

Excursiones por el Álgebra Lineal
y sus aplicaciones

ISBN: 978-956-306-073-7

Registro de Propiedad Intelectual: 200.527

Colección: Herramientas para la formación de profesores de matemáticas.

Diseño: Jessica Jure de la Cerda.

Diseño de Ilustraciones: Cristina Felmer Plominsky, Catalina Frávega Thomas.

Diagramación: Pedro Montealegre Barba, Francisco Santibáñez Palma.

Financiamiento: Proyecto Fondef D05I-10211.

Datos de contacto para la adquisición de los libros:

Para Chile:

1. En librerías para clientes directos.
2. Instituciones privadas directamente con:
Juan Carlos Sáez C.
Director Gerente
Comunicaciones Noreste Ltda.
J.C. Sáez Editor
jcsaezc@vtr.net
www.jcsaezeditor.blogspot.com
Oficina: (56 2) 3260104 - (56 2) 3253148
3. Instituciones públicas o fiscales: www.chilecompra.cl

Desde el extranjero:

1. Liberalia Ediciones: www.liberalia.cl
2. Librería Antártica: www.antartica.cl
3. Argentina: Ediciones Manantial: www.emanantial.com.ar
4. Colombia: Editorial Siglo del Hombre
Fono: (571) 3377700
5. España: Tarahumara, tarahumara@tarahumaralibros.com
Fono: (34 91) 3656221
6. México: Alejandría Distribución Bibliográfica, alejandria@alejandrialibros.com.mx
Fono: (52 5) 556161319 - (52 5) 6167509
7. Perú: Librería La Familia, Avenida República de Chile # 661
8. Uruguay: Dolmen Ediciones del Uruguay
Fono: 00-598-2-7124857

Excursiones por el Álgebra Lineal y sus aplicaciones — Omar Gil

Facultad de Ingeniería, Universidad de la República

omargil@fing.edu.uy

ESTA PRIMERA EDICIÓN DE 2.000 EJEMPLARES

Se terminó de imprimir en febrero de 2011 en **WORLD COLOR CHILE S.A.**

Derechos exclusivos reservados para todos los países. Prohibida su reproducción total o parcial, para uso privado o colectivo, en cualquier medio impreso o electrónico, de acuerdo a las leyes N°17.336 y 18.443 de 1985 (Propiedad intelectual). Impreso en Chile.

EXCURSIONES POR EL ÁLGEBRA LINEAL Y SUS APLICACIONES

Omar Gil

Universidad de la República (Uruguay)



UNIVERSIDAD
DE LA REPUBLICA
URUGUAY

Editores



Patricio Felmer, Universidad de Chile.
Doctor en Matemáticas, Universidad de Wisconsin-Madison,
Estados Unidos

Salomé Martínez, Universidad de Chile.
Doctora en Matemáticas, Universidad de Minnesota,
Estados Unidos

Comité Editorial Monografías



Rafael Benguria, Pontificia Universidad Católica de Chile.
Doctor en Física, Universidad de Princeton,
Estados Unidos

Servet Martínez, Universidad de Chile.
Doctor en Matemáticas, Universidad de Paris VI,
Francia

Fidel Oteíza, Universidad de Santiago de Chile.
Doctor en Currículum e Instrucción, Universidad del Estado de Pennsylvania,
Estados Unidos

Dirección del Proyecto Fondef D05I-10211
Herramientas para la Formación de Profesores de Matemática



Patricio Felmer, Director del Proyecto
Universidad de Chile.

Leonor Varas, Directora Adjunta del Proyecto
Universidad de Chile.

Salomé Martínez, Subdirectora de Monografías
Universidad de Chile.

Cristián Reyes, Subdirector de Estudio de Casos
Universidad de Chile.

Presentación de la Colección



La colección de monografías que presentamos es el resultado del generoso esfuerzo de los autores, quienes han dedicado su tiempo y conocimiento a la tarea de escribir un texto de matemática. Pero este esfuerzo y generosidad no se encuentra plenamente representado en esta labor, sino que también en la enorme capacidad de aprendizaje que debieron mostrar, para entender y comprender las motivaciones y necesidades de los lectores: Futuros profesores de matemática.

Los autores, encantados una y otra vez por la matemática, sus abstracciones y aplicaciones, enfrentaron la tarea de buscar la mejor manera de traspasar ese encanto a un futuro profesor de matemática. Éste también se encanta y vibra con la matemática, pero además se apasiona con la posibilidad de explicarla, enseñarla y entregarla a los jóvenes estudiantes secundarios. Si la tarea parecía fácil en un comienzo, esta segunda dimensión puso al autor, matemático de profesión, un tremendo desafío. Tuvo que salir de su oficina a escuchar a los estudiantes de pedagogía, a los profesores, a los formadores de profesores y a sus pares. Tuvo que recibir críticas, someterse a la opinión de otros y reescribir una y otra vez su texto. Capítulos enteros resultaban inadecuados, el orden de los contenidos y de los ejemplos era inapropiado, se hacía necesario escribir una nueva versión y otra más. Conversaron con otros autores, escucharon sus opiniones, sostuvieron reuniones con los editores. Escuchar a los estudiantes de pedagogía significó, en muchos casos, realizar eventos de acercamiento, desarrollar cursos en base a la monografía, o formar parte de cursos ya establecidos. Es así que estas monografías recogen la experiencia de los autores y del equipo del proyecto, y también de formadores de profesores y estudiantes de pedagogía. Ellas son el fruto de un esfuerzo consciente y deliberado de acercamiento, de apertura de caminos, de despliegue de puentes entre mundos, muchas veces, separados por falta de comunicación y cuya unión es vital para el progreso de nuestra educación.

La colección de monografías que presentamos comprende una porción importante de los temas que usualmente encontramos en los currículos de formación de profesores de matemática de enseñanza media, pero en ningún caso pretende ser exhaustiva. Del mismo modo, se incorporan temas que sugieren nuevas formas de abordar los contenidos, con énfasis en una matemática más pertinente para el futuro profesor, la que difiere en su enfoque de la matemática para un ingeniero o para un licenciado en matemática, por ejemplo. El formato de monografía, que aborda temas específicos

con extensión moderada, les da flexibilidad para que sean usadas de muy diversas maneras, ya sea como texto de un curso, material complementario, documento básico de un seminario, tema de memoria y también como lectura personal. Su utilidad ciertamente va más allá de las aulas universitarias, pues esta colección puede convertirse en la base de una biblioteca personal del futuro profesor o profesora, puede ser usada como material de consulta por profesores en ejercicio y como texto en cursos de especialización y post-títulos. Esta colección de monografías puede ser usada en concepciones curriculares muy distintas. Es, en suma, una herramienta nueva y valiosa, que a partir de ahora estará a disposición de estudiantes de pedagogía en matemática, formadores de profesores y profesores en ejercicio.

El momento en que esta colección de monografías fue concebida, hace cuatro años, no es casual. Nuestro interés por la creación de herramientas que contribuyan a la formación de profesores de matemática coincide con un acercamiento entre matemáticos y formadores de profesores que ha estado ocurriendo en Chile y en otros lugares del mundo. Nuestra motivación nace a partir de una creciente preocupación en todos los niveles de la sociedad, que ha ido abriendo paso a una demanda social y a un interés nacional por la calidad de la educación, expresada de muy diversas formas. Esta preocupación y nuestro interés encontró eco inmediato en un grupo de matemáticos, inicialmente de la Universidad de Chile, pero que muy rápidamente fue involucrando a matemáticos de la Pontificia Universidad Católica de Chile, de la Universidad de Concepción, de la Universidad Andrés Bello, de la Universidad Federico Santa María, de la Universidad Adolfo Ibáñez, de la Universidad de La Serena y también de la Universidad de la República de Uruguay y de la Universidad de Colorado de Estados Unidos.

La matemática ha adquirido un rol central en la sociedad actual, siendo un pilar fundamental que sustenta el desarrollo en sus diversas expresiones. Constituye el cimiento creciente de todas las disciplinas científicas, de sus aplicaciones en la tecnología y es clave en las habilidades básicas para la vida. Es así que la matemática actualmente se encuentra en el corazón del currículo escolar en el mundo y en particular en Chile. No es posible que un país que pretenda lograr un desarrollo que involucre a toda la sociedad, descuide el cultivo de la matemática o la formación de quienes tienen la misión de traspasar de generación en generación los conocimientos que la sociedad ha acumulado a lo largo de su historia.

Nuestro país vive cambios importantes en educación. Se ha llegado a la convicción que la formación de profesores es la base que nos permitirá generar los cambios cualitativos en calidad que nuestra sociedad ha impuesto. Conscientes de que la tarea formativa de los profesores de matemática y de las futuras generaciones de jóvenes es extremadamente compleja, debido a que confluyen un sinnúmero de factores y disciplinas, a través de esta colección de monografías, sus editores, autores y todos los que han participado del proyecto en cada una de sus etapas, contribuyen a esta tarea, poniendo a disposición una herramienta adicional que ahora debe tomar vida propia en los formadores, estudiantes, futuros profesores y jóvenes de nuestro país.

Patricio Felmer y Salomé Martínez
Editores

Agradecimientos



Agradecemos a todos quienes han hecho posible la realización de este proyecto Fondef: “Herramientas para la formación de Profesores de Matemáticas”. A Cristián Cox, quien apoyó con decisión la idea original y contribuyó de manera crucial para obtener la participación del Ministerio de Educación como institución asociada. Agradecemos a Carlos Eugenio Beca por su apoyo durante toda la realización del proyecto. A Rafael Correa, Edgar Kausel y Juan Carlos Sáez, miembros del Comité Directivo. Agradecemos a Rafael Benguria, Servet Martínez y Fidel Oteiza, miembros del Comité Editorial de la colección, quienes realizaron valiosos aportes a los textos. A Guillermo Marshall, Decano de la Facultad de Matemáticas de la Pontificia Universidad Católica de Chile y José Sánchez, entonces Decano de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Concepción, quienes contribuyeron de manera decisiva a lograr la integridad de la colección de 15 monografías. A Jaime San Martín, director del Centro de Modelamiento Matemático por su apoyo durante toda la realización del proyecto. Agradecemos a Víctor Campos, Ejecutivo de Proyectos de Fondef, por su colaboración y ayuda en las distintas etapas del proyecto.

Agradecemos también a Bárbara Ossandón de la Universidad de Santiago, a Jorge Ávila de la Universidad Católica Silva Henríquez, a Víctor Díaz de la Universidad de Magallanes, a Patricio Canelo de la Universidad de Playa Ancha en San Felipe y a Osvaldo Venegas y Silvia Vidal de la Universidad Católica de Temuco, quienes hicieron posible las visitas que realizamos a las carreras de pedagogía en matemática. Agradecemos a todos los evaluadores, alumnos, académicos y profesores -cuyos nombres no incluimos por ser más de una centena- quienes entregaron sugerencias, críticas y comentarios a los autores, que ayudaron a enriquecer cada uno de los textos.

Agradecemos a Marcela Lizana por su impecable aporte en todas las labores administrativas del proyecto, a Aldo Muzio por su colaboración en la etapa de evaluación, y también a Anyel Alfaro por sus contribuciones en la etapa final del proyecto y en la difusión de los logros alcanzados.

Dirección del Proyecto

Índice General



Prefacio	17
Capítulo 1: Presentación y revisión de conceptos básicos	23
1.1 Los números de Fibonacci	23
1.2 Cambios de coordenadas en \mathbb{R}^n y matrices semejantes	28
1.3 Normas, módulos y distancias	35
Capítulo 2: Vectores y valores propios	43
2.1 Vectores y valores propios	43
2.2 Cálculo de valores y vectores propios	50
2.3 Diagonalización	56
2.4 Radio espectral y potencias de una matriz	65
Capítulo 3. Producto escalar	77
3.1 Bases ortonormales de \mathbb{R}^n	79
3.2 Bases ortonormales y proyecciones ortogonales	86
3.3 El método de Gramm-Schmidt y la descomposición QR	95
3.4 Mínimos cuadrados	102
Capítulo 4. Teorema espectral y descomposición en valores singulares	109
4.1 Teorema espectral para matrices simétricas	109
4.2 Descomposición en valores singulares	122
4.3 Extensiones y aplicaciones de la SVD	131
Capítulo 5. Cadenas de Markov	143
5.1 Cadenas de Markov	143
5.2 Métrica $\ \cdot\ _1$ y matrices de transición	148
Capítulo 6. Códigos correctores de errores	155
6.1 Detección y corrección de errores	155
6.2 La distancia de Hamming en \mathbb{Z}_2^n	163
6.3 Códigos lineales	165

Apéndice A. Preliminares	173
A.1 Matrices y álgebra de matrices	173
A.2 Vectores y matrices columnas	174
A.3 Independencia lineal y bases	174
A.4 Coordenadas	175
A.5 Interpretaciones geométricas	175
A.6 Producto escalar en \mathbb{C}^n	176
Apéndice B. Cuerpos finitos	177
Apéndice C. Completitud y puntos fijos	179
C.1 Contracciones y puntos fijos	179
Bibliografía	183
Índice de figuras	185
Índice de notaciones	187
Índice de autores	189
Índice Analítico	191

Prefacio



Esta monografía pretende explorar algunos aspectos del Álgebra Lineal en el contexto de sus conexiones con otras ramas de la Matemática y sus aplicaciones.

El primer capítulo es introductorio. Comienza retomando un problema clásico del siglo XIII, cuyo alcance e interés ha trascendido largamente su propósito original de motivar el estudio de la aritmética. Luego, en la segunda sección, se revisan algunos de los requisitos previos necesarios para seguir adelante, con especial atención al concepto de cambio de base o cambio de coordenadas. Un cambio de coordenadas puede pensarse como un intento de buscar un punto de vista adecuado para atacar un problema, y buena parte del material del texto esta motivado por esta idea, que es de amplio alcance, incluso fuera de la matemática. En esta categoría están incluidas las búsquedas de vectores propios en el capítulo 2, la construcción de bases ortonormales en el 3 y las fundamentales descomposiciones de matrices que proporcionan el teorema espectral y la descomposición en valores singulares en el capítulo 4. La tercera sección del capítulo 1 explora diversas estructuras geométricas.

Uno de los propósitos de esta monografía es mostrar en diversos contextos la interacción entre la estructura lineal y diversas geometrías. Los capítulos 3 y 4 se concentran en generalizaciones de los conceptos usuales de distancia y perpendicularidad a espacios de cualquier dimensión. Aunque este mundo ya es riquísimo, hay más posibilidades que las de ampliar el alcance de la vieja geometría de Euclides: en el capítulo 5 empleamos una geometría diferente en el plano y el espacio, la “geometría del taxista”, para probar resultados sobre modelos con un rango de aplicación tan dispar que incluye desde la epidemiología al diseño de buscadores sobre la web. En un nuevo giro, el capítulo 6 se construye alrededor de una geometría discreta, útil en el marco de la moderna teoría de la información.

Tal como su título permite conjeturar, la monografía no tiene un hilo conductor nítido que la recorra y estructure. Pero toda ella está animada por el espíritu de establecer puentes entre la teoría y las aplicaciones, rescatando interpretaciones y significados, ayudando al profesor a desarrollar el reflejo de identificar la matemática allí donde esté presente, para llevarla al aula y compartirla con sus alumnos. En nuestras sociedades tan matematizadas, buena parte de la visión del mundo que hemos construido colectivamente, y de las cosas que nos rodean, son posibles porque se ha

desarrollado la matemática necesaria para sostenerlas. Por lo tanto, cuando la educación matemática colabora a iluminar estas relaciones se vuelve una herramienta para ampliar los espacios de libertad y creatividad de cada persona. Más allá del éxito o fracaso en contribuir a este propósito, es desde esta convicción que hemos intentado escribir estas páginas.

En este mismo sentido, el lector encontrará secciones y capítulos que no se ordenan según la secuencia de axiomas-definiciones-enunciados-demostraciones que, siguiendo la estructuración lógica de la Matemática, es bastante frecuente en la literatura escolar. Porque cuando la Matemática se desarrolla lo habitual es que primero aparezcan problemas e ideas no completamente dibujadas, luego se descubran conceptos y teoremas, y recién al final quede claro cuáles son los postulados necesarios y las buenas definiciones. Es así que, históricamente, las definiciones y axiomas suelen ser de lo último en aparecer. En varios pasajes hemos intentado capturar aspectos de esta atmósfera de tanteos e incertidumbres, recorriendo el camino desde ideas fundamentales hasta conceptos que pueden ser formalizados. Opción hecha a conciencia de que puede generar dificultades a más de un lector acostumbrado a otro estilo de exposición, pero que aún así encontramos válida.

Por aquí y allá asoman conexiones con problemas de estadística, combinatoria, dinámica, análisis de señales, análisis numérico, economía, etcétera. Algunas que no cupieron en este texto se hicieron un lugar en [7]. La idea es siempre abrir ventanas hacia diversos mundos, en los que el futuro profesor pueda buscar significados y actividades para compartir con sus futuros estudiantes. Tal vez las opciones sobre temas incluidos no sean las mejores posibles. Tal vez ni siquiera existan las mejores opciones. Pero la monografía trata de acercar tópicos potencialmente estimulantes y valiosos para un Profesor de Matemática. Quizás ninguno de ellos sea indispensable para su formación, pero probablemente todos contribuyan a poner en contextos más amplios los temas con los que deberá trabajar en el aula.

Requisitos previos y notación

Los requisitos previos son habitualmente cubiertos en un curso estándar de Álgebra Lineal, con la posible excepción de algunas nociones sobre cuerpos finitos. De todos modos los describimos en el apéndice A, y presentamos en [6] una versión algo más desarrollada. En el apéndice B hemos incluido los pocos conocimientos necesarios sobre cuerpos finitos.

Las notaciones no se apartan de lo habitual en el área, salvo un par de excepciones que discutimos en el apéndice A. Las recogemos en el índice de la página 184.

Posibles recorridos por la monografía

Esta monografía puede usarse como base para un curso de tópicos de Álgebra Lineal y sus aplicaciones, o partes de ellas pueden emplearse como complemento de un curso introductorio acerca del mismo tema.

Comenzamos por discutir la dependencia lógica entre los capítulos y secciones.

1. Dentro de cada capítulo cada sección se apoya en las anteriores, con las siguientes excepciones:
 - desde un punto de vista lógico la sección 1.1 no es un requisito previo para nada posterior, pero puede servir como motivación para hablar de vectores propios, del teorema espectral o incluso de las nociones de producto escalar y perpendicularidad en \mathbb{R}^2 . Tampoco la sección 1.2 es necesaria para la lectura de la 1.3;
 - a lo largo de la sección 3.2 empleamos una y otra vez la proposición 3.8, página 86, que asegura la existencia de bases ortonormales para cualquier subespacio de \mathbb{R}^n . Su demostración recién aparece en la sección 3.3. Si bien desde el punto de vista de la estructuración lógica del texto ambas secciones pueden invertirse, nos pareció más adecuado mostrar los resultados de existencia de bases ortonormales recién después de dejar claro para qué las necesitamos.
2. Cada capítulo es esencialmente independiente del resto, y perfectamente podrían leerse en forma autónoma, con las siguientes excepciones y consideraciones:
 - algunos ejemplos aparecen una y otra vez a lo largo del libro y el lector que siga el desarrollo completo se beneficiará de hacerlo. Pero en cada caso se retoma lo necesario para hacer la lectura independiente;
 - difícilmente alguien quiera leer el capítulo 1 y nada más, pero si el lector desea hacerlo: ¡adelante!;
 - la sección 2.3 del capítulo 2 requiere manejar bien las nociones de cambio de base de la sección 1.2;
 - el capítulo 4 es excepcional, ya que depende de buena parte de los capítulos 2 y 3. Hace falta haber cubierto el inicio de la sección 2.3, en la que se expone la noción de diagonalización, y la sección 3.2, para poder avanzar en él;
 - para la sección 6.2 hacen falta algunos resultados de la 1.3, y para comprender la 6.3 ayuda haber visto antes la noción de vector y valor propio, que se expone en la sección 2.1;
 - el capítulo 7 es autocontenido, salvo la referencia a la distancia de Hamming, que se introduce en la sección 1.3.

A continuación sugerimos algunos recorridos:

1. Comenzar con los cambios de coordenadas (sección 1.2); discutir las nociones de vector propio y diagonalización (secciones 2.1, 2.2 y 2.3); ver la posibilidad de descomponer \mathbb{R}^n como suma directa de espacios ortogonales (secciones 3.1, 3.2 y 3.3) y cubrir luego el capítulo 4.

El teorema espectral para matrices simétricas y la descomposición en valores singulares (SVD) son resultados fundamentales acerca de la estructura de las matrices, con significados y consecuencias que se relacionan con contenidos de la matemática escolar. Además de ofrecer una muy limpia caracterización geométrica de la acción de cualquier matriz sobre los vectores de \mathbb{R}^n , la SVD tiene un importante lugar en muchas aplicaciones, por lo que le hemos dado un lugar importante, incluso a costa de recortar tópicos mas tradicionales como la forma canónica de Jordan. Recomendamos mostrar su existencia e interés a los alumnos de pedagogía en Matemática.

2. Trabajar sobre el capítulo 3 y culminar con el análisis de problemas de mínimos cuadrados, que movilizan ideas aplicables en una gran variedad de contextos (incluyendo algunos suficientemente simples como para ser discutidos en aulas de enseñanza media).
3. Cubrir los materiales necesarios para comprender el comportamiento asintótico de las cadenas de Markov, que se discuten en el capítulo 5. Como preparación para este capítulo, basta recorrer previamente la sección 2.1 dedicada a valores y vectores propios, y partes de la sección 1.3.
4. Estudiar los resultados para matrices con coeficientes positivos o no negativos, contenidos en las secciones 2.1, 2.2 y 2.4.
5. Visitar el capítulo 6 sobre códigos correctores de errores. Este capítulo es casi autocontenido y trata de un tema muy interesante que se conecta con materiales que pueden ser muy bien explotados para cursos de enseñanza media (e incluso de básica). Es especialmente interesante mostrar a los estudiantes cómo las herramientas del Álgebra Lineal funcionan bien en este contexto discreto¹, tan diferente del habitual² de \mathbb{Q} , \mathbb{R} o \mathbb{C} .

¹Es de presumir que las conexiones con problemas de combinatoria sean de interés para un futuro profesor de Matemática. Escapan al Álgebra Lineal y por razones de espacio no aparece en este texto, pero recomendamos explorarlas.

²La experiencia del autor con estos temas es que los estudiantes, para quienes todo es nuevo o prácticamente nuevo, los reciben muy bien, y que para ellos trabajar con el álgebra de \mathbb{Z}_2 no representa ninguna dificultad. Más bien al contrario, al poco tiempo de conocerla prefieren calcular con ejemplos sobre \mathbb{Z}_2 a hacerlo sobre \mathbb{R} , en los que todo suele ser más trabajoso. Sin embargo, los docentes, presumiblemente atrapado en sus hábitos, tienden a manifestar que “el tema es difícil”, o que “los estudiantes no entenderán”.

Agradecimientos

Pablo Fernández y Ernesto Mordecki aportaron lecturas críticas y variadas sugerencias durante la preparación de este trabajo. Gracias a Marcelo Cerminara distintos recursos necesarios para la escritura estuvieron disponibles en el momento en que fueron necesarios. Pablo Cancela colaboró en la preparación de algunas de las figuras. Parte de este material fue ensayado y criticado en un curso para formadores de profesores de Matemática dictado en el marco de la Administración Nacional de Educación Pública (ANEP) de Uruguay, y se benefició de la interacción con Andrés Abreu, Mario Bartolic, Teresita Carrión, Alejandro Duarte, Matías Guichón, Román Herrero, María de los Ángeles Inella, Fabián Luaces, Ariel Mazza, Emma Odriozola, Eduardo Peraza, Alicia Pereira, Mariana Pizarossa, y Ricardo Vilaró. Jorge González Lorca, Mariana Saavedra, Alejandro Sepúlveda, Víctor Trujillo, Alicia Venegas y Osvaldo Venegas leyeron versiones preliminares y devolvieron muchísimo material interesante. Aunque es casi seguro que sus aportes no hayan sido aprovechados en todo su potencial, gracias a ellos, y a la cuidada revisión de Ramón Reyes, este texto es mejor que los intentos que le precedieron.

La monografía se ha ido formando en el calor de la camaradería y el excelente ambiente de trabajo en el proyecto FONDEF “Herramientas para la Formación de Profesores de Matemática”, por lo que agradecemos a los demás autores y a los coordinadores del proyecto por la magnífica experiencia de trabajar en él.

Por último, sólo nos queda desear al lector un feliz encuentro con lo que elija recorrer de lo que aquí se le ofrece.

Omar Gil
Montevideo, septiembre de 2010

Capítulo 1: Presentación y revisión de conceptos básicos



Dedicamos la sección 1.1 a presentar un problema clásico que nos servirá para motivar una parte importante del contenido de esta monografía. En la sección 1.2 revisamos algunos conceptos relativos a cambios de coordenadas, que luego usaremos reiteradamente. Por último, la sección 1.3 recoge varias nociones geométricas y de convergencia que aparecerán luego en diversas partes del texto. La lectura de las distintas partes de la sección 1.3 puede posponerse hasta que surja la necesidad de emplear las nociones que allí se exponen.

1.1 Los números de Fibonacci

Comenzaremos por plantear un problema clásico: en un lugar cercado un hombre tiene una pareja de conejos, ¿cuántos conejos tendrá al cabo de un año, si una pareja de conejos puede engendrar cada mes una nueva pareja, que a su vez es capaz de engendrar una pareja cada mes a partir de su segundo mes de vida?

