por supuesto). Sin embargo, sólo hay un número finito de formas posibles de elegir S, y cada una de ellas está descrita por un enunciado invariante adecuado. Supongamos, sin pérdida de generalidad, que S es sólo el conjunto de los enteros positivos $\leq m$ para algún $m \leq N$. Podemos aplicar el Lemma de B. H. Neumann's 5.0.1 y deducir que 5.1 es equivalente a

$$\theta(\mathfrak{M},\vec{a}) \subseteq \bigcup_{i<m} \theta_i(\mathfrak{M},\vec{a}). \tag{5.2}$$

Pongamos $K = \theta(\mathfrak{M},\vec{0}) \cap \bigcap_{i<m} \theta(\mathfrak{M},\vec{0})$. Como $\theta(\mathfrak{M},\vec{a})$ y $\theta_i(\mathfrak{M},\vec{a})$ para $i < m$ son son unión de clases laterales de K en M,5.2 puede escribirse equivalentemente

$$\theta(\mathfrak{M},\vec{a})/K \subseteq \bigcup_{i<m} \theta_i(\mathfrak{M},\vec{a})/K. \tag{5.3}$$

Como $\theta(\mathfrak{M},\vec{a})/K$ es finito, podemos utilizar algunos argumentos combinatoriales (esperemos) bien conocidos y replantear 5.3 de forma equivalente

$$\sum_X (-1)^{|x|} |(\theta(\mathfrak{M},\vec{a}) \cap \bigcap_{i\in X} \theta_i(\mathfrak{M},\vec{a}))/K| = 0 \tag{5.4}$$

donde X abarca los subconjuntos de $\{0,1,\ldots,m-1\}$. Para cada X, pongamos

$$k(X) = |\theta(\mathfrak{M},\vec{0}) \cap \bigcap_{i\in X} \theta_i(\mathfrak{M},\vec{0}) : K|;$$

Obsérvese que, cuando $\theta(\mathfrak{M},\vec{a}) \cap \bigcap_{i\in X} \theta_i(\mathfrak{M},\vec{a})/K \neq \emptyset$,

$$k(X) = |(\theta(\mathfrak{M},\vec{a}) \cap \bigcap_{i\in X} \theta_i(\mathfrak{M},\vec{a})/K|.$$

Además $k(X) \leq N!^N$. De ahí que hayamos demostrado que $\mathfrak{M}$ satisface $\alpha(\vec{a})$ si y sólo si $\sum(-1)^{|X|}k(X) = 0$, donde la suma concierne a todos los subconjuntos X de $\{0,1,\ldots,m-1\}$ tales que $\mathfrak{M} \models \exists w(\theta(w,\vec{a}) \wedge \bigwedge_{i\in X} \theta_i(w,\vec{a})$, y por tanto si y sólo si $\mathfrak{M}$ satisface una disyunción conveniente de conjunciones de enunciados invariantes y pp-fórmulas. Esto es lo que ocurre para un S dado. Como sólo hay un número finito de $S's$ posibles, se puede encontrar algún β adecuado y $\gamma(\vec{v})$, válido para todo **R**-módulo $\mathfrak{M}$.

■

Observemos que

1. *Obsérvese que el procedimiento dado en la demostración de Teorema 2.6.3 es efectivo y proporciona explícitamente para cada $\alpha(\vec{v})$ las fórmulas requeridas β y $\gamma(\vec{v})$. Además, β es en realidad una combinación booleana finita de enunciados invariantes relativos a pp-fórmulas $\varphi(v)$, $\psi(v)$ (con a lo sumo una variable libre).*
2. *En particular, cuando α es una sentencia de $\mathscr{L}_{\mathbb{R}}$, lo que produce el procedimiento anterior es simplemente una combinación booleana β de enunciados invariantes (relativos a pp-fórmulas $\varphi(v), \psi(v)$ con a lo sumo una variable libre) tal que $\alpha \iff \beta \in T_{\mathbb{R}}$.*
3. *Fijemos ahora un **R**-módulo $\mathfrak{M}$. Entonces, para cada fórmula $\alpha(\vec{v})$ de $\mathscr{L}_{\mathbb{R}}$, existe una combinación booleana $\gamma(\vec{v})$ de pp-fórmulas tal que $\mathfrak{M} \models \forall\vec{v}(\alpha(\vec{v}) \iff \gamma(\vec{v}))$ (de hecho, sabemos que $\alpha(\vec{v})$ es equivalente $\beta \wedge \gamma(\vec{v})$ para alguna combinación booleana $\gamma(\vec{v})$ de pp-fórmulas y alguna sentencia β; así, si $\mathfrak{M} \models \beta$, entonces $\alpha(\vec{v})$ es equivalente a $\gamma(\vec{v})$, mientras que, si $\mathfrak{M} \models \neg\beta$, entonces $\alpha(\mathfrak{M}^n)$ está vacía y en consecuencia $\alpha(\vec{v})$ es equivalente a $\delta(\vec{v}) \wedge \neg\delta(\vec{v})$, donde $\delta(\vec{v})$ es una pp-fórmula arbitraria).*

Con respecto a los conjuntos definibles en módulos, esto es lo que implica el teorema 5.1.