Nota Histórica 1.1. *Este ejercicio está tomado del libro de texto Liber Abaci, de Fibonacci, publicado en 1202. Tenía como propósito motivar el aprendizaje de la aritmética básica de los números naturales empleando la notación arábica, corriente hoy en día, pero que en esos años recién se estaba difundiendo por Europa gracias al impulso de pioneros como el propio Fibonacci. Su propuesta, aparentemente ingenua, da lugar a la sucesión de números de Fibonacci, rica en propiedades y en conexiones con diversas ramas de la matemática. Una revista, The Fibonacci Quarterly, se especializa en problemas matemáticos relacionados con los números de Fibonacci.*

Las reglas según las que se reproducen los conejos del problema implican que el número f_{n+1} de parejas de conejos que habrá en el mes $n+1$, el siguiente al mes n , será

$$(1.1) \quad f_{n+1} = f_n + f_{n-1} \quad n \geq 1.$$

Porque f_n es el número de parejas ya nacidas al mes n , y f_{n-1} el número de parejas recién nacidas, descendientes de las parejas que existían en el mes $n-1$ y que en el mes n son fértiles. El total f_{n+1} para el mes $n+1$ es la suma de ambas cantidades.

El problema original de Fibonacci pretendía motivar el estudio de la aritmética básica, no la cunicultura, y puede resolverse estudiando los primeros términos de la

sucesión f_n . Nosotros tampoco estamos interesados en los conejos, pero estudiaremos la sucesión infinita de números f_n que se generan a partir de la recurrencia (1.1) y la inicialización

$$(1.2) \quad f_0 = 0, \quad f_1 = 1.$$

Los términos de esta sucesión f_n son conocidos como los *números de Fibonacci*:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, \dots$$

En la portada aparecen $f_8 = 21$ conejos. En las próximas páginas veremos como algunos conceptos importantes del Álgebra Lineal permiten contestar las siguientes preguntas:

- ¿cómo crecen los números f_n cuando n tiende a infinito?
- ¿hay una fórmula explícita para los números f_n , que para cada valor de n permita calcularlos directamente?

La recurrencia (1.1) requiere ir dos pasos atrás para calcular f_{n+1} . Usaremos un artificio corriente en el estudio de problemas de evolución para reescribir (1.1) como una recurrencia en la que el paso $n+1$ sólo depende del paso n : se trata de aumentar la dimensión del espacio y estudiar las parejas

$$(1.3) \quad F_n = (f_n, f_{n+1}),$$

que ya no están formadas por conejos, sino por un número de Fibonacci f_n y su siguiente f_{n+1} (en la monografía [5] el lector puede encontrar otros ejemplos en que se aplica este procedimiento). Entonces (1.1) implica

$$\begin{bmatrix} f_{n+1} \\ f_{n+2} \end{bmatrix} = \begin{bmatrix} f_{n+1} \\ f_n + f_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix},$$

por lo que la definición (1.3) de las parejas F_n permite escribir

$$(1.4) \quad F_{n+1} = MF_n, \quad n \geq 1,$$

con

$$(1.5) \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Combinando (1.2) con (1.3) encontramos que la inicialización de la sucesión de parejas F_n debe ser $F_0 = (0, 1)$.

Al representar en el plano las parejas (1.3) generadas por (1.4) encontramos el gráfico de la figura 1.1. Vemos allí que las parejas F_n tienden a aproximarse a una línea que pasa por el origen con una cierta pendiente λ . Esto sugiere que para valores grandes de n debe satisfacerse

$$(1.6) \quad f_{n+1} \simeq \lambda f_n.$$

Otra evidencia de esto proviene de estudiar los cocientes f_{n+1}/f_n :

n	1	2	3	4	5	6	7	8	9	10
f_{n+1}/f_n	1	2	1,5	1,66..	1,6	1,625	1,615..	1,619..	1,617..	1,618..

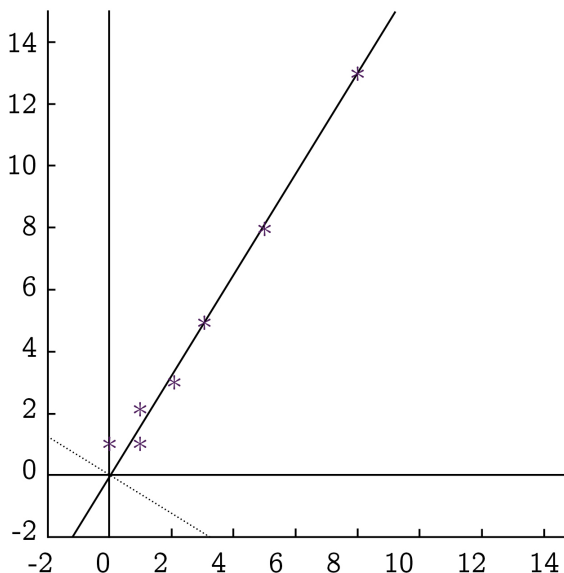


FIGURA 1.1. Parejas de números de Fibonacci consecutivos

Naturalmente, si la fórmula (1.6) es correcta también

$$(1.7) \quad f_{n+2} \simeq \lambda f_{n+1},$$

Combinando (1.6), (1.7) y (1.4) concluimos que es de esperar una relación del tipo

$$(1.8) \quad MF_n = F_{n+1} \simeq \lambda F_n,$$

para n muy grande. La constante λ aún debe ser determinada. Para encontrar λ y entender la figura 1.1 buscaremos parejas X de \mathbb{R}^2 que satisfagan

$$(1.9) \quad MX = \lambda X,$$

que es una versión exacta de (1.8). Si las hay, es de presumir que que las F_n se estén aproximando a ellas.

Observación 1.1. Las parejas, o vectores, de \mathbb{R}^2 que satisfacen una relación como (1.9) son los *vectores propios* de la matriz M . El número λ es un *valor propio* de M . Estos conceptos serán estudiados con cierto detalle en el capítulo 2.

Observación 1.2. Para una aproximación a los números de Fibonacci basada en el estudio de los cocientes f_{n+1}/f_n ver el ejercicio C.7, en la página 180 del apéndice C.1.1.

Para $X = (x_1, x_2)$ la igualdad (1.9) es equivalente al sistema

$$\begin{cases} x_2 = \lambda x_1, \\ x_1 + x_2 = \lambda x_2. \end{cases}$$

Sustituyendo x_2 por λx_1 en la segunda ecuación reducimos el problema a

$$\begin{cases} x_2 = \lambda x_1, \\ (\lambda^2 - \lambda - 1)x_1 = 0. \end{cases}$$

Sólo hay soluciones distintas de $X = (0, 0)$, para (1.9) si

$$(1.10) \quad \lambda^2 - \lambda - 1 = 0.$$

La ecuación (1.10) tiene soluciones

$$\lambda = (1 \pm \sqrt{5})/2.$$

Con el signo de más encontramos a la célebre *razón áurea*

$$\lambda_+ = \frac{1 + \sqrt{5}}{2} \simeq 1,618,$$

y soluciones de (1.9) de la forma

$$(1.11) \quad x_1 \left(1, (1 + \sqrt{5})/2 \right), \quad x_1 \in \mathbb{R}.$$

Las soluciones que corresponden a $\lambda_- = (1 - \sqrt{5})/2 \simeq -0,618$, son

$$(1.12) \quad x_1 \left(1, (1 - \sqrt{5})/2 \right), \quad x_1 \in \mathbb{R}.$$

Al representar las soluciones (1.11) y (1.12) en el plano (x_1, x_2) encontramos las dos líneas inclinadas, perpendiculares entre sí, que aparecen en la figura 1.1. La respuesta parece estar ahora ante nuestros ojos: los F_n van aproximándose a la línea que corresponde al valor λ_+ , la razón áurea. Pero, ¿por qué?

Para entenderlo recurriremos a la estructura vectorial de \mathbb{R}^2 . Si llamamos

$$X_+ = \left(1, (1 + \sqrt{5})/2 \right), \quad X_- = \left(1, (1 - \sqrt{5})/2 \right)$$

la pareja

$$\mathcal{A} = (X_+, X_-)$$

es una base de \mathbb{R}^2 .

Ejercicio 1.1. Comprobar que \mathcal{A} es una base de \mathbb{R}^2 y hallar la expresión de cualquier vector (x_1, x_2) como combinación lineal de \mathcal{A} .

Además, los dos vectores de \mathcal{A} tienen la importante propiedad de que sobre ellos M actúa simplemente como la multiplicación por un escalar:

$$(1.13) \quad MX_+ = \lambda_+ X_+, \quad MX_- = \lambda_- X_-.$$

Es decir, usando los términos de la observación 1.1, X_+ y X_- son vectores propios de M , con valores propios λ_+ y λ_- . Por lo tanto, es posible descomponer cualquier

vector de \mathbb{R}^2 como la suma de dos vectores sobre los que la acción de M está dada por las sencillas fórmulas en (1.13).

Para el vector $F_0 = (0, 1)$ que inicializa la recurrencia vectorial (1.4) que origina los números f_n tenemos la expresión

$$(1.14) \quad F_0 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix} - \frac{1}{\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1-\sqrt{5}}{2} \end{bmatrix}.$$

como una combinación lineal de un vector X_+ y un vector X_- . Por lo tanto

$$F_1 = MF_0 = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right) \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right) \begin{bmatrix} 1 \\ \frac{1-\sqrt{5}}{2} \end{bmatrix}.$$

Ejercicio 1.2. Comprobar que esta fórmula para F_1 es correcta y permite determinar f_2 y f_1 .

Cada aplicación de M hace aparecer factores λ_+ y λ_- en los vectores de la descomposición (1.14). Razonando inductivamente concluimos

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \begin{bmatrix} 1 \\ \frac{1-\sqrt{5}}{2} \end{bmatrix}.$$

Como $|\lambda_+| > 1$ y $|\lambda_-| < 1$, al multiplicar por M en cada paso, según la fórmula iterativa (1.4), la componente según X_+ de F_n va creciendo exponencialmente, pero la componente según X_- va decreciendo exponencialmente y en el límite termina por desaparecer. Para valores grandes de n tendremos

$$(1.15) \quad F_n \simeq \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n \begin{bmatrix} 1 \\ \frac{1+\sqrt{5}}{2} \end{bmatrix}.$$

En cuanto a los números de Fibonacci y su comportamiento asintótico, encontramos

$$(1.16) \quad f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n \sim \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n.$$

Ejercicio 1.3. Supongamos que los números de Fibonacci se inicializan con

1. $f_1 = 1 + \sqrt{5}$, $f_0 = 2$;
2. $f_1 = 1 - \sqrt{5}$, $f_0 = 2$;
3. $f_1 = 1$, $f_0 = -1$.

Esquematizar en cada caso cuál sería la ubicación en el plano de las parejas F_n .

Ejercicio 1.4. Para $n \geq 0$, hallar una fórmula explícita para la n -ésima potencia M^n de la matriz M en (1.4).

Ejercicio 1.5. Buscar información sobre los números de Fibonacci, la razón áurea, y sus conexiones con otros temas de la Matemática y de otras áreas de la actividad humana. Considerar los aspectos históricos.

1.2 Cambios de coordenadas en \mathbb{R}^n y matrices semejantes

El objetivo de esta sección es revisar rápidamente la noción de *cambio de base*, o *cambio de coordenadas*, y discutir con un poco más de profundidad como los cambios de coordenadas¹ afectan a la representación de las transformaciones que las matrices definen en los espacios \mathbb{R}^n .

Recordemos que una base \mathcal{A} en un subespacio \mathbb{S} de \mathbb{R}^n permite representar a cada $X \in \mathbb{R}^n$ por sus coordenadas $X_{\mathcal{A}}$, y que, una vez fijada una base \mathcal{A} , hay una correspondencia uno a uno entre los vectores X y sus coordenadas. Un caso especialmente importante es cuando $\mathbb{S} = \mathbb{R}^n$.

Ejemplo 1.1. La pareja de vectores

$$(1.17) \quad X_+ = \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix}, \quad X_- = \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix}$$

forma una base $\mathcal{A} = (X_+, X_-)$ de \mathbb{R}^2 . Cualquier vector $X = (x_1, x_2)$ admite una única expresión como combinación lineal de \mathcal{A} , en la forma

$$(x_1, x_2) = \left(\frac{1}{\sqrt{5}}x_1 + \frac{\sqrt{5}-1}{2\sqrt{5}}x_2 \right) X_+ + \left(-\frac{1}{\sqrt{5}}x_1 + \frac{\sqrt{5}+1}{2\sqrt{5}}x_2 \right) X_-.$$

El vector

$$(1.18) \quad X_{\mathcal{A}} = \begin{bmatrix} \frac{1}{\sqrt{5}}x_1 + \frac{\sqrt{5}-1}{2\sqrt{5}}x_2 \\ -\frac{1}{\sqrt{5}}x_1 + \frac{\sqrt{5}+1}{2\sqrt{5}}x_2 \end{bmatrix},$$

es el vector de coordenadas de X en la base \mathcal{A} .

Ejemplo 1.2. El vector de coordenadas de $X \in \mathbb{R}^n$ respecto a la base canónica \mathcal{C} de \mathbb{R}^n es igual a X . Es decir, $X_{\mathcal{C}} = X$.

Una matriz cuadrada M de orden n define una transformación (lineal)

$$(1.19) \quad X \mapsto MX, \quad X \in \mathbb{R}^n.$$

de \mathbb{R}^n en sí mismo, que a cada $X \in \mathbb{R}^n$ le hace corresponder el producto MX .

Ejemplo 1.3. En \mathbb{R}^2 , la matriz

$$(1.20) \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

que define la recursión de los números de Fibonacci, transforma $X = (x_1, x_2)$ en $MX = (x_2, x_1 + x_2)$.

¹El lector que conozca la teoría de transformaciones lineales entre espacios vectoriales de dimensión finita y el manejo de los cambios de base reconocerá en esta sección las matrices asociadas con transformaciones lineales, las matrices de cambio de base y los resultados que describen cómo cambian las matrices asociadas con transformaciones al cambiar de base. Pero conocer esta teoría no es necesario para leer la sección, ni el resto de la monografía.

Si \mathcal{A} es una base de \mathbb{R}^n la transformación $X \mapsto MX$ puede describirse en las coordenadas respecto a esa base. En este nuevo sistema de coordenadas, X está representado por $X_{\mathcal{A}}$ y MX por $(MX)_{\mathcal{A}}$. La idea entonces es estudiar la correspondencia

$$X_{\mathcal{A}} \mapsto (MX)_{\mathcal{A}}.$$

Notablemente, una buena elección de \mathcal{A} en muchos casos hace que esta segunda transformación sea especialmente simple, y nos permita entender la transformación original $X \mapsto MX$. Las técnicas del cálculo matricial permiten pasar de un sistema de coordenadas a otro. Para emplearlas llamemos A a la matriz cuadrada de orden n cuyas columnas son los vectores de la base \mathcal{A} . Entonces, para cada $X \in \mathbb{R}^n$ se tiene que

$$(1.21) \quad X = AX_{\mathcal{A}}, \quad X_{\mathcal{A}} = A^{-1}X.$$

La primera igualdad en (1.21) implica

$$(1.22) \quad MX = MAX_{\mathcal{A}}.$$

La segunda, aplicada a MX y combinada con (1.22), nos dice que

$$(1.23) \quad (MX)_{\mathcal{A}} = A^{-1}MX = A^{-1}MAX_{\mathcal{A}}.$$

Por lo tanto, para pasar de $X_{\mathcal{A}}$ a $(MX)_{\mathcal{A}}$ todo lo que hay que hacer es multiplicar por la matriz

$$(1.24) \quad N = A^{-1}MA.$$

Concluimos que N es la matriz que en la base \mathcal{A} representa la acción de M .

Ejemplo 1.4. La matriz que representa la acción de M en la base canónica \mathcal{C} es la propia matriz M .

Ejemplo 1.5. La matriz A asociada con la base \mathcal{A} del ejemplo 1.1 es

$$(1.25) \quad A = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ 1 & 1 \end{bmatrix}.$$

Ejercicio 1.6. Verificar que al formar el producto $AX_{\mathcal{A}}$ de A con el vector $X_{\mathcal{A}}$ en (1.18) se recupera el vector X , tal como expresa la primera ecuación en (1.21)

La inversa de A es

$$(1.26) \quad A^{-1} = \begin{bmatrix} \frac{1}{\sqrt{5}} & \frac{\sqrt{5}-1}{2\sqrt{5}} \\ -\frac{1}{\sqrt{5}} & \frac{\sqrt{5}+1}{2\sqrt{5}} \end{bmatrix}.$$

Ejercicio 1.7. Comprobar que A^{-1} es efectivamente la inversa de A , y que

$$X_{\mathcal{A}} = A^{-1}X.$$

Comparar con la fórmula (1.18).

Para las matrices M en (1.20) y A en (1.25) el producto $A^{-1}MA$ es

$$(1.27) \quad D = \begin{bmatrix} \frac{1+\sqrt{5}}{2} & \\ & \frac{1-\sqrt{5}}{2} \end{bmatrix},$$

una matriz diagonal, que debe representar en las nuevas coordenadas el efecto de M

Volveremos a encontrar (1.27) por otro camino. Un vector X de \mathbb{R}^2 tiene coordenadas

$$X_{\mathcal{A}} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

si y sólo si

$$X = y_1 X_+ + y_2 X_-.$$

Por lo tanto

$$MX = M(y_1 X_+ + y_2 X_-) = y_1 MX_+ + y_2 MX_-.$$

Recordando ahora que

$$M_+ X_+ = \frac{1+\sqrt{5}}{2} X_+, \quad MX_- = \frac{1-\sqrt{5}}{2} y_2 X_-$$

(ver la fórmula (1.13) en la página 26, o simplemente hacer el cálculo), tenemos

$$MX = \frac{1+\sqrt{5}}{2} y_1 X_+ + \frac{1-\sqrt{5}}{2} y_2 MX_-.$$

Esta expresión es equivalente a

$$(MX)_{\mathcal{A}} = \begin{bmatrix} \frac{1+\sqrt{5}}{2} y_1 \\ \frac{1-\sqrt{5}}{2} y_2 \end{bmatrix} = \begin{bmatrix} \frac{1+\sqrt{5}+1}{2} & \\ & \frac{1-\sqrt{5}+1}{2} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

Confirmamos así que la matriz D en (1.27) es la que representa como se transforman las coordenadas respecto a la base \mathcal{A} cuando M transforma a los vectores de \mathbb{R}^2 . Fue este cambio a las coordenadas en la base \mathcal{A} , el que nos permitió entender el comportamiento de la sucesión de números de Fibonacci en la sección 1.1.

Si dos matrices M y N satisfacen la igualdad $N = A^{-1}MA$ como en (1.24) también satisfacen

$$(1.28) \quad M = ANA^{-1},$$

que puede obtenerse multiplicando (1.24) a la izquierda por A y a la derecha por A^{-1} . Cuando dos matrices N y M satisfacen las fórmulas (1.24)-(1.28) para una matriz invertible A , representan la misma transformación vista en distintos sistemas de coordenadas. Se dice entonces que las matrices son *semejantes*. Todas las matrices semejantes a una matriz M dada son todas las posibles representaciones de M respecto a todos las posibles bases de \mathbb{R}^n .

Ejercicio 1.8. Mostrar que la relación de semejanza es una relación de equivalencia en el conjunto de las matrices cuadradas $n \times n$ con coeficientes en \mathbb{R} .

Ejemplo 1.6. Para la matriz M que genera la sucesión de números de Fibonacci la fórmula (1.28) toma la forma

$$(1.29) \quad M = ADA^{-1},$$

donde D es la matriz diagonal (1.27).

Cualquiera de las fórmulas (1.24)-(1.28) es también equivalente a

$$(1.30) \quad MA = AN,$$

que tiene una interpretación muy sugerente. La i -ésima columna de MA es el producto de M por A_i , la i -ésima columna de A , que es también el i -ésimo vector de la base \mathcal{A} . En virtud de (1.30) debe ser igual a la i -ésima columna de AN , donde está almacenado el producto de A por la i -ésima columna N_i de N . Por lo tanto,

$$MA_i = AN_i,$$

que es equivalente a

$$(MA_i)_{\mathcal{A}} = N_i.$$

En definitiva, cada columna de N contiene las coordenadas en \mathcal{A} de las imágenes por M de los vectores de la base \mathcal{A} .

Ejemplo 1.7. Al transformar con la matriz M que genera los números de Fibonacci a los vectores X_+ y X_- en (1.17) que forman la base \mathcal{A} encontramos

$$(1.31) \quad MX_+ = \lambda_+ X_+, \quad MX_- = \lambda_- X_-,$$

con $\lambda_{\pm} = (1 \pm \sqrt{5})/2$. De (1.31) concluimos inmediatamente que

$$(MX_+)_{\mathcal{A}} = \begin{bmatrix} \lambda_+ \\ 0 \end{bmatrix}, \quad (MX_-)_{\mathcal{A}} = \begin{bmatrix} 0 \\ \lambda_- \end{bmatrix}.$$

Estos vectores de coordenadas son las columnas de la matriz D en (1.27).

Observación 1.3. Cuando un cambio de base lleva a M a una forma simple, como ocurre en los ejemplos 1.5 y 1.6, entonces:

- la fórmula (1.28) es un resultado de factorización de M como el producto de una matriz sencilla por matrices de cambios de coordenadas;
- la fórmula (1.30) es una especificación fácil de entender de la manera en que M transforma una base del espacio.

La posibilidad de obtener estas descripciones simples de la acción de M es la principal razón para desarrollar toda esta teoría.

Ejercicio 1.9. Hallar la matriz que representa en la base

$$\mathcal{A} = ((1, 1, 1), (1, -1, 0), (0, 1, -1))$$

de \mathbb{R}^3 la acción de la matriz

$$M = \frac{1}{3} \begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{bmatrix}.$$

Interpretar geoméricamente la transformación que M representa.

Ejercicio 1.10. En la base

$$\mathcal{A} = ((1, 1, 1), (1, -1, 0), (0, 1, -1))$$

de \mathbb{R}^3 la acción de una cierta matriz M está representada por

$$N = \begin{bmatrix} 2 & 0 & -3 \\ -1 & 1 & 0 \\ -2 & -2 & 1 \end{bmatrix}.$$

Hallar M .

Diremos que un subespacio $\mathbb{S} \subset \mathbb{R}^n$ es *invariante* por una matriz M si para todo $X \in \mathbb{S}$ se tiene que $MX \in \mathbb{S}$.

Ejercicio 1.11. Consideremos la matriz

$$M = \begin{bmatrix} 3 & 1 & -1 \\ 1 & 3 & -1 \\ 2 & -1 & 3 \end{bmatrix}$$

y los subespacios

$$\mathbb{S}_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3, x_1 = x_2\}, \quad \mathbb{S}_2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3, x_1 = 0, x_2 = x_3\}.$$

1. Mostrar que \mathbb{S}_1 y \mathbb{S}_2 son invariantes para M .
2. Mostrar que

$$\mathcal{A}_1 = ((1, 1, 1), (0, 0, 1)), \quad \mathcal{A}_2 = ((0, 1, 1)),$$

son respectivamente bases de \mathbb{S}_1 y \mathbb{S}_2 , y que

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 = (((1, 1, 1), (0, 0, 1), (0, 1, 1)))$$

es una base de \mathbb{R}^3 .

3. Calcular la matriz N que representa la acción de M en las coordenadas definidas por \mathcal{A} y observar que es una matriz de la forma

$$N = \begin{bmatrix} N_1 & \\ & n_{33} \end{bmatrix},$$

donde N_1 es una matriz 2×2 , ¿podría explicar este fenómeno a partir de las partes anteriores de este ejercicio?

4. Verificar que las columnas de N son las coordenadas en \mathcal{A} de los transformados por M de los vectores de \mathcal{A} .

Nuestro próximo ejercicio generaliza los resultados del ejercicio anterior.

Ejercicio 1.12. Sean $\mathcal{A} = (A_1, \dots, A_k, A_{k+1}, \dots, A_n)$ una base de \mathbb{R}^n , \mathbb{S}_1 el subespacio generado por los primeros k vectores de \mathcal{A} , \mathbb{S}_2 el subespacio generado por los

últimos $n - k$ vectores de \mathcal{A} , y M una matriz tal que \mathbb{S}_1 y \mathbb{S}_2 son invariantes para M . Mostrar que la matriz N que representa la acción de M en la base \mathcal{A} es de la forma

$$N = \begin{bmatrix} N_k & \\ & N_{n-k} \end{bmatrix},$$

donde N_k y N_{n-k} son submatrices $k \times k$ y $(n - k) \times (n - k)$, y el resto de los coeficientes de N son necesariamente nulas.

1.2.1 Cambios de base en \mathbb{R}^n y \mathbb{R}^m

Esta sección generaliza los resultados de la anterior. Consideraremos ahora matrices M cualesquiera, cuadradas o no, de tamaño $m \times n$, con coeficientes en \mathbb{R} . Para una base \mathcal{A} en \mathbb{R}^n y una base \mathcal{B} en \mathbb{R}^m llamaremos A y B a las matrices cuyas columnas son los vectores de \mathcal{A} y \mathcal{B} respectivamente. Indicaremos con $X_{\mathcal{A}}$ e $Y_{\mathcal{B}}$ a las coordenadas de $X \in \mathbb{R}^n$ y de $Y \in \mathbb{R}^m$ respecto a las bases \mathcal{A} y \mathcal{B} respectivamente. Entonces

$$(1.32) \quad AX_{\mathcal{A}} = X, \quad (MX)_{\mathcal{B}} = B^{-1}MX.$$

La primera igualdad en (1.32) implica

$$(1.33) \quad MX = MAX_{\mathcal{A}}.$$

Combinándola con la segunda concluimos que

$$(1.34) \quad (MX)_{\mathcal{B}} = NX_{\mathcal{A}},$$

siendo

$$(1.35) \quad N = B^{-1}MA.$$

Es así que N representa en las bases \mathcal{A} y \mathcal{B} la acción de M . De manera análoga a los resultados que obtuvimos antes, la matriz M satisface

$$(1.36) \quad M = BNA^{-1}.$$

También es cierta la igualdad

$$(1.37) \quad MA = BN,$$

que nuevamente permite leer N como la codificación en términos de la base \mathcal{B} de cómo M transforma a los vectores de \mathcal{A} .

Ejemplo 1.8. La matriz

$$M = \begin{bmatrix} 3 & -1 \\ -1 & 3 \\ -2 & -2 \end{bmatrix}$$

admite la factorización

$$(1.38) \quad M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ -2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{bmatrix}.$$

Si tenemos en cuenta que

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

encontramos

$$M \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ -2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 4 \\ 0 & 0 \end{bmatrix},$$

donde leemos el hecho de que M transforma los vectores de la base

$$\mathcal{A} = \left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right),$$

en $2[1, 1, -2]$ y $4[1, -1, 0]$ respectivamente.

Ejercicio 1.13. Calcular directamente los dos productos de M por los vectores de \mathcal{A} y verificar este resultado.

La simplicidad de la descripción en estas bases de la acción de M , tiene que ver con la sencilla estructura de la segunda matriz en el miembro de la derecha de (1.38).

Observación 1.4. Los resultados de esta sección pueden aplicarse al caso particular $m = n$. Entonces se consiguen fórmulas como (1.36) e (1.37) con matrices M y N cuadradas.

Ejercicio 1.14. Consideremos las bases

$$\mathcal{A} = ((1, 1, 1), (1, -1, 0), (0, 1, -1)), \quad \mathcal{B} = ((-2, 3), (-1, 1)),$$

de \mathbb{R}^3 y \mathbb{R}^2 respectivamente.

1. Dada la matriz

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

hallar la matriz N que representa en las bases \mathcal{A} y \mathcal{B} la acción de M , en el sentido de (1.34).

2. Hallar N , si la matriz N que representa a M en las bases \mathcal{A} y \mathcal{B} en el sentido de (1.34) es

$$M = \frac{1}{3} \begin{bmatrix} 1 & 1 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$$

Ejercicio 1.15. En las base

$$\mathcal{A} = ((1, 1, 1), (1, -1, 0), (0, 1, -1)) \quad \mathcal{B} = ((2, 1, 1), (1, 0, 1), (1, 1, 1))$$

de \mathbb{R}^3 la acción de una cierta matriz M está representada por

$$\begin{bmatrix} 2 & 0 & 3 \\ 1 & 1 & -1 \\ -2 & -2 & 0 \end{bmatrix},$$

en el sentido de (1.34).

1. Hallar M .
2. Hallar la matriz N tal que $(MX)_{\mathcal{A}} = NX_{\mathcal{B}}$.
3. Hallar las matrices que representan a M en todas las posibles combinaciones de las bases \mathcal{A} , \mathcal{B} y \mathcal{C} , donde \mathcal{C} es la base canónica de \mathbb{R}^3 .

1.3 Normas, módulos y distancias

Nociones como la “longitud de un vector” o el “tamaño” de los coeficientes de una matriz son bastante intuitivas. Están relacionadas con estructuras geométricas en los espacios de vectores y matrices reales, y permiten desarrollar una teoría de límites en estos espacios. Presentaremos estas ideas para espacios de matrices. Cuando no hagamos mención explícita de su tamaño asumiremos que son $m \times n$. Como podemos identificar a \mathbb{R}^n con las matrices reales $n \times 1$ todo lo que hagamos para matrices se aplicará también a vectores. Aunque en algunos casos quedará implícito, en otros formularemos definiciones y enunciados específicamente para \mathbb{R}^n . Con cambios mínimos, todos los conceptos pueden extenderse a matrices y vectores complejos.

1.3.1 Convergencia coeficiente a coeficiente

Nuestra próxima definición contiene una primera aproximación a la noción de convergencia para matrices.

Definición 1.1. Diremos que una sucesión M_k , $k = 0, 1, \dots$, de matrices converge a una matriz M cuando $k \rightarrow \infty$ si cada una de los coeficientes de M_k converge en \mathbb{R} al coeficiente correspondiente de M .

Indicaremos la convergencia con la notación $M_k \rightarrow M$ o $\lim_{k \rightarrow \infty} M_k = M$.

Ejemplo 1.9. La sucesión de matrices

$$\begin{bmatrix} (1 + 1/k)^k & k \operatorname{sen}(1/k) \\ (2k + 1)/k & \pi \end{bmatrix}$$

converge a

$$\begin{bmatrix} e & 1 \\ 2 & \pi \end{bmatrix}.$$

Ejercicio 1.16. Mostrar que $M_k \rightarrow M$ si y sólo si $M_k - M \rightarrow O$.

1.3.2 Normas

La convergencia de una sucesión de matrices reales puede caracterizarse a través de una única sucesión numérica. Si M es una matriz $m \times n$ con coeficientes m_{ij} definimos

$$(1.39) \quad \|M\|_* = \max \{|m_{ij}|, i = 1, \dots, m, j = 1, \dots, n.\},$$

que es simplemente el más grande de los módulos de los coeficientes de M .

Ejercicio 1.17. Mostrar que $M_k \rightarrow M$ si y sólo si $\|M_k - M\|_* \rightarrow 0$.

Los números $\|M\|_*$ son una manera de medir el “tamaño” de las matrices, que se generaliza en el sentido la siguiente definición.

Definición 1.2. Norma. Una *norma* en el conjunto de las matrices reales $m \times n$ es una función $\|\cdot\|$ que a cada matriz le asocia un número real y que tiene las siguientes propiedades:

1. **No negatividad y no degeneración.** $\|M\| \geq 0$ y $\|M\| = 0$ si y sólo si $M = O$;
2. **Homogeneidad:** $\|\alpha M\| = |\alpha| \|M\|$ para cualquier número α y matriz M .
3. **Desigualdad triangular:** $\|M + N\| \leq \|M\| + \|N\|$ para cualquier par de matrices M y N .

Ejercicio 1.18. Mostrar que la función $\|\cdot\|_*$ definida por (1.39) es una norma en el sentido de la definición 1.2.

Sobre los conjunto de matrices $m \times n$, o sobre los espacios \mathbb{R}^n , es posible definir muchas normas diferentes, que dan lugar a geometrías diferentes. Introduciremos ahora en \mathbb{R}^n un ejemplo al que volveremos en el capítulo 5. Para

$$X = (x_1, \dots, x_n) \in \mathbb{R}^n$$

definimos

$$(1.40) \quad \|X\|_1 = \sum_{i=1}^n |x_i|.$$

Ejemplo 1.10. Para $(1, 2, -1) \in \mathbb{R}^3$ la fórmula (1.40) implica $\|(1, 2, -1)\|_1 = 4$.

Ejercicio 1.19. Demostrar que la función $\|\cdot\|_1$ definida en \mathbb{R}^n por la fórmula (1.40) es una norma.

Cualquier norma $\|\cdot\|$, no solo $\|\cdot\|_*$, proporciona una noción de convergencia para matrices o vectores.

Definición 1.3. Convergencia respecto a una norma. Una sucesión

$$M_k, \quad k = 1, 2, \dots,$$

de matrices converge a M respecto a la norma $\|\cdot\|$ si

$$\lim_{k \rightarrow \infty} \|M - M_k\| = 0.$$

Proposición 1.4. Una sucesión X_k en \mathbb{R}^n converge a X respecto a la norma $\|\cdot\|_1$ si y sólo si converge en el sentido de la definición 1.1.

Demostración. Llamemos $x_{k,i}$ y x_i a los i -ésimos coeficiente de los vectores X_k y X , respectivamente. Para cada valor de i se satisface

$$|x_{k,i} - x_i| \leq \|X_k - X\|_1,$$

lo que implica que si $\|X_k - X\|_1 \rightarrow 0$ entonces cada una de las sucesiones $x_{k,i}$ converge a x_i cuando $n \rightarrow \infty$.

Recíprocamente, si para todo $i = 1, \dots, n$ se tiene que

$$(1.41) \quad \lim_{k \rightarrow \infty} |x_{k,i} - x_i| = 0,$$

sumando los n posibles valores de i en (1.41) concluimos que

$$\lim_{k \rightarrow \infty} \sum_{i=1}^n |x_{k,i} - x_i| = 0,$$

que es la condición para la convergencia de X_k a X respecto a la norma $\|\cdot\|_1$. \square

1.3.3 El producto escalar y el módulo

Una importante noción de tamaño para los vectores es su *longitud* o *módulo*. Este concepto depende del *producto escalar* definido para una pareja cualquiera X e Y de vectores en \mathbb{R}^n por

$$(1.42) \quad X \cdot Y = \sum_{i=1}^n x_i y_i.$$

La noción de *módulo* está definida por

$$(1.43) \quad |X| = \sqrt{X \cdot X},$$

y satisface la fundamental desigualdad de Cauchy-Schwarz

$$|X \cdot Y| \leq |X||Y|,$$

que supondremos conocida para el lector.

Ejercicio 1.20. El módulo (1.43) es una norma en \mathbb{R}^n . Sugerencia: elevar el módulo al cuadrado y usar la desigualdad de Cauchy-Schwarz para demostrar la desigualdad triangular.

Ejemplo 1.11. El módulo de $(1, 2, -1) \in \mathbb{R}^3$ es $\sqrt{6}$, aunque su tamaño medido con $\|\cdot\|_1$ es igual a 4.

Un importante conjunto de vectores de \mathbb{R}^n es el que está formado por los vectores de módulo 1, al que llamaremos *esfera unidad* e indicaremos con S^{n-1} .

Ejercicio 1.21. Representar las esferas unidad S^1 y S^2 de \mathbb{R}^2 y de \mathbb{R}^3 respectivamente, y los vectores X tales que $\|X\|_1 = 1$. Comparar con S^1 y S^2 los conjuntos formados por estos vectores.

Ejercicio 1.22. Demostrar que si X_k , $k = 1, 2, \dots$, y X son vectores de \mathbb{R}^n entonces son equivalentes:

1. $X_k \rightarrow X$ en el sentido de la definición 1.1;
2. $X_k \rightarrow X$ respecto al módulo $|\cdot|$;

3. $X_k \rightarrow X$ respecto a la norma $\|\cdot\|_1$.

Observación 1.5. El ejercicio 1.22 es un caso particular de la siguiente afirmación general: todas las normas en \mathbb{R}^n definen la misma noción de convergencia. La geometría del espacio cambia al cambiar de norma (ver el ejercicio 1.21), pero no la convergencia de vectores, que es una noción topológica, de otra categoría diferente que la noción métrica definida por la norma².

Las nociones de producto escalar y módulo se generalizan a \mathbb{C}^n a partir de la fórmula

$$(1.44) \quad X \cdot Y = \sum_{i=1}^n x_i \overline{y_i}$$

donde \bar{z} indica el conjugado de un número complejo z .

1.3.4 Una nueva norma sobre las matrices

Cuando una matriz real M de tamaño $m \times n$ multiplica a un vector $X \in \mathbb{R}^n$, produce un nuevo vector $MX \in \mathbb{R}^m$ cuyo módulo $|MX|$ es en general diferente a $|X|$. Si $X \neq 0$ el cociente $|MX|/|X|$ mide la “dilatación” o “cambio de tamaño” que M produce sobre X .

Ejercicio 1.23. Para la matriz

$$(1.45) \quad M = \begin{bmatrix} 4 & 0 \\ 3 & -5 \end{bmatrix}.$$

calcular los cocientes $|MX|/|X|$ sobre los vectores $(1, 1)$, $(1, -1)$, $(1, 0)$, $(0, 1)$.

El valor máximo de los cocientes $|MX|/|X|$ con $X \neq 0$, es decir, la máxima dilatación que M produce sobre los vectores de \mathbb{R}^n , es una norma que indicaremos con la notación $\|\cdot\|_2$.

Ejercicio 1.24. Mostrar que el conjunto de valores que toman los cocientes $|MX|/|X|$ con $X \neq 0$ coincide con el conjunto de valores $|MY|$, con $Y \in S^{n-1}$.

Para mostrar que el máximo que estamos buscando realmente existe podemos recurrir al siguiente importante teorema del cálculo en \mathbb{R}^n :

Teorema 1.5. Sea $f : \mathbb{R}^n \rightarrow \mathbb{R}$ una función continua y \mathcal{X} un subconjunto cerrado y acotado de \mathbb{R}^n . Entonces f tiene en \mathcal{X} un máximo y un mínimo.

El ejercicio 1.24 implica que $\|M\|_2$ es el máximo sobre S^{n-1} de la función continua $X \mapsto |MX|$ que a cada $X \in \mathbb{R}^n$ le asocia el número real $|MX|$. Además S^{n-1} es un conjunto cerrado y acotado (ver el ejercicio 1.35, página 41). Entonces el teorema 1.5 asegura que el máximo $\|M\|_2$ efectivamente existe.

²Sólo en espacios vectoriales de dimensión infinita, normas diferentes pueden inducir nociones diferentes de convergencia. Los espacios de matrices y los espacios \mathbb{R}^n tienen todos dimensión finita.

En la sección 4.2 volveremos sobre este concepto. Allí caracterizaremos $\|M\|_2$ en términos de los *valores singulares* de M , y daremos una demostración alternativa, que no hace uso del teorema 1.5, de que el máximo $\|M\|_2$ existe.

Ejercicio 1.25. Mostrar que para todo $X \in \mathbb{R}^n$ se satisface $|MX| \leq \|M\|_2|X|$.

Ejercicio 1.26. Mostrar que $\|\cdot\|_2$ es una norma. Sugerencia: para demostrar la desigualdad triangular puede ser útil el resultado del ejercicio 1.25

1.3.5 Distancias

Una norma $\|\cdot\|$ definida sobre las matrices permite cuantificar con el número $\|M - N\|$ la diferencia entre dos matrices M y N , lo que genera en el espacio de las matrices una noción de *distancia*. La noción de distancia es aún más general, y puede definirse sobre conjuntos cualesquiera.

Definición 1.6. Distancia. Sea \mathcal{X} un conjunto cualquiera. Una *distancia* en \mathcal{X} es una función d que a cada par (x, y) de elementos de \mathcal{X} le asocia un número real $d(x, y)$ que tiene las propiedades:

1. **No negatividad y no degeneración.** $d(x, y) \geq 0$ y $d(x, y) = 0$ si y sólo si $x = y$;
2. **Simetría.** $d(x, y) = d(y, x)$ para x e y cualesquiera en \mathcal{X} ;
3. **Desigualdad triangular.** $d(x, y) \leq d(x, z) + d(z, y)$ para x, y y z cualesquiera en \mathcal{X} .

Ejercicio 1.27. Mostrar que si $\|\cdot\|$ es una norma en el conjunto de las matrices reales $m \times n$, entonces

$$(1.46) \quad d(M, N) = \|M - N\|$$

es una distancia, a la que se llama *distancia inducida por* $\|\cdot\|$.

En \mathbb{R}^n el módulo $|\cdot|$ induce una distancia que para $n = 2$ y $n = 3$ corresponde, respectivamente, a la distancia euclidiana en el plano y en el espacio. Para valores más grandes de n generaliza a la distancia euclidiana manteniendo muchas de sus propiedades. Ver el capítulo 3.

Ejercicio 1.28. Cuando decimos que dos esquinas opuestas de una manzana cuadrada en una ciudad están a doscientos metros de distancia, ¿qué noción de distancia estamos usando?, ¿la euclídea o una que corresponde a $\|\cdot\|_1$?

Observación 1.6. La distancia que $\|\cdot\|_1$ induce en \mathbb{R}^n suele llamarse *distancia del taxista*, y a la geometría que genera *geometría del taxista*. ¿Podría el lector justificar por qué?

Ejercicio 1.29. Mostrar que una sucesión de matrices M_k converge a M si y sólo si $d_*(M_k, M) \rightarrow 0$, donde d_* es la distancia inducida por la norma $\|\cdot\|_*$.

Cualquier distancia permite introducir una noción de convergencia en el conjunto \mathcal{X} en que está definida.

Definición 1.7. Consideremos un conjunto \mathcal{X} con una distancia d . Una sucesión X_k , $k = 1, 2, \dots$, de elementos de \mathcal{X} converge a $X \in \mathcal{X}$ respecto a la distancia d si y sólo si $\lim_{k \rightarrow \infty} d(X_k, X) = 0$.

Naturalmente, la definición 1.3 es el caso particular de la definición 1.7 en el que la distancia d es inducida por la norma $\|\cdot\|$. Usaremos normas, y distancias inducidas por normas, para manejar distintos procesos de paso al límite en varias partes de este texto.

Para ilustrar la flexibilidad del concepto, presentamos a continuación un ejemplo de distancia que toma valores discretos, y que origina una rica estructura geométrica que explotaremos en el capítulo 6, pero en la que la noción de convergencia es prácticamente irrelevante (ver el ejercicio 1.38, página 41).

Llamaremos \mathcal{X}^n al conjunto de todas las posibles listas (x_1, \dots, x_n) de longitud n formadas por elementos de un conjunto \mathcal{X} cualquiera. Un ejemplo de esta construcción, con $\mathcal{X} = \mathbb{R}$, es \mathbb{R}^n

Definición 1.8. Distancia de Hamming. La distancia de Hamming $d(X, Y)$ entre X e Y en \mathcal{X}^n es igual a la cantidad de posiciones en que las dos listas X e Y difieren.

Proposición 1.9. *La distancia de Hamming d es una distancia en \mathcal{X}^n .*

Demostración. Escribamos

$$d(X, Y) = |\{i : x_i \neq y_i\}|,$$

donde $|\cdot|$ indica el cardinal, o cantidad de elementos, de un conjunto. La comparación de Y con Z divide $\{i : x_i \neq y_i\}$ en dos conjuntos disjuntos, de modo que

$$|\{i : x_i \neq y_i\}| = |\{i : x_i \neq y_i, y_i = z_i\}| + |\{i : x_i \neq y_i, y_i \neq z_i\}|.$$

Además

$$\begin{aligned} |\{i : x_i \neq y_i, y_i = z_i\}| &= |\{i : x_i \neq z_i, y_i = z_i\}| \leq |\{i : x_i \neq z_i\}| = d(X, Z), \\ |\{i : x_i \neq y_i, y_i \neq z_i\}| &\leq |\{i : y_i \neq z_i\}| = d(Z, Y). \end{aligned}$$

Concluimos entonces que la desigualdad

$$d(X, Y) \leq d(X, Z) + d(Z, Y)$$

se satisface para cualquier terna de listas X , Y y Z . □

Ejercicio 1.30. Mostrar las propiedades de simetría, no negatividad y no degeneración de d para completar la demostración.

Una noción muy importante en un conjunto \mathcal{X} que tiene una distancia d es la de *isometría*. Una isometría es una función f que conserva la distancia, en el sentido de que

$$d(f(x), f(y)) = d(x, y), \quad x, y \in \mathcal{X}.$$

Las isometrías juegan un papel muy importante en la geometría elemental del plano y del espacio, pero no son sólo interesantes en este contexto. Ver el ejercicio 3.14 en la página 85, y la sección 4.1.4. También la monografía [1].

1.3.6 Ejercicios adicionales

Ejercicio 1.31. En lo que sigue consideraremos sucesiones convergentes de matrices $M_k \rightarrow M$ y $N_k \rightarrow N$.

1. Mostrar que si las sumas $M_k + N_k$ y $M + N$ existen entonces

$$M_k + N_k \rightarrow M + N.$$

2. Mostrar que si los productos $M_k N_k$ y MN existen entonces

$$M_k N_k \rightarrow MN.$$

Ejercicio 1.32. En este ejercicio todas las matrices son cuadradas $n \times n$ y A es invertible. Mostrar que $M_k \rightarrow M$ si y sólo si $AM_k A^{-1} \rightarrow AMA^{-1}$.

Ejercicio 1.33. Mostrar que existen constantes positivas c_1 y c_2 tales que las desigualdades

$$c_1 \|X\|_1 \leq |X| \leq c_2 \|X\|_1$$

se satisfacen para todo $X \in \mathbb{R}^n$. Determinar los valores óptimos de c_1 y c_2 .

Ejercicio 1.34. Mostrar que si $M_k \rightarrow M$ respecto a una norma $\|\cdot\|$, entonces $\|M_k\| \rightarrow \|M\|$. ¿Es cierto el recíproco?

Ejercicio 1.35. Mostrar que si X_k es una sucesión de vectores en $S^{n-1} \subset \mathbb{R}^n$ que converge a X entonces $|X| = 1$. Sugerencia: usar el ejercicio 1.34

Ejercicio 1.36. Mostrar que si M es una matriz $m \times n$ entonces

$$\|M\|_* \leq \|M\|_2 \leq n\sqrt{m}\|M\|_*.$$

Estudiar si estas acotaciones son óptimas.

Ejercicio 1.37. Sea \mathcal{X} un conjunto cualquiera. Mostrar que la función d definida por

$$d(x, y) = \begin{cases} 1, & x \neq y, \\ 0, & x = y, \end{cases}$$

es una distancia en \mathbb{X} . ¿Cuáles son las sucesiones convergentes respecto a la distancia d en el espacio \mathcal{X} ?

Ejercicio 1.38. ¿Cuáles son las sucesiones de \mathbb{R}^n que convergen respecto a la distancia de Hamming?, ¿cómo se compara esta noción de convergencia con las del ejercicio 1.22, página 37?, ¿contradice este resultado a la observación 1.5?

Capítulo 2: Vectores y valores propios



Una matriz cuadrada real $n \times n$ define una transformación

$$X \mapsto MX$$

de \mathbb{R}^n en \mathbb{R}^n . Lo mismo vale en \mathbb{C}^n para una matriz compleja $n \times n$. En este capítulo nos interesarán los vectores X que M transforma de una manera simple, en el sentido de que MX es un múltiplo escalar λX de X . Son lo que llamaremos *vectores propios* de M . Con λ indicamos un número real (o complejo), al que llamaremos *valor propio* de M . Los valores y vectores propios de una matriz constituyen información clave para entender su estructura, y suelen tener importancia a la hora de resolver problemas prácticos en los que intervienen matrices cuadradas.

En la sección 2.1 formalizamos los conceptos de valor y vector propio, y en la 2.2 discutimos cómo calcularlos. Cuando una matriz tiene una base de vectores propios se vuelve muy fácil trabajar con ella en esta nueva base. Discutir este fenómeno y algunas de sus aplicaciones es el objeto de la sección 2.3. Hay muchas más aplicaciones que las que se discuten en este texto, pero es imposible discutir las por razones de espacio. El lector interesado podrá encontrar información adicional en la literatura y en la web. En la sección 2.4 estudiamos las potencias M^k de matrices M , y su comportamiento cuando $k \rightarrow \infty$.

2.1 Vectores y valores propios

Cuando una matriz cuadrada M actúa sobre un vector X para producir MX se obtiene como resultado un nuevo vector que, en principio, no tiene por qué estar en la dirección de X .

Ejemplo 2.1. Al transformar con la matriz

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

los vectores $(1, 0)$ y $(0, 1)$ de \mathbb{R}^2 obtenemos

$$M \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad M \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Las imágenes no están alineadas con los vectores que fueron transformados. En realidad, para casi todos los vectores del plano la dirección de MX no coincide con la

de X . Pero hay vectores excepcionales:

$$M \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix} = \frac{1+\sqrt{5}}{2} \begin{bmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{bmatrix}, \quad M \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix} = \frac{1-\sqrt{5}}{2} \begin{bmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{bmatrix}.$$

El lector puede verificar estas fórmulas, o volver a la discusión de las secciones 1.1 y 1.2. Disponer de una base de \mathbb{R}^2 formada por esta clase de vectores fue clave en la resolución del problema de los números de Fibonacci en la sección 1.1.

Ejercicio 2.1. Considerar la matriz

$$(2.1) \quad M = \begin{bmatrix} 8 & -5 \\ 10 & -7 \end{bmatrix}$$

y para los vectores $(1, 1)$, $(1, 2)$, $(1, 0)$ y $(0, 1)$ comparar sus direcciones con las de sus imágenes por M .

Definición 2.1. Sea M una matriz $n \times n$. Si existen un número λ y un vector no nulo X tales que

$$(2.2) \quad MX = \lambda X,$$

diremos que X es un *vector propio* de M y que λ es el *valor propio* asociado a X .

Observación 2.1. Para que la definición 2.1 tenga algún sentido es importante la condición de que X sea un vector no nulo. Ya que el vector nulo O satisface trivialmente

$$MO = O = \lambda O$$

para cualquier matriz cuadrada M y cualquier valor de λ .

Tanto la definición como esta discusión pueden hacerse sobre cualquier cuerpo, pero trabajaremos con ella sobre \mathbb{R} y \mathbb{C} .

La ecuación (2.2) es equivalente a

$$(M - \lambda I)X = O,$$

donde I es la matriz identidad $n \times n$. Vemos entonces que los vectores propios son todos los vectores no nulos en $\ker(M - \lambda I)$, el núcleo de $M - \lambda I$, y existirán sólo para los valores de λ que hacen que ese núcleo no sea trivial. A la dimensión de $\ker(M - \lambda I)$ se le llama *multiplicidad geométrica* del valor propio λ .

Ejercicio 2.2. Mostrar que $\ker(M)$ es no trivial si y sólo si 0 es un valor propio de M .

Ejercicio 2.3. Mostrar que si M conmuta con N , y X es un vector propio de M con valor propio λ , entonces NX es el vector nulo o también es un vector propio de M con valor propio λ .