Corolario 5.1 Sea $\mathfrak{M}$ un **R**-módulo y n un número entero positivo. Entonces todo conjunto $X \subseteq M^n$ definible en $\mathfrak{M}$ es una combinación booleana finita de clases laterales de subgrupos pp-definibles.

Demostración. Existe una $\mathscr{L}$-fórmula $\alpha(\vec{v},\vec{w})$ y una secuencia $\vec{a}$ en M tales que $X = \alpha(\mathfrak{M}^n,\vec{a})$.Podemos suponer que $\alpha(\vec{v},\vec{w})$ es una combinación booleana de pp-fórmulas, y sabemos que, para toda pp-fórmula $\varphi(\vec{v},\vec{w})$, $\varphi(\mathfrak{M}^n,\vec{a})|$, cuando no está vacía, es una clase lateral del subgrupo pp-definible por $\varphi(\mathfrak{M}^n,\vec{0})$. ■

6. Conclusiones

6.1 Conclusiones

En conclusión, esta monografía ha proporcionado un análisis exhaustivo de la eliminación de cuantificadores y su impacto en diversos campos de la matemática y la lógica. A lo largo de nuestra exploración, hemos destacado la importancia de esta técnica en la simplificación y comprensión de fórmulas cuantificados, así como su influencia en la resolución de problemas matemáticos de índole compleja.

En primer lugar, hemos observado cómo la conexión entre la eliminación de cuantificadores y la teoría de orden lineal discreto ha permitido abordar problemas relacionados con estructuras ordenadas discretas de manera más clara y eficiente. La capacidad de traducir propiedades cuantificadas a un lenguaje más manejable en este contexto ha demostrado ser valiosa para la comprensión y manipulación de conjuntos ordenados de forma discreta.

Asimismo, al explorar la relación entre la eliminación de cuantificadores y la teoría de orden lineal denso, hemos extendido nuestra comprensión a estructuras más amplias y complejas. Esta conexión ha revelado la versatilidad de las técnicas de eliminación de cuantificadores al aplicarse a conjuntos ordenados de manera densa, ofreciendo herramientas adicionales para abordar problemas en contextos más generales.

La aplicación de la eliminación de cuantificadores en campos algebraicamente cerrados ha sido un tema destacado en nuestra investigación. Hemos observado cómo esta técnica ha permitido simplificar enunciados y demostraciones en este marco específico, proporcionando una perspectiva más profunda sobre la relación entre la eliminación de cuantificadores y la estructura algebraica de estos campos.

Además, cabe destacar que la eliminación de cuantificadores ha desempeñado un papel crucial al demostrar la decidibilidad, definibilidad y completitud de ciertas teorías matemáticas. La capacidad de traducir proposiciones cuantificadas a formas más manejables ha facilitado la exploración de la naturaleza y las propiedades fundamentales de estas teorías, ofreciendo así un enfoque más claro para evaluar su viabilidad y alcance.

En conjunto, esta monografía destaca la importancia de la eliminación de cuantificadores como una herramienta poderosa en el arsenal matemático y lógico. Al comprender sus diversas aplicaciones y conexiones con otras teorías, hemos ampliado nuestro conocimiento sobre cómo abordar problemas cuantificados de manera más efectiva. La eliminación de cuantificadores no solo simplifica la expresión de enunciados, sino que también ofrece nuevas perspectivas y oportunidades para la exploración de la verdad matemática en sus diversas manifestaciones, incluyendo la evaluación de la decidibilidad, definibilidad y completitud de teorías específicas.

Bibliografía

[1] **CHANG Chen & KEISLER H. Jerome.***Model Theory.* Third edition. New York, USA: Elsevier Science Pubilisher B.V. 1990. págs. 49-60.

[2] **CORI, Rene & LASCAR, Daniel**. *Mathematical Logic.* University of London: Editorial Oxford, 2006. págs. 112-135.

[3] **HODGES Wilfrid**. *Model Theory.* Universyty of London: Editorial Board 1993. págs. 66-75.

[4] **MANZANO María**. *Model Theory*. New York, USA: Editorial Oxford, 2006. págs. 203-218.

[5] **MARKER David**. *Model Theory An Introduction*. University of Illinois, Chicago, USA: Editorial Board, 2002. págs. 71-104

[6] **MIJAJLOVIC Zarko**. *An introduction to model theory.*, University of Novi Sad Institute of Mathematics, Yugoslavia: University of Novi Sad, 1987. págs. 3-24.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICADO DE CUMPLIMIENTO DE LA GUÍA PARA NORMALIZACIÓN DE TRABAJOS DE FIN DE GRADO

Fecha de entrega: 26/07/2024

INFORMACIÓN DEL AUTOR
Darío Gonzalo Matehu Tualongo
INFORMACIÓN INSTITUCIONAL
Facultad: Ciencias
Carrera: Matemática
Título a optar: Matemático
Dr. Leonidas Antonio Cerda Romero **Director del Trabajo de Integración Curricular** **Dr. Ramón Antonio Abancín Ospina** **Asesor del Trabajo de Integración Curricular**