Ejercicio 2.4. Sea M una matriz $n \times n$ y \mathbb{S} un subespacio de \mathbb{R}^n que es invariante para M y que tiene dimensión 1. Mostrar que todos los vectores no nulos de \mathbb{S} son vectores propios de M .

2.1.1 La web y Google: primera aproximación

En esta sección comenzamos a discutir un ingrediente del funcionamiento del buscador Google: el criterio de ordenamiento de los resultados de las búsquedas. Retomaremos luego este tema en la sección 5.1, en conexión con problemas de paseos al azar sobre una red.

Nota Histórica 2.1. *Buscar alguna pieza de información en la web es un auténtico desafío, cuya dificultad suele pasar inadvertida para el usuario porque cuenta con poderosas herramientas automáticas de búsqueda. Entre los muchos problemas que un buscador debe resolver está el de ordenar los resultados obtenidos, que pueden ser numerosísimos, de una manera útil. Por ejemplo, durante la escritura de este texto, buscando a partir de la expresión **vectores propios** conseguimos unas 15.800 respuestas. El mismo intento con la expresión inglesa **eigenvectors** devolvió más de un millón y medio de páginas, ¿por cuál empezar a mirar?*

En el celebrado artículo The Anatomy of a Large-Scale Hypertextual Web Search Engine de 1998, Serguei Brin y Larry Page presentan la idea de hacer un uso eficiente de la propia estructura de la web para ordenar las consultas: “The citation (link) graph of the web is an important resource that has largely gone unused in existing web search engines”¹. Por ejemplo, si una página web recibe muchos enlaces es de presumir que tendrá contenidos interesantes. Sobre estos conceptos está basado el algoritmo PageRank, que produce el ordenamiento que el buscador Google emplea para mostrar sus resultados. Si le interesa, el lector podrá reconstruir el resto de la historia. ¿Considera necesaria una sugerencia acerca de qué, dónde y cómo buscar?

Vamos a hacer un primer intento de ordenamiento siguiendo el lema ‘un enlace recibido, un voto recibido’, que implementaremos con herramientas de cálculo matricial.

En la web hay un cierto número N de páginas. Cada una de ellas puede ser numerada, asignándole un número natural i , con $1 \leq i \leq N$. Definimos una matriz C , cuadrada $N \times N$, con coeficientes c_{ij} tales que c_{ij} es igual a la cantidad de enlaces que hay desde la j -ésima página hacia la i -ésima. Llamaremos a esta matriz C la *matriz de conectividad* de la red.

Ejemplo 2.2. La red del primer esquema de la figura 2.1 tiene asociada la matriz

¹ “El grafo de citas (enlaces) de la web es un importante recurso que no ha sido usado en los motores de búsqueda existentes.”

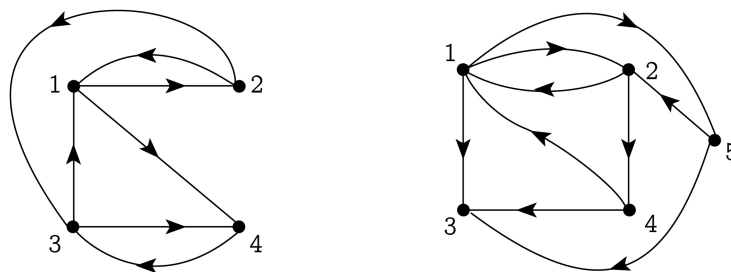


FIGURA 2.1. Dos redes sencillas

$$(2.3) \quad C = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Ejercicio 2.5. Escribir la matriz de conectividad de la segunda red en la figura 2.1. Generar una matriz cuadrada cualquiera con ceros y unos, y dibujar la red que representa.

En la i -ésima fila de una matriz de conectividad C aparecen registrados todos los enlaces entrantes a la i -ésima página. El número total de ellos es la suma de los coeficientes en esa fila. Por lo tanto, la suma de las columnas de C , que es el vector

$$(2.4) \quad P = C\mathbf{1},$$

donde $\mathbf{1}$ indica una columna de unos, contiene en el coeficiente i el número de enlaces que recibe la página i .

Ejemplo 2.3. Para la primera red de la figura 2.1 tenemos

$$P = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 2 \\ 2 \end{bmatrix}.$$

Nuestro ordenamiento considera menos importante al nodo 2, y empata en el primer puesto a los otros tres nodos, con dos enlaces cada uno.

Ejercicio 2.6. Calcular P para la segunda red de la figura 2.1

El vector P da una primera solución al problema del ordenamiento de las páginas, que consiste en asignar a cada página un puntaje igual a la cantidad de enlaces que recibe, y luego ordenarlas por este puntaje. Pero no es lo mismo recibir un enlace desde una página buena que desde otra irrelevante. Para levantar esta objeción

asignaremos a los enlaces que recibe la página i pesos diferentes, proporcionales a los puntajes de las páginas j desde las que vienen los enlaces. Luego sumaremos los votos así ponderados, para obtener el puntaje de la página i . Parece que para determinar los puntajes es necesario conocerlos previamente. Pero no es así. Nuestro nuevo modelo, más sofisticado que (2.4), genera un sistema de ecuaciones lineales que relaciona los puntajes. Ahora la contribución de la página j al puntaje de la página i no será simplemente c_{ij} sino

$$\alpha c_{ij} p_j,$$

donde p_j es el puntaje de la página j y α una constante positiva de proporcionalidad. Al sumar sobre todos los posibles valores de j concluimos que el puntaje p_i de la i -ésima página debe satisfacer

$$(2.5) \quad p_i = \alpha \sum_{j=1}^n c_{ij} p_j, \quad 1 \leq i \leq N.$$

Las N igualdades (2.5) pueden resumirse en la igualdad matricial

$$(2.6) \quad P = \alpha CP.$$

Tomando $\lambda = 1/\alpha$ escribimos (2.6) en la forma del problema de valores y vectores propios

$$(2.7) \quad CP = \lambda P.$$

La fórmula (2.7) nos está diciendo que P debe ser un vector propio de la matriz de conectividad C , con un valor propio λ positivo. Ya no se trata del sencillo vector P de puntajes en (2.4), es más difícil de calcular, pero mucho más significativo.

Ejemplo 2.4. Este nuevo criterio arroja para la primera red en la figura 2.1 el puntaje

$$P \simeq (0,2548, 0,1513, 0,2777, 0,3162),$$

que destaca a la página 4 como la más importante. El valor de la constante λ es 1,6838.

Los cálculos de este ejemplo, y los demás ejemplos de esta sección, fueron realizados con MatLab.

Observación 2.2. En realidad cualquier múltiplo positivo del vector de puntajes es admisible. La elección que hicimos fue normalizar el vector de modo que sus coeficientes sumaran 1. Si hubiéramos usado con $(2, 1, 2, 2)$ este mismo criterio el resultado habría sido aproximadamente igual a $(0,2857, 0,1429, 0,2857, 0,2857)$.

El modelo todavía puede refinarse un poco más: estamos permitiendo a cada página que ‘vote’ tantas veces quiera, poniendo enlaces. Además de pesar el voto de las páginas con su importancia individual, tiene sentido normalizarlo de modo tal que la incidencia total de la página no dependa de la cantidad de enlaces hacia otras páginas que contenga. Esto se consigue dividiendo el aporte de cada enlace por la cantidad total de enlaces que salen de la página, y origina una matriz de conectividad

normalizada N , donde cada entrada n_{ij} es igual a c_{ij} dividido el total de enlaces que contiene la página j . El vector P de puntajes se calcula ahora a partir de la ecuación

$$(2.8) \quad NP = \lambda P.$$

Ejemplo 2.5. Para la red de los ejemplos 2.3 y 2.4 la matriz normalizada es

$$(2.9) \quad N = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{bmatrix}$$

y el puntaje P determinado a partir de (2.8) es

$$(2.10) \quad P \simeq (0,2353, 0,1176, 0,3529, 0,2941),$$

y ahora la página 3 es la mejor puntuada. La constante λ toma el valor 1.

Observación 2.3. ¿Podremos ponernos de acuerdo? Es interesante observar que los distintos criterios de ordenamiento produjeron distintos resultados. Seguramente es también conocido para el lector algún ejemplo en el que la elección de un presidente o de representantes se vea afectada por las reglas que se adopten: existencia o no de primeras y segundas vueltas; división en circunscripciones o circunscripción única; sistemas de proporcionalidad integral o sistemas en los que el ganador se lleva todas las plazas; etcétera. O haya discutido cómo el sistema de disputa de algún campeonato deportivo favorece o perjudica a su equipo predilecto. Estas dificultades son típicas de los mecanismos sociales de elección.

Nota Histórica 2.2. *Un célebre teorema de Kenneth Arrow publicado en 1950 asegura que no puede existir un mecanismo de elección universal que satisfaga algunos principios simples que aparecen intuitivamente como deseables. Por ésta y otras contribuciones Arrow recibió el Premio Nobel de Economía en 1972.*

Ejercicio 2.7. Buscar información sobre los problemas matemáticos de la elección social. Una referencia útil puede ser [2].

2.1.2 Modelo de Leontief de una economía en equilibrio

Supongamos que podemos agrupar la actividad económica de un país en cuatro sectores productivos, a los que llamaremos, sin mayor pretensión que la de introducir una terminología que resulte sugerente, el transporte, la alimentación, la extracción de recursos naturales y la fabricación de útiles y herramientas. Estos interactúan entre sí, ya que cada sector utiliza recursos de los demás, al tiempo que los provee con parte de su producción. Supongamos además que las relaciones entre estos sectores pueden resumirse en la siguiente tabla:

	tr	al	ex	fa
tr	0.1	0.1	0.1	0.3
al	0.3	0.3	0.1	0.2
ex	0.4	0.3	0.1	0.4
fa	0.2	0.3	0.7	0.1

La tabla expresa que el 10 % del transporte se utiliza para mantener funcionando el propio sistema de transporte, el 30 % está dedicado a la distribución de alimentos, el 40 % afectado a la extracción de recursos naturales y el 20 % restante es un insumo para el sector de la economía que fabrica útiles y herramientas. Las restantes columnas de la tabla indican cómo se distribuye el producto de los otros tres sectores de la economía. Todas las columnas suman uno porque nuestro modelo asume que la economía es cerrada, y no hay interacciones con otras economías ni debe atenderse una demanda externa.

Este modelo atiende a la siguiente pregunta: ¿existen precios para el transporte, los alimentos, los recursos naturales y los útiles y herramientas que permitan el equilibrio de la economía, en el sentido de que cada sector reciba por sus productos una cantidad igual a la que paga por sus insumos? Si tales precios existen, el vector $P = [p_{tr}, p_{al}, p_{ex}, p_{fa}]$ de precios debe satisfacer la igualdad

$$(2.11) \quad MP = P.$$

donde M es la matriz formada por las entradas de la tabla. En resumen, el vector de precios debe ser un vector propio de M , con valor propio igual a 1. Para que los precios tengan sentido las entradas de P tienen que ser positivas, o al menos no negativas. Al calcular las soluciones de (2.11) encontramos que cualquier vector de la forma

$$\alpha(0,1667, 0,2083, 0,2917, 0,3333),$$

donde α es una constante positiva, es admisible como vector de precios. Un momento de reflexión nos convencerá de que la indeterminación expresada por la constante α es completamente natural, porque expresa que cualquier unidad monetaria puede ser tomada para expresar los precios.

Nota Histórica 2.3. *El economista Wassily Leontief introdujo modelos en los que la economía de un país se descompone en diversos sectores, cuyas interacciones pueden cuantificarse y analizarse. Por el desarrollo de los modelos input-output y su aplicación a importantes problemas económicos obtuvo el Premio Nobel de Economía en 1973.*

Ejercicio 2.8. Para una economía con tres sectores I , II y III , cuyas relaciones se expresan en la tabla

	I	II	III
I	0.1	0.8	0.7
II	0.5	0.1	0.0
III	0.4	0.1	0.3

hallar los vectores de precios en el estado de equilibrio de la economía.

Observación 2.4. Puntos fijos. Un *punto fijo* de una función $f : \mathcal{X} \rightarrow \mathcal{X}$, definida sobre algún conjunto \mathcal{X} , es un elemento x de \mathcal{X} que satisface

$$x = f(x).$$

Es decir, todo punto fijo es su propia imagen por f . El concepto de punto fijo es importante en muchas ramas de la matemática. En el apéndice C.1.1 mostramos un resultado de existencia de puntos fijos, que aplicaremos en el capítulo 5. Ver también las monografías [5] y [15].

Cuando la transformación f está definida por una matriz M la condición de que X sea un punto fijo se escribe como $MX = X$: los puntos fijos son los vectores propios de M con valor propio 1. Tal como el vector (2.10) para la matriz (2.5).

2.2 Cálculo de valores y vectores propios

En esta sección desarrollaremos algunas ideas sobre el cálculo de los valores propios de una matriz.

2.2.1 Polinomio característico

Una matriz cuadrada M tiene vectores propios asociados al valor propio λ si y sólo si el subespacio $\ker(M - \lambda I)$ es distinto del subespacio trivial $\{O\}$. Tal cosa ocurre si y sólo si la matriz $M - \lambda I$ es no invertible, y está caracterizada por el hecho de que

$$(2.12) \quad \det(M - \lambda I) = 0.$$

Ejemplo 2.6. Para la matriz

$$(2.13) \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

que en la sección 1.1 aparecía generando los números de Fibonacci, tenemos

$$\det(M - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ 1 & 1 - \lambda \end{vmatrix} = \lambda^2 - \lambda - 1.$$

La ecuación (2.12) toma la forma $\lambda^2 - \lambda - 1 = 0$, con raíces $\lambda_{\pm} = (1 \pm \sqrt{5})/2$. En la página 26 habíamos encontrado la misma ecuación (ecuación (1.10)), pero por un procedimiento diferente.

Una vez hallados los dos valores propios λ_{\pm} , con ellos se resuelven los dos sistemas de ecuaciones lineales

$$\left[\begin{array}{cc|c} -\lambda_{\pm} & 1 & 0 \\ 1 & 1 - \lambda_{\pm} & 0 \end{array} \right].$$

El conjunto de soluciones no triviales de cada uno de estos sistemas es

$$x_1(1, \lambda_{\pm}), \quad x_1 \in \mathbb{R}, \quad x_1 \neq 0.$$

Estos son justamente los vectores propios de M . El lector puede completar los detalles, que también aparecen en la página 26.

Para una matriz cuadrada $n \times n$ el determinante $\det(M - \lambda I)$ siempre es un polinomio $p(\lambda)$ de grado n en λ , al que se llama *polinomio característico* de M .

Ejercicio 2.9. Demostrar esta afirmación sobre $\det(M - \lambda I)$.

Los valores propios de M son justamente las raíces de su polinomio característico. A la multiplicidad de cada valor propio λ de M como raíz del polinomio característico se le llama *multiplicidad algebraica* de λ .

Ejemplo 2.7. La matriz

$$M = \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix}$$

tiene como polinomio característico

$$P(\lambda) = \lambda^2 - (6/5)\lambda + 1/5.$$

Sus valores propios son $\lambda = 1$ y $\lambda = 1/5$. El subespacio $\ker(M - I)$ contiene a todos los vectores propios asociados al valor propio 1 y está generado por $(3, 1)$. El subespacio $\ker(M - (1/5)I)$ está generado por $(-1, 1)$. Las multiplicidades algebraica y geométrica de ambos valores propios son iguales a 1.

Ejercicio 2.10. Hallar el polinomio característico, los valores propios y los vectores propios de la matriz $5M$, ¿cómo se relacionan con los de M ?

Ejercicio 2.11. Mostrar que dos matrices semejantes tienen el mismo polinomio característico y los mismos valores propios.

Ejemplo 2.8. El polinomio característico de

$$(2.14) \quad M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

es $\det(M - \lambda I) = \lambda^2 + 1$. Por lo tanto M no tiene ningún valor propio real ni vectores propios en \mathbb{R}^2 .

Observación 2.5. Como $\mathbb{R} \subset \mathbb{C}$ la matriz (2.14) del ejemplo 2.8 puede considerarse como una matriz compleja. La técnica de pasar al campo complejo para considerar problemas de números reales es útil en diversas partes de la matemática. Haremos uso de ella en varias partes de esta monografía. Ver, por ejemplo, el corolario 2.3, página 52.

Ejemplo 2.9. La matriz (2.14) admite los valores propios complejos $\pm i$. Para encontrar los vectores propios correspondientes resolvemos los dos sistemas

$$\left[\begin{array}{cc|c} \mp i & -1 & 0 \\ 1 & \mp i & 0 \end{array} \right].$$

Los vectores propios son de la forma

$$z \begin{bmatrix} 1 \\ i \end{bmatrix}, \quad z \begin{bmatrix} 1 \\ -i \end{bmatrix},$$

respectivamente, para cualquier z no nulo en \mathbb{C} .

Ejercicio 2.12. Hallar los valores y vectores propios de

$$\begin{bmatrix} 0 & -4 \\ 1 & 2\sqrt{3} \end{bmatrix}.$$

Proposición 2.2. *Toda matriz cuadrada compleja tiene al menos un valor propio.*

Demostración. Por el Teorema Fundamental del Álgebra (ver la monografía [11]), el polinomio característico de la matriz tiene al menos una raíz λ en \mathbb{C} , que es un valor propio de la matriz. \square

Corolario 2.3. *Toda matriz cuadrada real tiene al menos un valor propio sobre \mathbb{C} .*

Ejercicio 2.13. Encontrar los valores y vectores propios de las matrices reales

$$\begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 4 & -3 \\ 3 & -2 \end{bmatrix}.$$

Hallar las multiplicidades algebraica y geométrica de los valores propios. Estudiar en cada caso si es posible formar una base de \mathbb{R}^2 con vectores propios.

Observación 2.6. Calculando valores propios de verdad. Anular el polinomio característico para hallar los valores propios de una matriz $n \times n$ sólo es práctico para $n = 2$, en que hay una fórmula explícita sencilla para encontrar las raíces de un polinomio. Para $n = 3$ y $n = 4$ existen fórmulas análogas pero son mucho más complicadas. Para $n \geq 5$ ya no hay una tal fórmula de validez general, ver la monografía [8]. Tampoco es útil formar el polinomio característico y calcular sus raíces numéricamente, porque el procedimiento es muy inestable. En resumen, en la práctica el método del polinomio característico es útil sólo para matrices muy pequeñas o con muchas raíces evidentes. Aunque en esta monografía lo emplearemos, no queremos dejar la falsa impresión de estar presentando un método útil para lidiar con problemas reales. Sobre esta cuestión nos limitamos a incluir en la página 68 una breve observación sobre el método de las potencias, y a referir al lector a la literatura. Por ejemplo, a [17].

2.2.2 Los círculos de Gerschgorin

Hay situaciones en las que es útil tener una estimación de los valores propios de una matriz, aunque se desconozca su valor exacto.

Definición 2.4. Discos de Gerschgorin. Para una matriz M compleja, cuadrada $n \times n$ con coeficientes m_{ij} , definiremos los n discos de Gerschgorin de M como

$$D_i = \overline{D}(m_{ii}, r_i) = \{z \in \mathbb{C}; |z - m_{ii}| \leq r_i\}, \quad i = 1 \dots, n,$$

donde

$$r_i = \sum_{\substack{j=1 \\ j \neq i}}^n |m_{ij}|$$

es el radio de cada disco, y m_{ii} su centro.

Proposición 2.5. *Si M es una matriz compleja $n \times n$ y λ es un valor propio de M , entonces λ pertenece a alguno de los n discos de Gershgorin asociados con M .*

Demostración. Si X es un vector propio asociado con λ entonces $MX = \lambda X$. La i -ésima componente de esta igualdad implica

$$\sum_{\substack{j=1 \\ j \neq i}}^n m_{ij} x_j = (\lambda - m_{ii}) x_i.$$

Por lo tanto, se satisfacen la n desigualdades

$$(2.15) \quad |\lambda - m_{ii}| |x_i| \leq \sum_{\substack{j=1 \\ j \neq i}}^n |m_{ij}| |x_j|, \quad i = 1, \dots, n.$$

Escojamos el valor de i para el que $|x_i|$ alcanza su valor máximo y la i -ésima de las n desigualdades en (2.15). Dividiendo entre $|x_i|$ resulta

$$|\lambda - m_{ii}| \leq \sum_{\substack{j=1 \\ j \neq i}}^n |m_{ij}|,$$

lo que implica que λ está en el i -ésimo disco de Gershgorin de M . □

Ejemplo 2.10. En la figura 2.2 ilustramos los dos discos de Gerschgorin de la matriz (2.13) que genera la recursión de los números de Fibonacci. También sus dos valores propios.

El teorema de Gerschgorin admite la siguiente generalización.

Teorema 2.6. *Sea M una matriz compleja $n \times n$. Si la unión $\mathcal{R} = \cup_{k=1}^l D_{i_k}$ de l de sus discos de Gerschgorin es disjunta con los restantes $n - l$ discos, entonces l autovalores de M , contados con su multiplicidad algebraica pertenecen a \mathcal{R} .*

Ejercicio 2.14.

1. Estimar los valores propios de

$$M = \begin{bmatrix} 1 & -10^{-5} & 2 \times 10^{-5} \\ 4 \times 10^{-5} & \frac{1}{2} & -3 \times 10^{-5} \\ 10^{-5} & 3 \times 10^{-5} & \frac{1}{10} \end{bmatrix}.$$

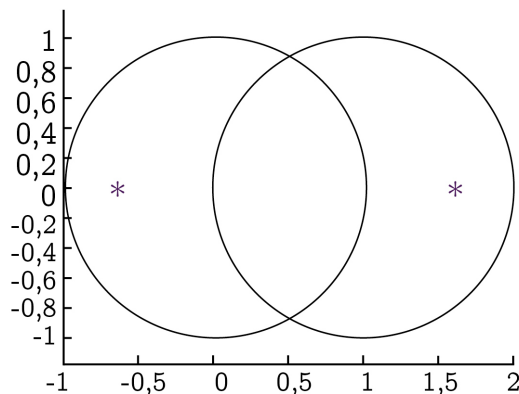


FIGURA 2.2. Discos de Gerschgorin y valores propios de la matriz que genera los números de Fibonacci

2. Para

$$A = \begin{bmatrix} \alpha & & \\ & 1 & \\ & & 1 \end{bmatrix},$$

con α real y no nulo, estimar los valores propios de AMA^{-1} . Usar el resultado para estimar los valores propios de M .

3. Escoger α para mejorar la estimación de uno de los valores propios de M .
4. Utilizar matrices similares a A para mejorar las estimaciones de los otros dos.

2.2.3 Ejercicios adicionales

Ejercicio 2.15. Hallar el polinomio característico, los valores propios y los vectores propios de la matriz

$$M = \begin{bmatrix} 8 & -5 \\ 10 & -7 \end{bmatrix}$$

del ejercicio 2.1, página 44.

Ejercicio 2.16. Para las matrices

$$\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} i & 1+i \\ 1 & 0 \end{bmatrix}$$

encontrar los valores y vectores propios complejos. Observar que la primera matriz no tiene valores ni vectores propios reales, ¿qué transformación representa esta matriz en el plano \mathbb{R}^2 ?

Ejercicio 2.17. Estudiar para qué valores de $\theta \in \mathbb{R}$ la matriz real

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

tiene valores propios reales. Interpretar geoméricamente el resultado.

Ejercicio 2.18. Mostrar que dos matrices semejantes tienen los mismos valores propios. Dar un ejemplo de dos matrices con los mismos valores propios que no sean semejantes. Sugerencia: buscar un ejemplo con matrices 2×2 .

Ejercicio 2.19. M indica una matriz cuadrada.

1. Mostrar que M y M^\top tienen los mismos valores propios, ¿puede afirmarse lo mismo respecto a sus vectores propios?
2. Mostrar que si todas las columnas de M suman 1 entonces 1 es un valor propio de M .
3. Concluir que las matrices de un modelo de Leontief, para una economía cerrada, ver la sección 2.1.2, página 48, y una matriz normalizada de enlaces sobre una red, como (2.9), página 48, tienen a 1 como valor propio.

Ejercicio 2.20. Mostrar que una matriz real M tal que $M^2 = -I$ no puede tener valores propios reales. ¿Puede existir una matriz real 3×3 tal que $M^2 = -I$?, ¿y una 4×4 ?

Ejercicio 2.21. Una matriz M se llama *nilpotente* cuando alguna potencia M^k es la matriz nula. El menor valor de k para el que M^k es nula se llama *orden de nilpotencia*.

1. Mostrar que

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix},$$

son matrices nilpotentes de orden 2, y que

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

es nilpotente de orden 3.

2. Mostrar que una matriz nilpotente tiene a 0 como su único valor propio.

Ejercicio 2.22.

1. Mostrar que si una matriz compleja M satisface las n desigualdades

$$(2.16) \quad \sum_{\substack{j=1 \\ j \neq i}}^n |m_{ij}| < |m_{ii}|, \quad i = 1, \dots, n,$$

entonces es invertible.

2. Enunciar y demostrar un resultado similar para matrices que satisfacen

$$\sum_{\substack{i=1 \\ i \neq j}}^n |m_{ij}| < |m_{jj}|, \quad i = 1, \dots, n.$$

Observación 2.7. Las matrices que satisfacen las desigualdades (2.16) reciben el nombre de *matrices con diagonal estrictamente dominante*.

2.3 Diagonalización

Sea M una matriz real, cuadrada $n \times n$, y supongamos que existe una base

$$\mathcal{A} = (A_1, \dots, A_n)$$

de \mathbb{R}^n formada por vectores propios de M , cada uno de ellos correspondiente a un valor propio λ_i , $i = 1, \dots, n$. Entonces

$$(2.17) \quad MA_i = \lambda_i A_i, \quad i = 1, \dots, n.$$

Si llamamos A a la matriz $[A_1 \ A_2 \ \dots \ A_n]$ cuyas columnas son los vectores en \mathcal{A} , las n igualdades vectoriales (2.17) son equivalentes a la identidad matricial

$$(2.18) \quad MA = AD,$$

donde

$$(2.19) \quad D = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{bmatrix}.$$

Naturalmente, la fórmula (2.18) es equivalente a

$$(2.20) \quad M = ADA^{-1},$$

que es una factorización de M como el producto de matrices de cambio de base y una matriz diagonal. Esta discusión es la demostración de nuestro próximo teorema.

Teorema 2.7. *Sea M una matriz real $n \times n$. Entonces M es semejante a una matriz diagonal si y sólo si existe una base de \mathbb{R}^n formada por vectores propios de M .*

Diremos que matriz semejante a una matriz diagonal es *diagonalizable*, y que *se diagonaliza* en la base formada por sus vectores propios.

Ejercicio 2.23. Generalizar las definiciones necesarias y el Teorema 2.7 para el caso de matrices complejas.

Ejemplo 2.11. La familia

$$\mathcal{A} = ((3, 1), (1, -1))$$

es una base de \mathbb{R}^2 formada por vectores propios de la matriz

$$M = \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix},$$

con valores propios 1 y $1/5$ respectivamente (ver el ejemplo 2.7, página 51). Se satisface entonces

$$(2.21) \quad \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 3 & \\ & 1/5 \end{bmatrix}.$$

Multiplicando a la izquierda por la inversa de la matriz cuyas columnas son la base \mathcal{A} obtenemos la factorización

$$(2.22) \quad \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 1/5 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -3 \end{bmatrix}$$

de M en términos de su forma diagonal.

Ejemplo 2.12. La matriz

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

que genera la sucesión de números de Fibonacci es diagonalizable. Una base que la diagonaliza es

$$\left(\left(1, (1 + \sqrt{5})/2 \right), \left(1, (1 - \sqrt{5})/2 \right) \right).$$

La forma diagonal de M tiene a $\lambda_{\pm} = (1 \pm \sqrt{5})/2$ en su diagonal. La igualdad

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \frac{1+\sqrt{5}}{2} & \\ & \frac{1-\sqrt{5}}{2} \end{bmatrix}$$

es la forma que para este ejemplo toma la igualdad (2.18).

Ejercicio 2.24. Hallar para M una factorización como (2.20).

Ejemplo 2.13. La matriz

$$M = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

es nilpotente y sólo tiene a 0 como valor propio (ver el ejercicio 2.21, página 55). Los vectores propios pertenecen entonces al núcleo de la matriz, que tiene dimensión 1 y está generado por $(0, 1)$. No hay entonces una base de \mathbb{R}^2 formada por vectores propios de M .

Ejemplo 2.14. Vimos en el ejemplo 2.8, página 51, que la matriz

$$(2.23) \quad M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

no tiene vectores propios reales, por lo que no es diagonalizable sobre \mathbb{R} . Pero es diagonalizable sobre \mathbb{C} . Por ejemplo en la base $((1, i), (1, -i))$ de \mathbb{C}^2 . Por lo tanto, la matriz M puede factorizarse como

$$(2.24) \quad M = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix} \begin{bmatrix} i & \\ & -i \end{bmatrix} \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}.$$

Ejercicio 2.25. Completar los detalles del cálculo que conduce a (2.24).

2.3.1 Diagonalización y potencias de matrices

Las potencias de una matriz M tienen interés en diversas situaciones. Un ejemplo relevante son las ecuaciones recursivas como

$$(2.25) \quad X_{k+1} = MX_k, \quad k \in \mathbb{N}$$

donde M es una matriz $n \times n$. Si el estado inicial X_0 es conocido entonces

$$(2.26) \quad X_k = M^k X_0, \quad k \in \mathbb{N},$$

por lo que las potencias M^k determinan el comportamiento de la sucesión X_k definida por (2.25).

Ejercicio 2.26. Mostrar que si una sucesión de vectores satisface (2.25) para $k = 0, 1, \dots$, es necesariamente de la forma (2.26).

Observación 2.8. Ecuaciones como (2.25) modelan diversos fenómenos de evolución. Cuando en la sección 1.1 estudiamos los números de Fibonacci lo hicimos a través de la recurrencia $F_{n+1} = MF_n$ (fórmula (1.4), página 24), que iba generando parejas de números. Aparecerán también en el capítulo 5 en el contexto de las cadenas de Markov. El lector interesado puede encontrar más detalles en [5].

En general, el cálculo de las potencias M^k de una matriz cualquiera M es inabordable directamente. Pero si se trata de una matriz diagonal

$$D = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix},$$

entonces

$$(2.27) \quad D^k = \begin{bmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{bmatrix}, \quad k = 0, 1, 2, \dots$$

Cuando M es semejante a una matriz diagonal, tenemos que

$$M = ADA^{-1},$$

con D diagonal. Formando el cuadrado resulta

$$M^2 = ADA^{-1}ADA^{-1} = AD^2A^{-1}.$$

La fórmula se generaliza inductivamente a

$$(2.28) \quad M^k = AD^kA^{-1}, \quad k = 0, 1, 2, \dots,$$

válida para cualquier potencia natural.

Ejemplo 2.15. Las potencias M^n de la matriz

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

que genera los números de Fibonacci son

$$M^n = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix} \begin{bmatrix} \left(\frac{1+\sqrt{5}}{2}\right)^n & \\ & \left(\frac{1-\sqrt{5}}{2}\right)^n \end{bmatrix} \begin{bmatrix} -\frac{1-\sqrt{5}}{2} & 1 \\ \frac{1+\sqrt{5}}{2} & -1 \end{bmatrix}.$$

De esta expresión pueden obtenerse fórmulas explícitas para los números de Fibonacci (comparar con (1.16), página 27).

Ejercicio 2.27. Investigar qué ocurre cuando la recurrencia $f_{n+1} = f_n + f_{n-1}$ se inicializa con números f_0 y f_1 cualesquiera.

Ejercicio 2.28. Calcular las potencias de las matrices

$$\begin{bmatrix} 8 & -5 \\ 10 & -7 \end{bmatrix}, \quad \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix},$$

que ya han aparecido en los ejercicios 2.1, y 2.13.

La diagonalización sobre \mathbb{C} puede usarse para el cálculo de potencias de matrices reales.

Ejercicio 2.29. Calcular las potencias de la matriz

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

1. Explorando algunas potencias y usando un argumento inductivo;
2. diagonalizándola sobre \mathbb{C} (fórmula (2.24)).

Ejercicio 2.30. Consideremos una matriz real

$$(2.29) \quad J = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

1. Mostrar que si $b \neq 0$ entonces J no es diagonalizable sobre \mathbb{R} , $a \pm ib$ son valores propios de J y hallar una base de \mathbb{C}^2 que diagonalice J ;
2. Existen $\rho \geq 0$ y $\theta \in [0, 2\pi)$ tales que el número complejo $a + ib$ puede representarse en la forma

$$(2.30) \quad a + ib = \rho e^{i\theta} = \rho(\cos \theta + i \operatorname{sen} \theta).$$

Usar la diagonalización de J sobre \mathbb{C} para mostrar que

$$(2.31) \quad \begin{bmatrix} a & -b \\ b & a \end{bmatrix}^k = \rho^k \begin{bmatrix} \cos(k\theta) & -\operatorname{sen}(k\theta) \\ \operatorname{sen}(k\theta) & \cos(k\theta) \end{bmatrix}, \quad k = 0, 1, 2, \dots$$

3. Observar que

$$J = \rho \begin{bmatrix} \cos \theta & -\operatorname{sen} \theta \\ \operatorname{sen} \theta & \cos \theta \end{bmatrix},$$

e interpretar geoméricamente J y la parte 2.

4. Aplicar estos resultados a las matrices

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

Observación 2.9. La diagonalización permite tratar también fenómenos de evolución gobernados por ecuaciones diferenciales. Por razones de espacio no abordamos este tema, sumamente importante e interesante. Pero invitamos al lector a consultar la abundante literatura disponible, como la monografía [5], o las referencias [9, 14, 16]. En estas páginas nos limitaremos a introducir la exponencial de una matriz en los ejercicios de la sección 2.4.5, página 75.

2.3.2 Forma canónica de Jordan

Algunas matrices no son diagonalizables porque sus vectores propios no alcanzan para formar una base del espacio, pero son semejantes a una matriz casi diagonal, la forma canónica de Jordan. En esta sección ilustramos algunos aspectos de esta teoría, que no desarrollaremos en profundidad.

Ejercicio 2.31. Mostrar que para cualquier valor de $\lambda \in \mathbb{R}$ la matriz real

$$(2.32) \quad J = \begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix}$$

no es diagonalizable.

Ejercicio 2.32. Consideremos la matriz:

$$M = \begin{bmatrix} 4 & -3 \\ 3 & -2 \end{bmatrix},$$

con la que ya habíamos trabajado en el ejercicio 2.13, página 52.

1. Si X no es un vector propio de M , mostrar que $(M - I)X$ sí lo es.
2. Hallar una base \mathcal{A} de \mathbb{R}^2 tal que la representación de M en \mathcal{A} sea (2.32) con $\lambda = 1$.

Ejercicio 2.33. Mostrar que si M es una matriz 2×2 que tiene un único valor propio real λ tal que $\dim \ker(M - \lambda I) = 1$, entonces M es semejante a una matriz de la forma (2.32). Sugerencia: usar que la imagen de $M - \lambda I$ es un subespacio de dimensión 1 invariante para M y el ejercicio 2.4, página 45.

El ejercicio 2.33 generaliza al 2.32. Ambos ilustran casos particulares de la siguiente proposición.

Proposición 2.8. Forma canónica de Jordan. Sea M una matriz compleja $n \times n$ y λ_i , $i = 1, \dots, k$ sus valores propios². Entonces M es semejante a una matriz diagonal por bloques

$$J = \begin{bmatrix} \Lambda_1 & & \\ & \ddots & \\ & & \Lambda_k \end{bmatrix},$$

donde a su vez cada bloque Λ_i es diagonal por bloques

$$\Lambda_i = \begin{bmatrix} \Lambda_i^1 & & \\ & \ddots & \\ & & \Lambda_i^l \end{bmatrix},$$

con $l = \dim \ker(M - \lambda_i I)$ y cada bloque Λ_i^m , $m = 1, 2, \dots, l$ es de la forma

$$\begin{bmatrix} \lambda_i & & & & \\ 1 & \lambda_i & & & \\ & 1 & \lambda_i & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda_i \end{bmatrix},$$

Ejemplo 2.16. Ejemplos de formas canónicas de Jordan son

$$\begin{bmatrix} 3 & & & \\ 1 & 3 & & \\ & & 3 & \\ & & 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} \pi & & & & \\ 1 & \pi & & & \\ & 1 & \pi & & \\ & & \sqrt{2} & \sqrt{2} & \\ & & 1 & \sqrt{2} \end{bmatrix}.$$

La primera corresponde a una matriz M con un único valor propio 3, y tal que $\ker(M - 3I) = 2$. La segunda a una matriz M con valores propios π y $\sqrt{2}$, y tal que $\dim(\ker(M - \pi I)) = 1$, $\dim(\ker(M - \sqrt{2}I)) = 1$.

Observación 2.10. El teorema de la forma canónica de Jordan se enuncia para matrices complejas, porque es necesario que todas las raíces del polinomio característico de M estén en el cuerpo sobre el que se trabaja para tener una forma canónica de ese tipo. Si una matriz real es tal que su polinomio característico no tiene raíces complejas entonces admite una forma canónica de Jordan como (2.3.2), donde los valores propios reales λ_i aparecen en la diagonal de J . La teoría puede extenderse al caso de matrices reales con valores propios complejos, pero no discutiremos esa posibilidad.

Nota Histórica 2.4. La forma canónica de Jordan fue introducida por Camille Jordan en un tratado publicado en 1870.

²Aquí $\lambda_i \neq \lambda_j$ si $i \neq j$. Cada valor propio de M aparece una vez, independientemente de su multiplicidad.

La forma canónica de Jordan da una buena comprensión de la estructura de una matriz cualquiera, y en muchos casos permite, con algo de esfuerzo adicional, generalizar resultados que para matrices diagonalizables son fáciles de obtener.

Ejercicio 2.34.

1. Mostrar que si dos matrices cuadradas M y N conmutan entonces

$$(M + N)^k = \sum_{i=0}^k \binom{k}{i} M^i N^{k-i}.$$

2. Considerar la matriz

$$M = \begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix} = \begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

y calcular M^k usando el resultado de la parte 1.

3. Para la matriz

$$M = \begin{bmatrix} 4 & -3 \\ 3 & -2 \end{bmatrix},$$

calcular M^{10} . Sugerencia: usar los resultados de las partes anteriores y del ejercicio 2.32.

2.3.3 Forma real de matrices con valores propios complejos

Comencemos con un ejemplo, que iremos retomando a lo largo de la sección.

Ejemplo 2.17. La matriz real

$$M = \begin{bmatrix} 0 & -4 \\ 1 & 2\sqrt{3} \end{bmatrix}$$

tiene valores propios $\sqrt{3} \mp i$, con vectores propios generados por $(\sqrt{3} \pm i, -1)$, respectivamente. Tal vez el lector ya lo sepa, por haber resuelto completa y cuidadosamente el ejercicio 2.12, página 52. De todos modos, presentamos los detalles más importantes del cálculo.

El polinomio característico de M es

$$P(\lambda) = \lambda^2 - 2\sqrt{3}\lambda + 4$$

con raíces $\sqrt{3} \mp i$. Cuando buscamos el núcleo de $M - \lambda I$ para $\lambda = \sqrt{3} - i$ debemos plantear para ese valor de λ el sistema $(M - \lambda I)X = 0$. Resulta

$$M = \left[\begin{array}{cc|c} -\sqrt{3} + i & -4 & 0 \\ 1 & \sqrt{3} + i & 0 \end{array} \right],$$

cuyas soluciones son de la forma $z(\sqrt{3} + i, -1)$, con $z \in \mathbb{C}$.

Ejercicio 2.35. Mostrar que para $\lambda = \sqrt{3} + i$ el núcleo $M - \lambda I$ está generado por $z(\sqrt{3} - i, -1)$.

Dado un vector complejo Z es posible definir su *parte real* $\Re(Z)$, su *parte imaginaria* $\Im(Z)$, y su *vector conjugado* \bar{Z} tomando partes real, imaginaria y conjugados coeficiente a coeficiente.

Ejemplo 2.18. Si $Z = (\sqrt{3} + i, -1)$ entonces

$$\Re(Z) = (\sqrt{3}, -1), \quad \Im(Z) = (1, 0), \quad \bar{Z} = (\sqrt{3} - i, -1).$$

Ejercicio 2.36. Hallar las partes real e imaginaria y el conjugado de $(\sqrt{3} - i, -1)$

Los vectores $\Re(Z)$ e $\Im(Z)$ son vectores reales tales que

$$(2.33) \quad Z = \Re(Z) + i\Im(Z), \quad \bar{Z} = \Re(Z) - i\Im(Z).$$

Ejercicio 2.37. Para $Z \in \mathbb{C}^n$ mostrar que

$$(2.34) \quad \Re(Z) = (Z + \bar{Z})/2, \quad \Im(Z) = (Z - \bar{Z})/(2i).$$

En el ejemplo 2.17 encontramos que la matriz real M tiene valores propios conjugados, con vectores propios conjugados. Esto es un hecho general.

Proposición 2.9. Sea M una matriz real que tiene un valor propio complejo $\lambda = a + ib$ con parte imaginaria no nula. Entonces

1. $\bar{\lambda}$ también es un valor propio de M ;
2. Z es un vector propio asociado a λ si y sólo si \bar{Z} es un vector propio asociado a $\bar{\lambda}$;
3. $(\Re(Z), \Im(Z))$ es linealmente independiente
4. El subespacio generado por $(\Re(Z), \Im(Z))$ es invariante para M , y

$$(2.35) \quad \begin{aligned} M\Re(Z) &= a\Re(Z) + b\Im(Z), \\ M\Im(Z) &= -b\Re(Z) + a\Im(Z). \end{aligned}$$

Demostración. Indicaremos como probar la primera igualdad en (2.35). Calculamos

$$M\Re(Z) = M \left(\frac{Z + \bar{Z}}{2} \right) = \frac{MZ + M\bar{Z}}{2} = \frac{\lambda Z + \bar{\lambda}\bar{Z}}{2}.$$

Escribiendo $\lambda = a + ib$, Z y \bar{Z} como en (2.33) y haciendo las cuentas se completa esta parte. La invariancia del subespacio generado por $(\Re(Z), \Im(Z))$ es una consecuencia directa de (2.35). El resto de la prueba requiere cálculos similares.

Ejercicio 2.38. Completar la demostración. □

Ejemplo 2.19. Volviendo a la matriz del ejemplo 2.17 encontramos

$$(2.36) \quad \begin{aligned} M \begin{bmatrix} \sqrt{3} \\ -1 \end{bmatrix} &= \begin{bmatrix} 4 \\ -\sqrt{3} \end{bmatrix} = \sqrt{3} \begin{bmatrix} \sqrt{3} \\ -1 \end{bmatrix} + 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \\ M \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} = (-1) \begin{bmatrix} \sqrt{3} \\ -1 \end{bmatrix} + \sqrt{3} \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \end{aligned}$$

en correspondencia con (2.35).

La proposición 2.9 tiene el siguiente corolario.

Corolario 2.10. Si $\lambda = a - ib$, con $b \neq 0$, es un valor propio de una matriz M real 2×2 y $Z \in \mathbb{C}^2$ es un vector propio asociado a λ , entonces $(\Re(Z), \Im(Z))$ es una base de \mathbb{R}^2 en la que la matriz M se representa por

$$(2.37) \quad \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Llamaremos a la matriz (2.37) la *forma canónica real* de M .

Observación 2.11. Notar el signo de la parte imaginaria de λ y de la segunda entrada en la primera fila de (2.37). Si λ se escribe en la forma usual $a + ib$ los signos quedan cambiados.

Ejemplo 2.20. Las fórmulas (2.36) son equivalentes a la igualdad matricial

$$\begin{bmatrix} 0 & -4 \\ 1 & 2\sqrt{3} \end{bmatrix} \begin{bmatrix} \sqrt{3} & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} \sqrt{3} & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{bmatrix},$$

que todavía puede transformarse en la factorización

$$\begin{bmatrix} 0 & -4 \\ 1 & 2\sqrt{3} \end{bmatrix} = \begin{bmatrix} \sqrt{3} & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}$$

que hace evidente la semejanza entre M y su forma canónica real. Usando que

$$\sqrt{3} + i = 2(\cos(\pi/6) + \operatorname{sen}(\pi/6))$$

y haciendo uso de la fórmula (2.31) encontramos

$$\begin{bmatrix} 0 & -4 \\ 1 & 2\sqrt{3} \end{bmatrix}^k = 2^k \begin{bmatrix} \sqrt{3} & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} \cos(k\pi/6) & -\operatorname{sen}(k\pi/6) \\ \operatorname{sen}(k\pi/6) & \cos(k\pi/6) \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \sqrt{3} \end{bmatrix}.$$

Ejercicio 2.39. Hallar una expresión explícita y sencilla para M^{19} .

Ejercicio 2.40. Hallar de dos maneras las potencias de $\begin{bmatrix} 1 & -4 \\ 1 & 1 \end{bmatrix}$:

1. diagonalizándola sobre \mathbb{C} ;
2. usando la forma canónica real (2.37).

Ejercicio 2.41. Demostrar el corolario 2.10. ¿Qué implica la proposición 2.9 para matrices reales $n \times n$ con $n = 3$? ¿Qué puede decirse para valores mayores de n ? Aplicar los resultados a la matriz

$$(2.38) \quad M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Estudiar las potencias de M directamente y usando las técnicas de esta sección.

2.3.4 Ejercicios adicionales

Ejercicio 2.42. Sean (λ_i, v_i) , $i = 1, \dots, k$, parejas de valores y vectores propios de una matriz M . Asumamos que todos los números λ_i son diferentes. Mostrar que la familia formada por los vectores v_i es linealmente independiente. Sugerencia: formar una combinación lineal de los v_i y aplicarle $T - \lambda_i I$ de manera conveniente.

Ejercicio 2.43. Mostrar que si una matriz $n \times n$ real (compleja) tiene n valores propios reales (complejos) diferentes entonces se diagonaliza sobre \mathbb{R} (\mathbb{C}).

Ejercicio 2.44. Mostrar que toda matriz real simétrica 2×2 se diagonaliza sobre \mathbb{R} .

Ejercicio 2.45. Demostrar la siguiente proposición:

Proposición 2.11. *Si M es una matriz compleja $n \times n$ tal que sus n discos de Gerschgorin son disjuntos, entonces se diagonaliza sobre \mathbb{C} . Si M es una matriz real $n \times n$ tal que sus n discos de Gerschgorin son disjuntos, entonces se diagonaliza sobre \mathbb{R} .*

Sugerencia: usar los resultados de los ejercicios 2.9 y 2.42, y el teorema 2.6.

Ejercicio 2.46. Mostrar que la matriz

$$\begin{bmatrix} 10 & 6 & -2 \\ 1 & -4 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

es diagonalizable e invertible, y hallar el signo de sus valores propios.

Ejercicio 2.47. Investigar el comportamiento de los números generados por la recurrencia

$$n_{k+1} = \frac{n_k + n_{k-1}}{2}, \quad k = 1, 2, \dots$$

Ejercicio 2.48. Mostrar que si M es diagonalizable e invertible la fórmula (2.28) es válida para cualquier valor entero de k .

Ejercicio 2.49. Mostrar que si M satisface $M^2 = M$ ó $M^2 = I$ es una matriz diagonalizable, ¿qué puede decir sobre la forma diagonal de M ?, ¿qué transformaciones del espacio representan estas matrices?

2.4 Radio espectral y potencias de una matriz

Estudiaremos el comportamiento de las potencias M^k de una matriz cuadrada cuando $k \rightarrow \infty$. Los requisitos previos sobre convergencia de sucesiones de matrices y vectores necesarios para esta sección se recogen en la sección sección 1.3.

El caso más fácil de analizar es el de cualquier matriz diagonal

$$D = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}.$$

Como

$$D^k = \begin{bmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{bmatrix}, \quad k = 0, 1, 2, \dots,$$

entonces

- si todas los λ_i tienen módulo menor que 1 las potencias D^k convergen a la matriz O cuando $k \rightarrow \infty$;
- si los módulos de los coeficientes en la diagonal son menores o iguales que 1 pero algún λ_i tiene módulo 1, las potencias D^k ya no convergen a O , pero sus coeficientes se mantienen acotados;
- si hay alguna λ_i con módulo mayor que 1 los coeficientes de las potencias ya no se mantienen acotadas.

Si M es semejante a una matriz diagonal y todos sus valores propios tienen módulo menor que 1 entonces también sus potencias tienden a la matriz nula, porque

$$M^k = AD^kA^{-1} \rightarrow AOA^{-1} = O.$$

Definición 2.12. Llamamos *radio espectral* $r(M)$ de una matriz $n \times n$ real o compleja M , al máximo del módulo de los valores propios de M .

Ejercicio 2.50. Mostrar que $r(aM) = |a|r(M)$. Investigar si es cierto o falso que $r(M + N) \leq r(M) + r(N)$.

Los resultados para matrices diagonalizables se generalizan parcialmente a matrices cualesquiera.

Proposición 2.13. Sea M una matriz real o compleja $n \times n$.

1. Si $r(M) < 1$, entonces $M^k \rightarrow O$;
2. si $r(M) = 1$ entonces existe una constante $c > 0$ tal que $\|M^k\|_* \geq c$ para todo k . Si además M es diagonalizable sobre \mathbb{R} o \mathbb{C} entonces existe $C > 0$ tal que $\|M^k\|_* \leq C$ para todo k ;
3. si $r(M) > 1$, entonces $\|M^k\|_* \rightarrow \infty$.

Corolario 2.14. Si M es una matriz cuadrada real o compleja, entonces $M^k \rightarrow O$ si y sólo si $r(M) < 1$.

Estudiaremos las potencias de tres matrices de radio espectral igual a 1.

Ejemplo 2.21. El primer caso es

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}.$$

Vemos que hay una entrada de las potencias que tiende a infinito.

Ejemplo 2.22. Al estudiar

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}^k = \begin{bmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{bmatrix};$$

encontramos que las potencias muestran un comportamiento oscilatorio.

Ejemplo 2.23. La factorización

$$M = \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{5} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -3 \end{bmatrix}$$

apareció en la fórmula (2.22), página 57. Implica

$$M^k = \begin{bmatrix} 3 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 5^{-k} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -3 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 3+5^{-k} & 3-3 \times 5^{-k} \\ 1-5^{-k} & 1+3 \times 5^{-k} \end{bmatrix}.$$

Concluimos que las potencias de M se aproximan a la matriz límite

$$(2.39) \quad \frac{1}{4} \begin{bmatrix} 3 & 3 \\ 1 & 1 \end{bmatrix}.$$

Ejercicio 2.51. Mostrar que la matriz (2.39) es igual al producto de las matrices de cambio de base que diagonalizan M por el límite de la forma diagonal de M , ¿el producto puede formarse en cualquier orden?

Ejercicio 2.52. Completar los detalles del ejemplo 2.21 y observar el distinto comportamiento de las potencias de las matrices en los ejemplos 2.21, 2.22 y 2.23.

2.4.1 Valor propio dominante

El comportamiento de las potencias de M está esencialmente determinado por sus valores propios con mayor módulo.

Proposición 2.15. Si los valores propios λ_i , $i = 1, \dots, k$, de una matriz M satisfacen las desigualdades

$$|\lambda_1| > |\lambda_2| \geq |\lambda_3| \geq \dots |\lambda_k|$$

y $\dim(\ker(M - \lambda_1)) = 1$, entonces para cualquier vector X existe un vector

$$X_* \in \ker(M - \lambda_1)$$

tal que

$$\lambda_1^{-k} M^k X \rightarrow X_*$$

Demostración. (para M diagonalizable). Cuando M es diagonalizable cada vector X admite una expresión³

$$X = \alpha_1 X_1 + \alpha_2 X_2 + \dots \alpha_n X_n,$$

donde cada vector X_i , $i = 1, \dots, n$, es un vector propio con valor propio λ_i . Entonces

$$M^k X = \alpha_1 \lambda_1^k X_1 + \alpha_2 \lambda_2^k X_2 + \dots \alpha_n \lambda_n^k X_n.$$

³En esta fórmula cada valor propio aparece tantas veces como su multiplicidad.

Dividiendo entre λ_1^k resulta

$$\frac{1}{\lambda_1^k} M^k X = \alpha_1 X_1 + \alpha_2 \left(\frac{\lambda_2}{\lambda_1} \right)^k X_2 + \dots + \alpha_d \left(\frac{\lambda_d}{\lambda_1} \right)^k X_d \rightarrow \alpha_1 X_1,$$

porque todos los cocientes de valores propios decaen exponencialmente a cero. \square

Ejercicio 2.53. ¿Qué ocurre con las columnas de M^k cuando M tiene un valor propio dominante?, ¿tienden todas al mismo límite?, ¿qué resultado asintótico puede enunciarse?

Ejercicio 2.54. Deducir de la proposición 2.15 la fórmula asintótica (1.15), página 27, que apareció en la discusión de los números de Fibonacci.

Ejercicio 2.55. Mostrar que la convergencia de las potencias en el ejemplo 2.23 puede explicarse porque 1 es el valor propio dominante de la matriz cuyas potencias aparecen en el cálculo.

Observación 2.12. Método de las potencias. Dado que las potencias de una matriz tienden a magnificar el valor propio dominante cuando este existe, calcular las potencias es una técnica para identificarlo y hallar un vector propio asociado. El siguiente ejercicio requiere utilizar una calculadora o computadora para realizar los cálculos.

Ejercicio 2.56. Para las matrices

$$C = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}, \quad N = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{bmatrix}$$

calcular recursivamente una sucesión de vectores $X_{k+1} = CX_k$, tomando como X_0 los vectores de la base canónica de \mathbb{R}^3 . Cada vez que X_k se haga demasiado grande dividirlo por la suma de sus entradas. Comprobar que el procedimiento tiende a estabilizarse, y usarlo para identificar para cada matriz el valor propio dominante λ_1 y un vector propio asociado con λ_1 . Comparar los resultados con los ejemplos 2.4 y 2.5 de la sección 2.1 (páginas 47 y 48).

2.4.2 Método iterativo de Jacobi

Si A es una matriz cuadrada e invertible el sistema $AX = Y$ tiene una única solución X . Si escribimos

$$A = D + C,$$

donde D es una matriz diagonal que contiene los coeficientes de la diagonal de A , y C una matriz con ceros en la diagonal, entonces

$$(D + C)X = Y.$$

Si ningún coeficiente de la diagonal de A es nulo podemos escribir

$$X = D^{-1}(Y - CX) = D^{-1}Y - D^{-1}CX.$$

Llamando

$$Z = D^{-1}Y, \quad M = -D^{-1}C$$

encontramos que X satisface la igualdad vectorial

$$(2.40) \quad X = MX + Z.$$

Ejemplo 2.24. El sistema

$$(2.41) \quad \begin{bmatrix} 4 & 1 \\ -1 & 3 \end{bmatrix} X = \begin{bmatrix} 6 \\ 5 \end{bmatrix}$$

tiene $X = [1, 2]$ como su única solución. En este caso las matrices D y C son

$$D = \begin{bmatrix} 4 & \\ & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

por lo tanto

$$M = -D^{-1}C = \begin{bmatrix} 0 & -\frac{1}{4} \\ \frac{1}{3} & 0 \end{bmatrix}, \quad Z = D^{-1}Y = \begin{bmatrix} \frac{3}{2} \\ \frac{5}{3} \end{bmatrix}.$$

Un cálculo directo muestra que la solución X satisface (2.40).

El interés de transformar el sistema $AX = Y$ en la ecuación (2.40) es que su solución aparece como un punto fijo para la transformación

$$X \mapsto MX + Z.$$

Esto es la base para un procedimiento, conocido como *método iterativo de Jacobi*, que busca aproximarse a la solución:

1. en el primer paso damos un primer valor tentativo a la solución, al que llamaremos X_0 ;
2. a partir de cada aproximación X_k construimos

$$(2.42) \quad X_{k+1} = MX_k + Z.$$

Ahora bien, ¿convergerá a X nuestra sucesión X_k ? La clave para contestar esta pregunta es estudiar la evolución de los errores

$$E_k = X_k - X$$

que se producen en cada paso de la iteración. Encontramos

$$E_{k+1} = X_{k+1} - X = MX_k - MX = M(X_k - X) = ME_k,$$

una fórmula iterativa con matriz M ! Por lo tanto el error E_k es igual a $M^k E_0$ y su comportamiento asintótico depende esencialmente del radio espectral de M .

Ejemplo 2.25. La iteración de Jacobi para el sistema (2.41) del ejemplo 2.24 es

$$X_{k+1} = \begin{bmatrix} 0 & -1/4 \\ 1/3 & 0 \end{bmatrix} X_k + \begin{bmatrix} 3/2 \\ 5/3 \end{bmatrix}.$$

Comenzando desde $X_0 = O$ se genera, aproximadamente, la sucesión

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1,50 \\ 1,67 \end{bmatrix}, \begin{bmatrix} 1,0833 \\ 2,1667 \end{bmatrix}, \begin{bmatrix} 0,9583 \\ 2,0278 \end{bmatrix}, \begin{bmatrix} 0,9931 \\ 1,9861 \end{bmatrix}, \begin{bmatrix} 1,0035 \\ 1,9977 \end{bmatrix}, \begin{bmatrix} 1,0006 \\ 2,0012 \end{bmatrix} \cdots$$

que converge rápidamente a la solución. El radio espectral de la matriz de la iteración es $1/\sqrt{12}$.

Ejercicio 2.57. Observar cómo se va aproximando X_k a la solución (1, 2). Si es necesario calcular más aproximaciones y/o hacer un dibujo, tal vez recurriendo a una computadora, ¿puede explicar el patrón que se observa?

Al igual que en el ejemplo, la matriz M del método de Jacobi siempre tiene ceros en su diagonal. Si llamamos a_{ij} a los coeficientes de la matriz A del sistema, entonces los radios r_i de los discos de Gerschgorin de M son

$$r_i = |a_{ii}|^{-1} \sum_{\substack{j=1 \\ j \neq i}}^n |a_{ij}|, \quad i = 1, \dots, n.$$

Cuando A es estrictamente diagonal dominante (ver la observación 2.7, página 56) todos los radios r_i son menores que 1. La proposición 2.5, página 53, implica que $r(M) < 1$, y la proposición 2.13 que $E_k \rightarrow O$. Por lo tanto, la sucesión X_k del método de Jacobi converge a la solución.

Ejercicio 2.58. Resolver aproximadamente usando el método de Jacobi el sistema $AX = Y$, para

$$A = \begin{bmatrix} 4 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 10 & 1 \\ -1 & 0 & 0 & 2 \end{bmatrix} \quad Y = \begin{bmatrix} 6 \\ -2 \\ 1 \\ -1 \end{bmatrix}.$$

El método de Jacobi es un primer ejemplo de *método iterativo*. para la resolución de sistemas lineales, pero hay muchas otras posibilidades. El lector interesado puede encontrar, por ejemplo, información sobre el método de Gauss-Seidel en [9, 14], y sobre métodos de sobrerrelajación en [14].

Ejercicio 2.59. Buscar información sobre métodos iterativos y métodos directos para resolver sistemas lineales, la comparación entre ambos, y su uso en problemas prácticos.

Sobre la aproximación a puntos fijos usando métodos iterativos el lector puede consultar la sección C.1, o las monografías [5, 15].

2.4.3 Una serie de potencias para $(I - M)^{-1}$

La célebre fórmula

$$\frac{1}{1-q} = \sum_{k=0}^{\infty} q^k$$

para la serie geométrica puede extenderse al caso matricial. Para una matriz cuadrada M y para $K \in \mathbb{N}$ vale la identidad

$$(2.43) \quad I - M^{K+1} = (I - M) \sum_{k=0}^K M^k.$$

Ejercicio 2.60. Demostrar la validez de (2.43).

Si $r(M) < 1$ entonces $M^{K+1} \rightarrow O$. Además, existe

$$\lim_{K \rightarrow \infty} \sum_{k=0}^K M^k = \sum_{k=0}^{\infty} M^k,$$

resultado que aceptaremos sin demostración. Por lo tanto, pasando al límite en (2.43) concluimos

$$I = (I - M) \sum_{k=0}^{\infty} M^k.$$

Este razonamiento justifica la siguiente proposición.

Proposición 2.16. *Si $r(M) < 1$ entonces*

$$(2.44) \quad (I - M)^{-1} = \sum_{k=0}^{\infty} M^k.$$

Ejemplo 2.26. La matriz

$$M = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

tiene a 0 como su único valor propio. Por lo tanto $r(M) = 0$. La matriz

$$I - M = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

tiene inversa

$$(I - M)^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \sum_{k=0}^{\infty} M^k.$$

Para este caso tan particular, en que M^k es nula para $k \geq 2$, hemos verificado la fórmula (2.44).

Ejercicio 2.61. Calcular $r(M)$ y la inversa de $I - M$ para

$$M = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Verificar la fórmula (2.44).

Ejercicio 2.62. Para matrices M diagonalizables con $r(M) < 1$ mostrar directamente la fórmula (2.44) calculando sus dos miembros a partir de la expresión $M = ADA^{-1}$, con D diagonal.

Ejemplo 2.27. Modelo de Leontief para una economía abierta. En este modelo los sectores de una economía no consumen todo lo que producen, y deben atender una demanda externa. Supondremos conocidos los precios de lo producido por cada sector, que se expresarán en alguna unidad monetaria, como peso, dólar o euro. Las relaciones entre los diferentes sectores pueden esquematizarse en una tabla, en la que la entrada de la fila i y la columna j representa el precio de los bienes del sector i que el sector j consume para producir una unidad de valor de sus productos. Por ejemplo, para los sectores de **transporte**, **alimentación**, **extracción** de recursos naturales y **fabricación** de útiles y herramientas la tabla podría ser

	tr	al	ex	fa
tr	0.2	0.1	0.2	0.2
al	0.1	0.1	0.1	0.1
ex	0.0	0.4	0.0	0.4
fa	0.5	0.3	0.5	0.2

FIGURA 2.3. Matriz de consumo para una economía

A la matriz C formada por las entradas de tal tabla, la llamaremos *matriz de consumo* de la economía. Los volúmenes de producción, medidos en la unidad monetaria, forman un vector $X \in \mathbb{R}^n$ con coeficientes mayores o iguales que cero. En lo sucesivo indicaremos con la notación $C \geq O$, o $X \geq O$, cuando una matriz C o vector X tienen todas sus entradas mayores o iguales que cero (en la siguiente sección extenderemos un poco más esta notación).

Ejercicio 2.63.

1. Si $M \geq O$ es $m \times n$ y $X \geq O$ un vector de \mathbb{R}^n , mostrar que $MX \geq O$.
2. Si $M \geq O$ y $N \geq O$ son matrices que pueden multiplicarse entonces $MN \geq O$.
3. Si $M \geq O$ y $N \geq O$ pueden sumarse entonces $M + N \geq O$.
4. Si una sucesión de matrices $M_k \geq O$ converge a una matriz M , entonces $M \geq O$.

El producto CX representa la parte de X consumida por la propia producción, y $X - CX$ el excedente. Este excedente permite atender demandas externas, que

representaremos por medio de un vector $D \geq O$. La economía puede satisfacer una demanda dada $D \geq O$ si la ecuación

$$(2.45) \quad X - CX = D$$

tiene una solución $X \geq O$. ¡La condición de no negatividad es esencial para que X pueda representar un vector de producción!

Proposición 2.17. *Sea $C \geq O$ la matriz de consumo de una economía. Si $r(C) < 1$ entonces se puede satisfacer cualquier vector de demanda $D \geq O$.*

Demostración. Si $r(C) < 1$ la inversa de $I - C$ existe y puede escribirse como una serie de potencias de C según la fórmula (2.44). Como $C \geq O$ el ejercicio 2.63 implica $(I - C)^{-1} \geq O$. Como $D \geq O$ entonces

$$X = (I - C)^{-1}D \geq O$$

resuelve (2.45) y representa un nivel de producción de la economía que satisface la demanda D . \square

Ejercicio 2.64. Mostrar que si todas las filas o todas las columnas de una matriz cuadrada C con entradas no negativas suman menos que 1 entonces existe $(I - C)^{-1}$ y tiene entradas no negativas. Interpretar en términos del modelo económico del ejemplo (2.27) el significado de que las columnas de C sumen menos que 1.

Ejercicio 2.65. Calcular la inversa de $I - C$ para la matriz C formada por las entradas de la tabla 2.3, y verificar que tiene coeficientes no negativos.

2.4.4 Matrices con coeficientes positivos

En esta sección usaremos las siguientes notaciones:

- si M es una matriz o vector entonces $|M|$ es la matriz⁴ o vector formado por los módulos de los coeficientes de M ;
- si todos los coeficientes de una matriz o vector M son mayores (mayores o iguales) que todos los respectivos coeficientes de N lo indicaremos con $M > N$ ($M \geq N$). Por ejemplo $|M| \geq O$.

Proposición 2.18. *Sea $M > O$ una matriz cuadrada. Entonces su radio espectral $r(M)$ es un valor propio de M y tiene asociado un vector propio $X > O$.*

Necesitaremos algunos resultados sobre matrices y vectores positivos y no negativos, que dejamos como ejercicio para el lector.

Ejercicio 2.66. M denota matrices reales o complejas, X e Y vectores reales o complejos, y α números reales o complejos.

1. Demostrar que $|\alpha X| = |\alpha||X|$ y que $|MX| \leq |M||X|$.
2. Demostrar que si $M > O$ y $X \geq O$ no es nulo entonces $MX > O$.

⁴Para M cuadrada, ¡no confundir $|M|$ con el determinante de M !

3. Demostrar que si $X > O$ e $Y \geq O$ existe $\epsilon > 0$ tal que $X > \epsilon Y$.

Ejercicio 2.67. Mostrar que si $M > 0$, y $MX > X$ entonces la desigualdad $M^k X > X$ se satisface para $k = 1, 2, \dots$, ¿qué variantes admite este resultado, cambiando algunos signos $>$ por \geq ?

Demostración de la proposición 2.18. La matriz M tiene un valor propio λ de módulo máximo $|\lambda| = r(M)$, con un vector propio X asociado⁵. Entonces

$$(2.46) \quad |MX| = |\lambda X| = |\lambda||X| = r(M)|X|.$$

Por lo tanto $r(M)|X| \leq |M||X| = M|X|$, de modo que

$$(2.47) \quad M|X| - r(M)|X| \geq O.$$

Mostraremos que hay igualdad en (2.47). Si no la hubiera, por la parte 2 del ejercicio 2.66, tendríamos que

$$M(M|X| - r(M)|X|) > O.$$

De la parte 3 del mismo ejercicio deducimos que existe un número $\epsilon > 0$ tal que

$$(2.48) \quad M(M|X| - r(M)|X|) > \epsilon M|X|.$$

Operando a partir de (2.48) concluimos

$$(2.49) \quad \frac{M}{r(M) + \epsilon} M|X| > M|X|.$$

Aplicando a (2.49) el resultado del ejercicio 2.67 concluimos

$$(2.50) \quad \left(\frac{M}{r(M) + \epsilon} \right)^k M|X| > M|X|, \quad k = 1, 2, \dots$$

Pero la matriz

$$\frac{M}{r(M) + \epsilon}$$

tiene radio espectral

$$\frac{r(M)}{r(M) + \epsilon} < 1,$$

por lo que el miembro de la izquierda en (2.50) tiende a cero cuando $k \rightarrow \infty$, en contradicción con que según (2.50) siempre es mayor que $M|X| > 0$. \square

Corolario 2.19. Si $M > O$ entonces $r(M) > 0$.

Demostración. M tiene un vector propio $X > O$ tal que $r(M)X = MX > O$, por lo que $r(M)$ no puede ser nulo. \square

El resultado que hemos probado es una parte del siguiente teorema, debido a Oskar Perron.

⁵En principio λ y el vector X podrían ser complejos. Por esa razón enunciamos el ejercicio 2.66 para números reales o complejos.

Teorema 2.20. Teorema de Perron.

Si $M > O$ es una matriz cuadrada entonces $r(M)$ es un valor propio de M , $\ker(M - \lambda I)$ tiene dimensión 1, está generado por un vector $X > O$, y contiene a todos los vectores propios de M cuyos coeficientes sean todas positivas. Además $r(M)$ es mayor que el módulo de cualquier otro valor propio de M .

En el ejercicio 5.17, página 150, proponemos al lector demostrar el teorema 2.20

Notablemente, una matriz $M \geq 0$ puede tener radio espectral nulo. Ver el ejemplo 2.26 y el ejercicio 2.61. También puede ocurrir que no haya un valor propio dominante. Sin embargo, vale el siguiente resultado.

Teorema 2.21. Teorema de Frobenius.

Si $M \geq 0$ es una matriz cuadrada entonces $r(M)$ es un valor propio de M que tiene asociado un vector propio con entradas no negativas.

Los resultados sobre valores y vectores propios de matrices no negativas son muy variados, y admiten diversas extensiones. El lector interesado puede encontrar en [3] una exposición amena al respecto, y muchas otras referencias.

2.4.5 Ejercicios adicionales

Ejercicio 2.68. ¿Es cierto que si todas las entradas de una matriz cuadrada M tienen módulo menor que 1 las potencias M^k tienden a O ?

Ejercicio 2.69. Para cada valor de λ hallar el radio espectral de la matriz

$$\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix}$$

y calcular directamente $(I - M)^{-1}$ cuando exista. Hallar los valores de λ que hacen que las matrices M e $(I - M)^{-1}$ tengan sus entradas no negativas y comparar los resultados con el enunciado de la proposición 2.17.

Para una matriz cuadrada M definimos la matriz exponencial

$$(2.51) \quad e^{Mt} = \sum_{i=0}^{\infty} \frac{(t^i M^i)}{i!}.$$

La serie en (2.51) siempre converge a una matriz que es de interés para la teoría de las ecuaciones diferenciales. Ver la monografía [5].

Ejercicio 2.70.

1. Para la matriz $D = \begin{bmatrix} \lambda_1 & \\ & \lambda_2 \end{bmatrix}$ mostrar que $e^{Dt} = \begin{bmatrix} e^{\lambda_1 t} & \\ & e^{\lambda_2 t} \end{bmatrix}$.
2. Mostrar que si $M = ADA^{-1}$ con D diagonal entonces $e^{Mt} = Ae^{Dt}A^{-1}$.

3. Calcular e^{Mt} para

$$M = \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix}, \quad M = \begin{bmatrix} 1 & 0 \\ 3 & 2 \end{bmatrix}.$$

Ejercicio 2.71. Para

$$J = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

encontrar e^{Jt} .

Ejercicio 2.72. Diagonalizar

$$M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

sobre \mathbb{C} y hallar e^{Mt} .

Capítulo 3: Producto escalar



Un concepto fundamental es que dos vectores X e Y son *ortogonales* o *perpendiculares* entre sí cuando su producto escalar $X \cdot Y$ es nulo.

Proponemos dos pequeños ejercicios para refrescar resultados de importancia que usaremos una y otra vez.

Ejercicio 3.1. Teorema de Pitágoras. Mostrar que dos vectores X e Y de \mathbb{R}^n son ortogonales entre sí si y sólo si

$$|X + Y|^2 = |X|^2 + |Y|^2.$$

A lo largo del texto hemos usado libremente la identificación natural entre vectores de \mathbb{R}^n , o \mathbb{C}^n , con matrices columna $n \times 1$, reales o complejas. El próximo ejercicio contiene resultados fundamentales para vincular el cálculo matricial con la estructura geométrica que el producto escalar genera en los espacios \mathbb{R}^n y \mathbb{C}^n .

Ejercicio 3.2.

1. Mostrar que

$$(3.1) \quad X \cdot Y = X^\top Y.$$

2. Mostrar que si M es una matriz real $m \times n$, entonces

$$(3.2) \quad (MX) \cdot Y = X \cdot (M^\top Y).$$

y

$$(3.3) \quad (MX) \cdot (MY) = (MX)^\top MY = X^\top M^\top MY,$$

3. Encontrar la forma que toman (3.1), (3.2) y (3.3) para matrices y vectores complejos.

Nota Histórica 3.1. La fórmula del producto escalar entre vectores, tal como la conocemos, tiene antecedentes antiguos. Ya en 1773, Joseph Louis Lagrange introdujo su expresión componente a componente para estudiar el tetraedro en tres dimensiones. La fundamental desigualdad de Cauchy-Schwarz fue descubierta para el caso de números por Augustin Cauchy en 1821.

Un paso hacia la sistematización en forma de un producto fue la introducción, por el matemático irlandés William Rowan Hamilton, del producto de cuaterniones en 1834. En sus fórmulas para los cuaterniones están implícitas las del producto escalar y el producto vectorial de vectores de \mathbb{R}^3 . Oliver Heaviside y Josiah Willard Gibbs

impulsaron y defendieron la adopción del producto escalar como objeto de interés en sí mismo. También la del producto vectorial, concepto que no trataremos en esta monografía. El logro de Heaviside de simplificar las ecuaciones del electromagnetismo de Maxwell, y el tratado sobre análisis vectorial de Gibbs fueron hitos en la clarificación y aceptación de este concepto, que tiene sentido físico y geométrico.

En esta última dirección, digamos que a partir de los productos escalares en \mathbb{R}^2 y en \mathbb{R}^3 pueden reconstruirse, respectivamente, toda la geometría euclidiana del plano y del espacio. Su extensión (1.42) a \mathbb{R}^n implica la generalización de esta geometría a espacios de dimensión finita pero arbitrariamente alta, y a situaciones que en una primera mirada podrían percibirse como carentes de geometría. Éstas son ideas que desarrollaremos algo más en los capítulos 3 y 4, y de las que mostraremos aplicaciones.

Se puede ir aún más allá. En honor de David Hilbert se llama espacios de Hilbert a una familia de espacios de dimensión infinita, en los que a través del concepto de producto interno, una generalización del producto escalar, se pueden definir las nociones de ángulo y ortogonalidad. De hecho, Buniakovsky y Schwarz descubrieron versiones de la desigualdad de Cauchy-Schwarz para integrales, en el marco de espacios de funciones. En la actualidad todos estas desigualdades son casos particulares de un teorema general válido para cualquier producto interno.

El propio Hilbert utilizó estas estructuras de dimensión infinita en el estudio de ecuaciones integrales. Se aplican en muy diversos dominios, entre ellos en la formalización de la mecánica cuántica. Pero quedándonos en el terreno de la geometría euclidiana del plano y el espacio, área en cuyos fundamentos también trabajó Hilbert, el producto escalar permite construir un modelo de la geometría en el que, dando definiciones adecuadas, los famosos postulados de Euclides pasan a ser teoremas.

Ejercicio 3.3. Buscar información sobre la construcción de modelos de la geometría de Euclides basados en el producto escalar. En particular, sobre las nociones de *espacio afín* y de *espacio euclídeo*.

Ejercicio 3.4. Buscar información sobre la extensión a espacios de dimensión infinita conocida como *espacios de Hilbert*, sobre sus aplicaciones, y sobre el propio Hilbert y sus contribuciones a la matemática.

En la sección 3.1 introduciremos la importante noción de *base ortonormal* y en la 3.2 mostraremos como las bases ortonormales permiten construir proyecciones. En la sección 3.3 mostramos como construir bases ortonormales y la versión matricial de este procedimiento, que da lugar a la importante factorización *QR* de cualquier matriz M . Todas estas ideas se aplican en la sección 3.4 a la resolución de sistemas lineales en el sentido de la aproximación por *mínimos cuadrados*.

3.1 Bases ortonormales de \mathbb{R}^n

Si $e \in \mathbb{R}^n$ es un vector de módulo 1 entonces $(X \cdot e)e$ es la proyección ortogonal de X sobre el subespacio generado por e .

Ejemplo 3.1. Si $X = (0, 1) \in \mathbb{R}^2$ y $e = (\sqrt{3}/2, 1/2)$ entonces $X \cdot e = 1/2$,

$$(X \cdot e)e = (\sqrt{3}/4, 1/4), \quad X - (X \cdot e)e = (-\sqrt{3}/4, 3/4).$$

El producto

$$(X - (X \cdot e)e) \cdot e = (\sqrt{3}/4, 1/4) \cdot (-\sqrt{3}/4, 3/4) = 0$$

indica que $X - (X \cdot e)e$ es ortogonal a e . Esto ocurre porque $(X \cdot e)e$ captura la

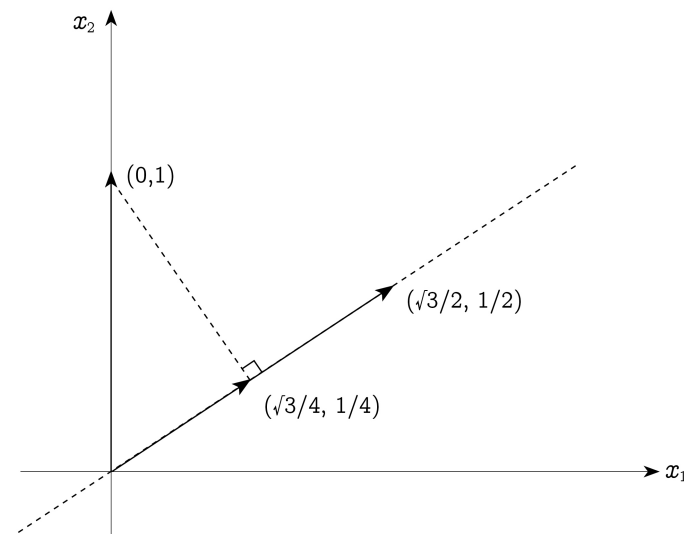


FIGURA 3.1. Proyección de $(0, 1)$ sobre $(\sqrt{3}/2, 1/2)$

componente de X según e , tal como se ilustra en la figura 3.1.

Ejercicio 3.5. Mostrar que si $|e| = 1$ y $X \in \mathbb{R}^n$ entonces $X - (X \cdot e)e$ es ortogonal a e .

Ejercicio 3.6. Mostrar que $\lambda = X \cdot e$ es el valor de λ que minimiza $|X - \lambda e|$. Interpretar geoméricamente estos resultados. Sugerencia: para minimizar $|X - \lambda e|$ es conveniente considerar $|X - \lambda e|^2$.

Para proyectar sobre un vector Y cualquiera de módulo distinto de 1 construimos un vector de módulo 1 colineal con Y ,

$$e_Y = Y/|Y|$$

dividiendo Y entre $|Y|$, procedimiento que llamamos *normalizar* Y . Entonces la proyección ortogonal de X sobre el subespacio generado por Y es

$$(3.4) \quad P(X) = (X \cdot e_Y)e_Y = \frac{X \cdot Y}{Y \cdot Y}Y.$$

Ejercicio 3.7. Aplicar (3.4) para calcular la proyección de $(0, 1)$ sobre el subespacio generado por $Y = (3, \sqrt{3})$ y comparar con el ejemplo 3.1. Representar el vector Y en la figura 3.1.

Para obtener las componentes de X en más de una dirección introduciremos las nociones de familia ortogonal y familia ortonormal.

Definición 3.1. Diremos que una familia

$$\mathcal{Q} = (Q_1, Q_2, \dots, Q_k) \subset \mathbb{R}^n$$

es **ortogonal** si cada vector de la familia es ortogonal a todos los demás. Diremos que la familia

$$\mathcal{O} = (O_1, O_2, \dots, O_k)$$

es **ortonormal** si es ortogonal y además todos los vectores en ella tienen módulo igual a 1.

Observación 3.1. La condición de que una familia \mathcal{O} sea ortonormal se expresa en términos de la delta de Kronecker como $O_i \cdot O_j = \delta_{ij}$.

Ejemplo 3.2. La familia $((1, 1), (2, -2))$ es ortogonal pero no ortonormal. Normalizando sus dos vectores construimos la familia ortonormal

$$\left((1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2}) \right).$$

Ejercicio 3.8. Construir en \mathbb{R}^3 una familia ortogonal con dos vectores y una con tres vectores, tales que ambas contengan a $(1, 2, 3)$. Normalizarlas para producir familias ortonormales.

Los vectores de una familia ortonormal están en direcciones del espacio tan diferentes entre sí como pueden serlo. En particular, vale la siguiente proposición.

Proposición 3.2. *Una familia ortonormal es linealmente independiente.*

La prueba hace uso de una técnica muy útil que mostramos en el lema 3.3: formar productos escalares con vectores convenientemente elegidos del espacio.

Lema 3.3. *Si $\mathcal{O} = (O_1, O_2, \dots, O_k)$ es ortonormal y X es una combinación lineal*

$$(3.5) \quad X = \sum_{i=1}^k \lambda_i O_i$$

entonces para $i = 1, \dots, k$ tenemos $\lambda_i = X \cdot O_i$.

PRUEBA. Haciendo el producto escalar de (3.5) con O_j se obtiene

$$X \cdot O_j = \sum_{i=1}^k \lambda_i O_i \cdot O_j = \sum_{i=1}^k \lambda_i \delta_{ij} = \lambda_j.$$

□

Prueba de la proposición 3.2. Al hacer una combinación lineal como en (3.5) que sea igual al vector nulo y aplicar el lema 3.3 se obtiene

$$0 = O \cdot X_i = \lambda_i, \quad i = 1, \dots, k.$$

□

Ejercicio 3.9. ¿Cuál es la condición necesaria y suficiente para que una familia ortogonal sea linealmente independiente?

Corolario 3.4. Una familia ortonormal $\mathcal{O} = (O_1, O_2, \dots, O_n)$ formada por n vectores de \mathbb{R}^n es una base de \mathbb{R}^n y para cada $X \in \mathbb{R}^n$ se tiene

$$(3.6) \quad X = \sum_{i=1}^n (X \cdot O_i) O_i.$$

Ejemplo 3.3. La base canónica

$$\mathcal{C} = (e_1, e_2, \dots, e_n)$$

de \mathbb{R}^n es ortonormal. Si $X = (x_1, \dots, x_n)$ entonces $X \cdot e_i = x_i$, y la expresión

$$X = \sum_{i=1}^n x_i e_i$$

es la forma que para este caso toma (3.6).

3.1.1 Expresión matricial y matrices ortogonales

Si M es una matriz, en el coeficiente de la fila i y la columna j de la matriz $M^\top M$ aparece el producto escalar de la i -ésima y la j -ésima columna de M .

Ejercicio 3.10. Demostrar esta afirmación.

Esta observación tiene la siguiente consecuencia.

Proposición 3.5. Sea O una matriz real $n \times k$. Las columnas de O forman un conjunto ortonormal en \mathbb{R}^n si y sólo si $O^\top O = I_k$, la matriz identidad $k \times k$.

Particularizándola al caso $k = n$ obtenemos nuestra próxima proposición.

Proposición 3.6. Sea O una matriz real $n \times n$. Las columnas de O forman una base ortonormal de \mathbb{R}^n si y sólo si $O^\top = O^{-1}$.

Ejercicio 3.11. Completar los detalles de una demostración de la proposición 3.6.

Definición 3.7. Llamaremos *matriz ortogonal* a una matriz cuadrada $n \times n$ tal que su traspuesta es igual a su inversa (o, equivalentemente, a aquella cuyas columnas forman una base ortonormal de \mathbb{R}^n).

Observación 3.2. Consideremos una matriz cuadrada O de orden n y un vector X cualquiera en \mathbb{R}^n . Cada uno de los coeficientes del vector $O^\top X$ es el producto escalar de una columna de O con X . Si las columnas de O forman una base ortonormal \mathcal{O} , entonces la fórmula (3.6), la definición del producto $O(O^\top X)$ como la combinación lineal de las columnas de O con los coeficientes de $O^\top X$ y la propiedad asociativa para el producto de matrices implican

$$X = O(O^\top X) = (OO^\top) X.$$

Por lo tanto la matriz OO^\top debe ser igual a la matriz identidad $n \times n$. Ésta es otra manera de ver que la matriz formada con los vectores de una base ortonormal resulta ser ortogonal.

Ejemplo 3.4. Un cálculo directo muestra que las columnas de la matriz

$$(3.7) \quad O = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 0 & 2/\sqrt{6} & 1/\sqrt{3} \\ -1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \end{bmatrix}$$

forman un conjunto ortonormal. Por lo tanto son una base ortonormal de \mathbb{R}^3 .

Ejercicio 3.12. Expresar cualquier vector $X \in \mathbb{R}^3$ como combinación lineal de las columnas de O . Verificar que los coeficientes de la combinación lineal son los coeficientes de $O^\top X$.

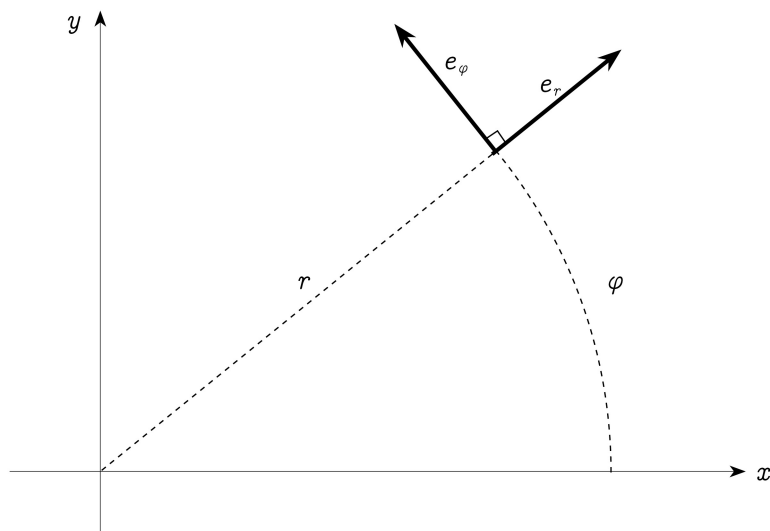
Ejemplo 3.5. Además de las coordenadas cartesianas, es corriente trabajar en el plano (x, y) con *coordenadas polares*, identificando cada punto (x, y) por su distancia r al origen y un ángulo φ de modo que

$$x = r \cos \varphi, \quad y = r \sin \varphi.$$

Asociado con este sistema de coordenadas, para cada valor de φ hay una base ortonormal (e_r, e_φ) del plano, donde e_r y e_φ son las columnas de la matriz

$$\begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}.$$

En la figura 3.2 mostramos esta base. La geometría se ve con más claridad al dibujar la base (e_r, e_φ) en el punto del plano con coordenadas (r, φ) , por lo que hemos adoptado esa representación (una convención similar se emplea en la figura 3.3). Una extensión al espacio tridimensional \mathbb{R}^3 se obtiene agregando a r y φ una tercera coordenada z .

FIGURA 3.2. Base ortonormal (e_r, e_φ)

Esto produce las llamadas *coordenadas cilíndricas* que tienen asociada para cada φ y θ la base ortonormal (e_r, e_φ, e_z) de \mathbb{R}^3 formada por las columnas de la matriz

$$\begin{bmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Notar que el vector e_z no es otra cosa que nuestro viejo conocido e_3 , de la base canónica de \mathbb{R}^3 .

En el espacio es posible usar también las *coordenadas esféricas* (r, φ, θ) que representan respectivamente la distancia a un origen O de referencia, y la longitud y la longitud sobre una esfera de centro O y radio unidad. Las columnas $(e_r, e_\varphi, e_\theta)$ de la matriz

$$\begin{bmatrix} \cos \varphi \cos \theta & -\sin \varphi & -\cos \varphi \sin \theta \\ \sin \varphi \cos \theta & \cos \varphi & -\sin \varphi \sin \theta \\ \sin \theta & 0 & \cos \theta \end{bmatrix}.$$

son para cada valor de φ y θ una base ortonormal de \mathbb{R}^3 , que está asociada con este sistema y que hemos representado en la figura 3.3.

En este ejemplo el lector debe prestar atención al hecho de que las mismas notaciones e_r y e_φ se usan para vectores diferentes de los vectores e_r y e_φ asociados con las coordenadas cilíndricas.

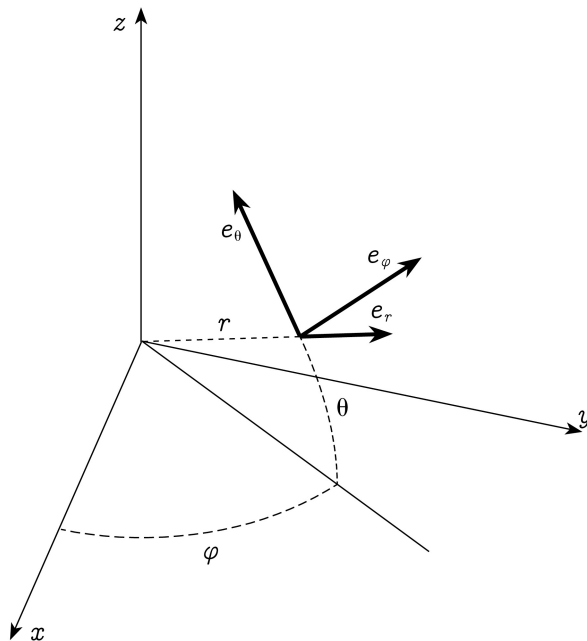


FIGURA 3.3. Base ortonormal $(e_r, e_\varphi, e_\theta)$

3.1.2 Matrices ortogonales e isometrías en \mathbb{R}^n

Para una matriz ortogonal O tenemos

$$(3.8) \quad (OX) \cdot (OY) = (OX)^\top (OY) = X^\top O^\top OY = X^\top Y = X \cdot Y.$$

Esto implica que una matriz ortogonal mantiene los productos internos entre vectores, y también sus módulos, ya que

$$|OX|^2 = (OX) \cdot (OX) = X \cdot X = |X|^2.$$

Además

$$|OX - OY| = |O(X - Y)| = |X - Y|,$$

por lo tanto O conserva la distancia euclidiana entre dos vectores cualesquiera X e Y y define una isometría en \mathbb{R}^n . Los próximos dos ejercicios caracterizan las isometrías en \mathbb{R}^n .

Ejercicio 3.13. Sea $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ una isometría tal que $f(O) = O$.

1. Mostrar que f preserva los productos escalares. Es decir,

$$f(X) \cdot f(Y) = X \cdot Y, \quad X, Y \in \mathbb{R}^n.$$

2. Sea (O_1, O_2, \dots, O_n) una base ortonormal de \mathbb{R}^n . Probar que

$$(3.9) \quad f(X) = \sum_{i=1}^n X \cdot O_i f(O_i).$$

Sugerencia: Mostrar que $(f(O_1), \dots, f(O_n))$ es una base ortonormal de \mathbb{R}^n y hallar la expresión de $f(X)$ en esta base.

3. Deducir de (3.9) que f es de la forma $f(X) = QX$, con Q una matriz ortogonal.

Ejercicio 3.14. Mostrar que $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ es una isometría si y sólo si es de la forma $f(X) = P + QX$, donde P es un vector fijo de \mathbb{R}^n que corresponde al valor que f toma en $O \in \mathbb{R}^n$, y Q es una matriz ortogonal.

Ejercicio 3.15. Describir todas las isometrías del plano \mathbb{R}^2 y del espacio \mathbb{R}^3 que no tienen ningún punto fijo.

Ejercicio 3.16. Relacionar el resultado del ejercicio 3.14 con los resultados de la geometría euclidiana acerca de las isometrías del plano y del espacio.

3.1.3 Ejercicios adicionales

Ejercicio 3.17. Mostrar que si M es una matriz $m \times n$ entonces MX queda determinado para cualquier vector de \mathbb{R}^n si se conoce MY para cualquier vector Y de \mathbb{R}^n que tenga módulo 1.

Ejercicio 3.18. Sea O una matriz real $n \times n$. Mostrar que las columnas de O forman una base ortonormal de \mathbb{R}^n si y sólo si sus filas forman una base ortonormal de \mathbb{R}^n .

Ejercicio 3.19. Verificar directamente que las filas de la matriz

$$\begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 0 & 2/\sqrt{6} & 1/\sqrt{3} \\ -1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \end{bmatrix}$$

con la que trabajamos en el ejemplo 3.4 forman una base ortonormal de \mathbb{R}^3 .

Ejercicio 3.20. Mostrar que la igualdad

$$MX \cdot Y = X \cdot MY.$$

se satisface para cualquier pareja de vectores X e Y en \mathbb{R}^n si y sólo si M es una matriz $n \times n$ simétrica.

Ejercicio 3.21. Mostrar que si X_1 y X_2 son vectores propios de una matriz simétrica M con valores propios λ_1 y λ_2 diferentes, entonces X_1 es ortogonal a X_2 .

Ejercicio 3.22. Con M indicaremos matrices cuadradas $n \times n$.

1. Mostrar que M satisface

$$(3.10) \quad (MX) \cdot (MY) = X \cdot Y, \quad X, Y \in \mathbb{R}^n,$$

si y sólo si es una matriz ortogonal.

2. Mostrar que $|MX| = |X|$ se satisface para todo $X \in \mathbb{R}^n$ si y sólo si es cierta (3.10).

3. Concluir que $|MX| = |X|$ se satisface para todo $X \in \mathbb{R}^n$ si y sólo si M es ortogonal.

Ejercicio 3.23. Mostrar que si Q_1 y Q_2 son matrices ortogonales entonces también es ortogonal su producto $Q_1 Q_2$.

Ejercicio 3.24. Sea \mathcal{O} una base ortonormal de \mathbb{R}^n . Para dos vectores X_1 y X_2 llamemos respectivamente Y_1 e Y_2 a sus coordenadas respecto a \mathcal{O} . Mostrar que

$$X_1 \cdot X_2 = Y_1 \cdot Y_2, \quad |X_1| = |Y_1|, \quad |X_2| = |Y_2|.$$

Ejercicio 3.25. Reformular para \mathbb{C}^n todos los resultados de esta sección, introduciendo los cambios que sean necesarios.

3.2 Bases ortonormales y proyecciones ortogonales

Un subespacio \mathbb{S} en \mathbb{R}^n induce una descomposición de \mathbb{R}^n en \mathbb{S} y todo lo ortogonal a \mathbb{S} . Para mostrar este hecho haremos uso de la proposición 3.8, cuya demostración posponemos hasta la sección 3.3.

Proposición 3.8. *Cualquier subespacio $\mathbb{S} \neq \{O\}$ de \mathbb{R}^n tiene una base ortonormal.*

También recurriremos al resultado del siguiente ejercicio.

Ejercicio 3.26. Un teorema de Pitágoras generalizado. Mostrar:

1. si $(Q_1, \dots, Q_k) \subset \mathbb{R}^n$ es ortogonal entonces $\left| \sum_{i=1}^k Q_i \right|^2 = \sum_{i=1}^k |Q_i|^2$.
2. si $(O_1, \dots, O_k) \subset \mathbb{R}^n$ es ortonormal entonces $\left| \sum_{i=1}^k \lambda_i O_i \right|^2 = \sum_{i=1}^k |\lambda_i|^2$.

3.2.1 Proyecciones sobre subespacios

Nuestra próxima proposición expresa que la proyección de un vector X de \mathbb{R}^n sobre un subespacio \mathbb{S} se obtiene haciendo productos escalares de X con una base ortonormal de \mathbb{S} .

Proposición 3.9. *Sea \mathbb{S} un subespacio de \mathbb{R}^n y $\mathcal{O} = (O_1, O_2, \dots, O_k)$ una base ortonormal de \mathbb{S} . Para cada $X \in \mathbb{R}^n$ definimos*

$$(3.11) \quad P_{\mathbb{S}} X = \sum_{i=1}^k (X \cdot O_i) O_i.$$

Entonces $X - P_{\mathbb{S}}X$ es ortogonal a cualquier vector de \mathbb{S} . Además, si $Y \in \mathbb{S}$ entonces

$$(3.12) \quad |X - P_{\mathbb{S}}X| \leq |X - Y|$$

y hay igualdad en (3.12) si y sólo si

$$(3.13) \quad Y = P_{\mathbb{S}}X.$$

Demostración. Para cada $j = 1, \dots, k$ calculamos

$$(X - P_{\mathbb{S}}X) \cdot O_j = X \cdot O_j - \sum_{i=1}^k (X \cdot O_i) O_i \cdot O_j.$$

Teniendo en cuenta que $O_i \cdot O_j = \delta_{ij}$ resulta

$$(X - P_{\mathbb{S}}X) \cdot O_j = X \cdot O_j - X \cdot O_j = 0.$$

Entonces $X - P_{\mathbb{S}}X$ es ortogonal a todos los vectores O_j , y a todas las combinaciones lineales de ellos, que son justamente los vectores de \mathbb{S} .

La segunda parte está basada en escribir un vector $Y \in \mathbb{S}$ como $Y = \sum_{i=1}^n \lambda_i O_i$. Tenemos luego que

$$X - Y = X - P_{\mathbb{S}}X + P_{\mathbb{S}}X - Y,$$

que escribimos en la forma

$$X - Y = (X - P_{\mathbb{S}}X) + \sum_{i=1}^n (X \cdot O_i - \lambda_i) O_i.$$

Por la ortogonalidad de todos los sumandos y el ejercicio 3.26 tenemos

$$|X - Y|^2 = |X - P_{\mathbb{S}}X|^2 + \sum_{i=1}^n |X \cdot O_i - \lambda_i|^2.$$

Concluimos inmediatamente que

$$(3.14) \quad |X - Y|^2 \geq |X - P_{\mathbb{S}}X|^2,$$

y que hay igualdad en (3.14) si y sólo si $\lambda_i = X \cdot O_i$, $i = 1, \dots, k$. □

Observación 3.3. Aunque construimos $P_{\mathbb{S}}X$ usando la fórmula (3.11) que depende de una base ortonormal de \mathbb{S} , el hecho de que $X - P_{\mathbb{S}}X$ sea ortogonal a cualquier vector de \mathbb{S} y la propiedad de optimalidad expresada por (3.12) y (3.13) implican que $P_{\mathbb{S}}X$ es único y sólo depende de \mathbb{S} y de X , pero no de la base ortonormal de \mathbb{S} que se emplee para construirlo. Es posible mostrar este mismo resultado usando argumentos de ortogonalidad, tal como se muestra en el siguiente ejercicio.

Ejercicio 3.27.

1. Mostrar que si U e V son dos vectores de \mathbb{R}^n ortogonales entre sí y tales que $O = U + V$, entonces $U = V = 0$.

2. Sean \mathbb{S} un subespacio de \mathbb{R}^n y $X \in \mathbb{R}^n$. Mostrar que si $X = U_1 + V_1$ y $X = U_2 + V_2$, donde U_1 y U_2 pertenecen a \mathbb{S} y V_1 y V_2 son ortogonales a todos los vectores de \mathbb{S} entonces $U_1 = U_2$ y $V_1 = V_2$.
3. Concluir que si \mathbb{S} es un subespacio de \mathbb{R}^n y $X \in \mathbb{R}^n$ entonces sólo puede existir un único vector $P_{\mathbb{S}}X \in \mathbb{S}$ tal que $V = X - P_{\mathbb{S}}X$ es ortogonal a todos los vectores de \mathbb{S} .

Definición 3.10. Proyección ortogonal sobre un subespacio. Dados un subespacio \mathbb{S} de \mathbb{R}^n y $X \in \mathbb{R}^n$ llamamos *proyección ortogonal* de X sobre \mathbb{S} al único vector $P_{\mathbb{S}}X$ de \mathbb{S} que satisface que $X - P_{\mathbb{S}}X$ es ortogonal a cualquier vector de \mathbb{S} .

Observación 3.4. De acuerdo con la proposición 3.9 el vector $P_{\mathbb{S}}X$ es el que hace mínimo el módulo $|X - Y|$ entre todos los $Y \in \mathbb{S}$. Vemos entonces que $P_{\mathbb{S}}X$ aparece como la mejor aproximación a X por vectores de \mathbb{S} . Esta caracterización de $P_{\mathbb{S}}X$ bien podría tomarse como definición de la proyección.

Ejemplo 3.6. La familia

$$\left(\left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}} \right), \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}} \right) \right)$$

es una base ortonormal de

$$\mathbb{S} = \{(x_1, x_2, x_3) \in \mathbb{R}^3, x_1 + x_2 + x_3 = 0\}.$$

Para proyectar $(0, 0, 1)$ sobre este subespacio calculamos los productos internos

$$\begin{aligned} (0, 0, 1) \cdot \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}} \right) &= -\frac{1}{\sqrt{2}}, \\ (0, 0, 1) \cdot \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}} \right) &= -\frac{1}{\sqrt{6}} \end{aligned}$$

y luego formamos la combinación lineal

$$P_{\mathbb{S}}(0, 0, 1) = -\frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}} \right) - \frac{1}{\sqrt{6}} \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}} \right) = \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3} \right).$$

La proyección se ilustra en la figura 3.4. Observemos que la diferencia

$$(0, 0, 1) - \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3} \right) = \frac{1}{3} (1, 1, 1)$$

es ortogonal a cualquier vector de \mathbb{S} .

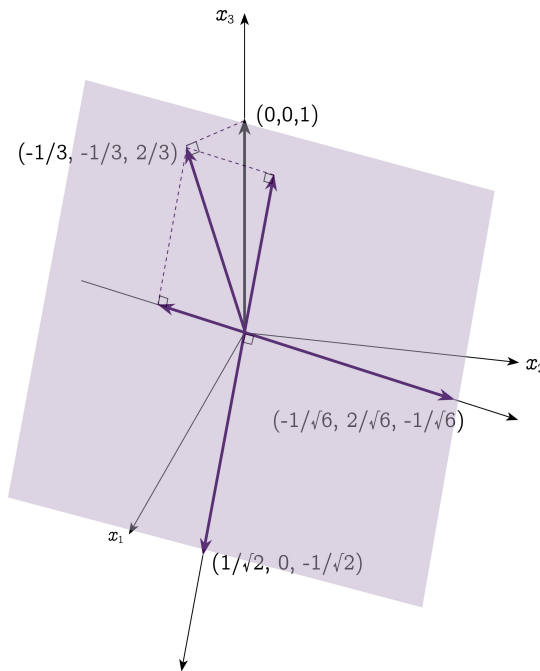
3.2.2 Expresión matricial de las proyecciones

La fórmula (3.11) para una proyección admite una expresión matricial. Si O es la matriz que tiene como columnas a los vectores O de una base ortonormal de \mathbb{S} , entonces $O^T X$ almacena los k productos escalares $X \cdot O_i$. El producto

$$(3.15) \quad O(O^T X) = OO^T X,$$

es justamente la combinación lineal en el miembro de la derecha de (3.11), por lo que

$$(3.16) \quad P_{\mathbb{S}}X = OO^T X.$$

FIGURA 3.4. Proyección de $(0,0,1)$ sobre \mathbb{S}

Ejemplo 3.7. Volvamos al subespacio \mathbb{S} y su base ortonormal del ejemplo 3.6. A partir de la base formamos la matriz

$$O = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{6} \\ 0 & 2/\sqrt{6} \\ -1/\sqrt{2} & -1/\sqrt{6} \end{bmatrix}.$$

La matriz

$$(3.17) \quad OO^\top = \frac{1}{3} \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}$$

representa la proyección sobre \mathbb{S}

Ejercicio 3.28. Hallar qué matriz es $O^\top O$, ¿el resultado es el esperado?

Observación 3.5. Cuando $\mathbb{S} = \mathbb{R}^n$ entonces $P_S X = O^\top O X = X$ y la matriz O es cuadrada y ortogonal. Ya habíamos encontrado este resultado en la observación 3.2, página 82.

Observación 3.6. Aunque las bases ortonormales son convenientes para los desarrollos teóricos, a la hora de calcular no es conveniente normalizar los vectores dividiéndolos entre su módulo. La razón es la siguiente: si Y es un vector cualquiera y

$$O_Y = \frac{Y}{|Y|}$$

entonces

$$(X \cdot O_Y)O_Y = \frac{X \cdot Y}{|Y|} \frac{Y}{|Y|} = \frac{X \cdot Y}{|Y|^2}.$$

Vemos que el factor de normalización $|Y|$ aparece elevado al cuadrado al final del cálculo, por lo que buscar la raíz de $Y \cdot Y$ para calcular $|Y|$ es inútil.

Ejercicio 3.29. Mostrar que si las columnas de una matriz Q son ortogonales y forman una base de un subespacio \mathbb{S} entonces

$$P_{\mathbb{S}}X = Q(Q^{\top}Q)^{-1}Q^{\top}X.$$

y

$$(3.18) \quad Q(Q^{\top}Q)^{-1}Q^{\top}$$

es la matriz que realiza la proyección ortogonal sobre \mathbb{S} .

Ejemplo 3.8. La familia

$$\mathcal{Q} = ((1, 0, -1), (-1, 2, -1))$$

es una base ortogonal del subespacio del ejemplo 3.6. Formamos a partir de ella la matriz

$$Q = \begin{bmatrix} 1 & -1 \\ 0 & 2 \\ -1 & -1 \end{bmatrix}.$$

Calculamos

$$Q^{\top}Q = \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix}, \quad (Q^{\top}Q)^{-1} = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/6 \end{bmatrix}.$$

Al completar los cálculos de $Q(Q^{\top}Q)^{-1}Q^{\top}$ encontramos nuevamente (3.17).

Ejercicio 3.30. Repetir los cálculos a partir de la base ortogonal

$$((0, -1, 1), (-2, 1, 1))$$

de \mathbb{S} y de la base que resulta de normalizar ambos vectores. Verificar que siempre se obtiene la misma matriz. Usarla para hallar la proyección de $(0, 0, 1)$. Comparar con el cálculo del ejemplo 3.6, página 88.

Ejercicio 3.31. Construir dos bases ortogonales diferentes del subespacio de \mathbb{R}^3 definido por la ecuación $x_1 - x_2 + 2x_3 = 0$, y calcular a partir de ellas la matriz que define la proyección ortogonal sobre ese subespacio.

3.2.3 Complementos ortogonales y proyecciones

Comenzamos esta sección con una definición, que esperamos que el lector encuentre bastante natural.

Definición 3.11. Si \mathcal{S} es un subconjunto cualquiera de \mathbb{R}^n , definimos su *conjunto ortogonal* \mathcal{S}^\perp como el conjunto de los vectores de \mathbb{R}^n que son ortogonales a cualquier vector de \mathcal{S} .

Ejemplo 3.9. Sea $\mathcal{C} = \{(1, 0, 0), (0, 1, 0)\} \subset \mathbb{R}^3$. Su conjunto ortogonal está formado por todos los vectores de la forma $(0, 0, z)$, con $z \in \mathbb{R}$.

Ejercicio 3.32. ¿Por qué?

Ejemplo 3.10. El conjunto ortogonal de \mathbb{R}^n es $\{O\}$, donde O indica al vector nulo, porque sólo el vector nulo es ortogonal a cualquier vector de \mathbb{R}^n . Escrito como una fórmula concisa: $(\mathbb{R}^n)^\perp = \{O\}$. Recíprocamente, $\{O\}^\perp = \mathbb{R}^n$.

Dado $Y \in \mathbb{R}^n$, la condición $X \cdot Y = 0$ es equivalente a que X satisfaga una ecuación lineal. Por la linealidad del producto escalar, el conjunto ortogonal a cualquier conjunto \mathcal{S} es un subespacio vectorial de \mathbb{R}^n .

Proposición 3.12. Para cualquier subconjunto \mathcal{S} de \mathbb{R}^n , su ortogonal \mathcal{S}^\perp es un subespacio vectorial de \mathbb{R}^n .

Ejercicio 3.33. Probar la proposición 3.12.

La proyección ortogonal de un vector X sobre un subespacio \mathbb{S} induce una única descomposición de X como la suma de los dos vectores ortogonales

$$P_{\mathbb{S}}X \in \mathbb{S}, \quad X - P_{\mathbb{S}}X \in \mathbb{S}^\perp.$$

Llamando s al primero y s^\perp al segundo, conseguimos nuestro próximo resultado.

Proposición 3.13. Dado un subespacio $\mathbb{S} \subset \mathbb{R}^n$, para cada $X \in \mathbb{R}^n$ existe una única pareja de vectores $s \in \mathbb{S}$, $s^\perp \in \mathbb{S}^\perp$, tales que

$$(3.19) \quad X = s + s^\perp.$$

La descomposición del espacio \mathbb{R}^n descrita por (3.19) permite mostrar que si \mathbb{S} es un subespacio, entonces es el conjunto ortogonal de su conjunto ortogonal.

Proposición 3.14. Sea \mathbb{S} un subespacio vectorial de \mathbb{R}^n . Entonces

$$(3.20) \quad \mathbb{S} = \mathbb{S}^{\perp\perp}.$$

Demostración. Si $X \in \mathbb{S}$ entonces es ortogonal a cualquier Y en \mathbb{S}^\perp , por definición de \mathbb{S}^\perp . Por lo tanto $X \in \mathbb{S}^{\perp\perp}$, lo que muestra que $\mathbb{S} \subset \mathbb{S}^{\perp\perp}$.

Para probar $\mathbb{S}^{\perp\perp} \subset \mathbb{S}$ consideremos $X \in \mathbb{S}^{\perp\perp}$. Podemos descomponer X en la forma (3.19), como

$$X = s + s^\perp, \quad s \in \mathbb{S}, \quad s^\perp \in \mathbb{S}^\perp.$$

El producto escalar de X con s^\perp es nulo, porque $X \in \mathbb{S}^{\perp\perp}$, entonces

$$0 = X \cdot s^\perp = (s + s^\perp) \cdot s^\perp = |s^\perp|^2.$$

Esto implica $s^\perp = O$, por lo que $X = s \in \mathbb{S}$. □

Ejercicio 3.34. Encontrar una base de \mathbb{S}^\perp para

$$\mathbb{S} = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 + x_3 = 0\},$$

y verificar (3.20).

3.2.4 Los cuatro subespacios

Como el producto MX de una matriz por un vector tiene como coeficientes los productos escalares de las filas de M con el vector X , la condición de que X esté en el núcleo de M puede formularse como una condición de ortogonalidad con las filas de M , o con las columnas de M^\top . En esa sección exploramos este tipo de relaciones.

Proposición 3.15. *Sea M una matriz real $m \times n$. Entonces*

1. $\ker M = (\operatorname{im}(M^\top))^\perp$;
2. $\operatorname{im} M = (\ker(M^\top))^\perp$;

Demostración. El breve argumento que precede al enunciado de la proposición es esencialmente una prueba de la parte 1, pero daremos otra a continuación.

$$X \in \ker(M) \Leftrightarrow MX = O \Leftrightarrow (MX) \cdot Y = 0, \forall Y \in \mathbb{R}^m \Leftrightarrow X \cdot (M^\top Y) = 0 \forall Y \in \mathbb{R}^m.$$

El conjunto formado por todos los vectores de la forma $M^\top Y$, cuando Y recorre todo \mathbb{R}^m es $\operatorname{im}(M^\top)$. Por lo tanto,

$$X \in \ker(M) \Leftrightarrow X \cdot Z = 0 \forall Z \in \operatorname{im}(M^\top) \Leftrightarrow X \in (\operatorname{im}(M^\top))^\perp.$$

Para probar la parte 2 observamos que la parte 1, aplicada a M^\top implica

$$\ker(M^\top) = (\operatorname{im}(M^{\top\top}))^\perp.$$

Teniendo en cuenta que $M^{\top\top} = M$ y tomando complementos ortogonales obtenemos

$$\ker(M^\top)^\perp = (\operatorname{im}(M))^{\perp\perp} = \operatorname{im}(M).$$

La última igualdad está justificada por la proposición 3.14. □

3.2.5 Ejercicios adicionales

Ejercicio 3.35. Desigualdad de Bessel e igualdad de Parseval. Sea \mathbb{S} un subespacio de \mathbb{R}^n , y $\mathcal{O} = (O_1, O_2, \dots, O_k)$ una base ortonormal de \mathbb{S} . Mostrar que para todo $X \in \mathbb{R}^n$ se tiene que

$$(3.21) \quad \sum_{i=1}^k |X \cdot O_i|^2 \leq |X|^2,$$

y que hay igualdad en (3.21) si y sólo si $X \in \mathbb{S}$.

Ejercicio 3.36. Si las columnas de una matriz Q forman una familia ortogonal y linealmente independiente entonces $Q(Q^\top Q)^{-1}Q^\top$ es la matriz de la proyección sobre la imagen de Q . Investigar si puede cambiarse el orden de los factores Q , $(Q^\top Q)^{-1}$ y Q^\top .

Ejercicio 3.37. Mostrar que una matriz cuadrada es la matriz de una proyección ortogonal si y sólo es simétrica y satisface $P^2 = P$. Sugerencia: mostrar que

$$X = PX + (X - PX)$$

induce una descomposición de cualquier vector X en dos vectores ortogonales.

Ejercicio 3.38. Mostrar que P es la matriz de una proyección ortogonal si y sólo si $I - P$ también lo es, ¿qué relación hay entre ambas proyecciones?

Ejercicio 3.39. Mostrar que T es una matriz ortogonal que satisface $T^2 = I$ si y sólo si $P = (T + I)/2$ representa una proyección ortogonal. Cuando esta condición se satisface, ¿cuál es la acción de T sobre los vectores del núcleo y la imagen de P ? Describir T geoméricamente.

Ejercicio 3.40. Si T es una matriz simétrica que satisface $T^2 = \alpha^2 I$ para algún número real α , mostrar que entonces existe una base ortonormal de \mathbb{R}^n formada por vectores propios de T .

Ejercicio 3.41. Mostrar que una matriz P es la matriz de una proyección ortogonal sobre un subespacio de \mathbb{R}^n si y sólo si existe una base ortonormal de \mathbb{R}^n en la que P queda representada por una matriz de la forma

$$\begin{bmatrix} I_k & \\ & \end{bmatrix},$$

donde I_k es la matriz identidad $k \times k$, y el resto de la matriz está formada por ceros, ¿cuál es la dimensión del espacio sobre el que se está proyectando?

Ejercicio 3.42. Mostrar que:

1. si $\mathcal{A} \subset B$ entonces $\mathcal{B}^\perp \subset \mathcal{A}^\perp$;
2. el conjunto ortogonal a un conjunto \mathcal{X} es igual al conjunto ortogonal al subespacio generado por \mathcal{X} .

Ejercicio 3.43. Para un conjunto $\mathcal{S} \subset \mathbb{R}^n$ cualquiera, investigar qué es $\mathcal{S}^{\perp\perp}$.

Ejercicio 3.44. Alternativa de Fredholm. Sean M una matriz $m \times n$ e Y un vector de \mathbb{R}^m . Mostrar que necesariamente ocurre una y sólo una de las siguientes dos posibilidades:

1. la ecuación $AX = Y$ tiene solución;
2. existe una solución de $A^\top X = O$ que satisface $Y^\top X \neq 0$.

En la monografía [4] se da una demostración diferente de la alternativa de Fredholm.

Ejercicio 3.45. Sea M una matriz real $n \times n$, simétrica.

1. Mostrar que $\ker(M)$ e $\operatorname{im}(M)$ son subespacios invariantes para M y ortogonales entre sí.
2. Generalizar la parte anterior para $\ker(M - \lambda I)$ e $\operatorname{im}(M - \lambda I)$, siendo λ un número cualquiera.
3. Mostrar que la unión de una base ortogonal de $\ker(M - \lambda I)$ con una base ortogonal de $\operatorname{im}(M - \lambda I)$ es una base ortogonal de \mathbb{R}^n .

Ejercicio 3.46. Verificar, haciendo explícitamente los cálculos, que cuando λ es un valor propio de

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

entonces $\ker(M - \lambda I)$ e $\operatorname{im}(M - \lambda I)$ son subespacios invariantes por M y ortogonales entre sí, ¿qué ocurre para los demás valores de λ ?

Ejercicio 3.47. Estudiar acerca de la ortogonalidad de los subespacios

$$\ker(M - \lambda I), \quad \operatorname{im}(M - \lambda I),$$

para la matriz

$$M = \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

y para todos los posibles valores de $\lambda \in \mathbb{R}$. Comparar los resultados con los del ejercicio anterior.

3.3 El método de Gramm-Schmidt y la descomposición QR

Cualquier subespacio de \mathbb{R}^n tiene bases ortonormales. Para mostrar que existen las construiremos usando un algoritmo, el *algoritmo de Gramm-Schmidt*, que produce una base ortogonal a partir de una base cualquiera. El resto es sencillo, porque para pasar de una base ortogonal a una ortonormal basta con una sencilla normalización que, como ya hemos comentado, a la hora de calcular más bien conviene no hacer (ver la observación 3.6, página 90).

3.3.1 Ortogonalización de Gram-Schmidt

Un ejemplo es ilustrativo de cómo funciona este algoritmo.

Ejemplo 3.11. A partir de la base

$$(3.22) \quad \mathcal{A} = (A_1, A_2, A_3) = ((1, 0, -1), (1, 1, -2), (0, 0, 1))$$

de \mathbb{R}^3 construiremos una base ortogonal $\mathcal{Q} = (Q_1, Q_2, Q_3)$.

PASO 1. Escogemos $Q_1 = A_1$. A continuación restaremos de los vectores restantes, A_2 y A_3 , sus proyecciones sobre la dirección de Q_1 . En la figura 3.5 mostramos a la

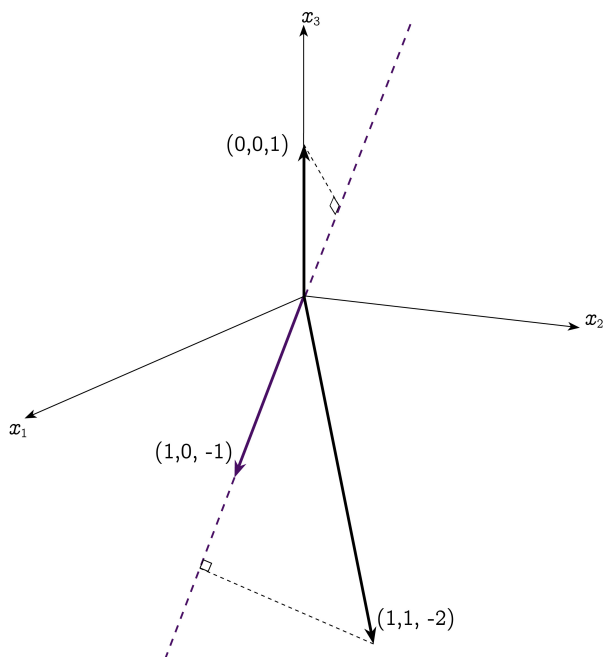


FIGURA 3.5. La base \mathcal{A}

base \mathcal{A} y las proyecciones de A_2 y A_3 sobre la dirección de A_1

Determinamos primero los coeficientes

$$r_{12} = \frac{A_2 \cdot Q_1}{Q_1 \cdot Q_1} = \frac{3}{2}, \quad r_{13} = \frac{A_3 \cdot Q_1}{Q_1 \cdot Q_1} = -\frac{1}{2}.$$

Luego restamos a cada vector su proyección sobre Q_1 :

$$\begin{aligned} (1, 1, -2) &\mapsto (1, 1, -2) - r_{12}(1, 0, -1) = \left(-\frac{1}{2}, 1, -\frac{1}{2}\right); \\ (0, 0, 1) &\mapsto (0, 0, 1) - r_{13}(1, 0, -1) = \left(\frac{1}{2}, 0, \frac{1}{2}\right). \end{aligned}$$

Hemos obtenido de A_2 y de A_3 dos nuevos vectores que llamaremos

$$A_2^{(1)} = \left(-\frac{1}{2}, 1, -\frac{1}{2}\right), \quad A_3^{(1)} = \left(\frac{1}{2}, 0, \frac{1}{2}\right).$$

En la nueva familia $\mathcal{A}^{(1)} = (Q_1, A_2^{(1)}, A_3^{(1)})$, el segundo y tercer vector son ortogonales al primero, por su construcción.

PASO 2 Escogemos $Q_2 = A_2^{(1)}$, y restamos de $A_3^{(1)}$ la componente según Q_2 . En la figura 3.6 aparece ahora $\mathcal{A}^{(1)}$ y la proyección de $(1/2, 0, 1/2)$ sobre nuestro recién adoptado Q_2 . Calculamos

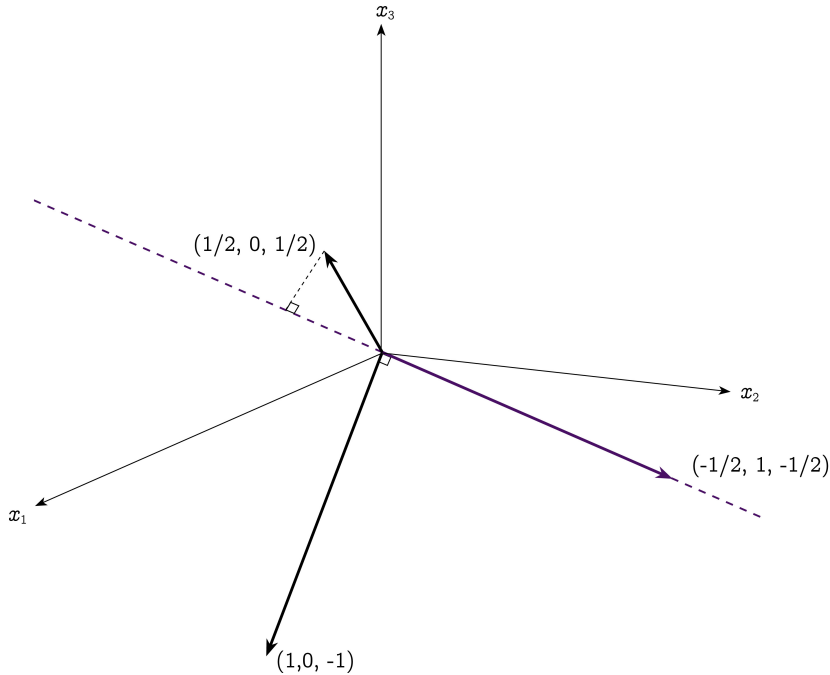


FIGURA 3.6. La base $\mathcal{A}^{(1)}$

$$r_{23} = \frac{A_3^{(1)} \cdot Q_2}{Q_2 \cdot Q_2} = -\frac{1}{3}.$$

y luego

$$A_2^{(3)} = \left(\frac{1}{2}, 0, \frac{1}{2}\right) - r_{23} \left(-\frac{1}{2}, 1, -\frac{1}{2}\right) = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right).$$

Observación 3.7. Al restar de $A_3^{(1)}$ la componente según Q_2 el resultado se mantiene ortogonal a Q_1 , porque estamos haciendo una combinación lineal de vectores ortogonales a Q_1 .

Ejercicio 3.48. Verificar directamente que $A_3^{(2)}$ es ortogonal a Q_1 .

Notemos también que Q_1 genera el mismo subespacio de dimensión 1 que A_1 , y que Q_1 y Q_2 generan el mismo subespacio dimensión 2 que A_1 y A_2 .

PASO 3. Elegimos $Q_3 = A_3^{(2)}$. Ya no quedan más vectores con los que trabajar, por lo que el algoritmo se detiene aquí.

La familia

$$(3.23) \quad \mathcal{Q} = ((1, 0, -1), (-1/2, 1, -1/2), (1/3, 1/3, 1/3))$$

es una base ortogonal de \mathbb{R}^3 . Normalizándola se obtiene

$$\mathcal{O} = \left(\left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}} \right), \left(-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}} \right), \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right) \right),$$

que es ortonormal. Representamos en la figura 3.7 la familia ortogonal \mathcal{Q} y su versión normalizada \mathcal{O} . Además el algoritmo produce la expresión

$$(3.24) \quad A_1 = Q_1, \quad A_2 = r_{12}Q_1 + Q_2, \quad A_3 = r_{13}Q_3 + r_{23}Q_2 + Q_3,$$

de los vectores de la base \mathcal{A} como combinaciones lineales de los vectores de \mathcal{Q} .

Ejercicio 3.49. Verificar las fórmulas (3.24) haciendo los cálculos.

Seguramente el lector podrá adaptar el procedimiento a nuevas situaciones.

Ejercicio 3.50. A partir de las bases

$$((1, 1, 1, 1), (1, 1, 1, 0), (1, 1, 0, 0), (1, 0, 0, 0))$$

y

$$((1, 0, 0, 0), (1, 1, 0, 0), (1, 1, 1, 0), (1, 1, 1, 1)),$$

de \mathbb{R}^4 construir bases ortonormales aplicando el método de Gramm-Schmidt. En cada caso escribir los vectores de la base original como combinaciones lineales de las nuevas bases.

Ejercicio 3.51. El subespacio \mathbb{S} formado por los vectores de \mathbb{R}^3 que satisfacen la ecuación $x_1 + x_2 + x_3 = 1$ tiene a

$$\mathcal{A} = ((1, 0, -1), (1, 1, -2))$$

como una de sus bases. Construir una base ortonormal de \mathbb{S} a partir de \mathcal{A} .

El procedimiento puede generalizarse para aplicarse a una familia linealmente independiente cualquiera $\mathcal{A} = (A_1, A_2, \dots, A_k)$ formada por k vectores de \mathbb{R}^n , como el siguiente algoritmo de ortogonalización:

1. inicializamos el proceso definiendo $\mathcal{Q}^{(0)} = \mathcal{A}$.

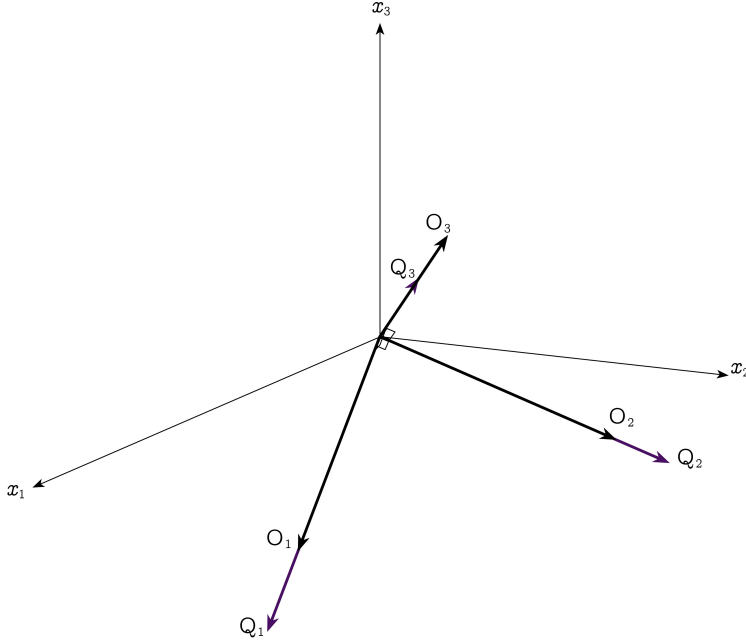


FIGURA 3.7. Las bases \mathcal{Q} y \mathcal{O} .

2. Para $k = 1, \dots, n-1$ actualizamos la familia $\mathcal{Q}^{(k-1)}$ por las reglas

$$\begin{cases} Q_j^k = Q_j^{k-1}, & 1 \leq j \leq k, \\ Q_j^{(k)} = Q_j^{k-1} - \frac{Q_j^{k-1} \cdot Q_k^k}{Q_k^k \cdot Q_k^k} Q_k^k, & k+1 \leq j \leq n. \end{cases}$$

Proposición 3.16. *Cuando el algoritmo de ortogonalización se aplica a una familia \mathcal{A} linealmente independiente produce una familia ortogonal $\mathcal{Q} = \mathcal{Q}^{(n-1)}$ con las siguientes propiedades:*

1. todos los vectores de \mathcal{Q} son no nulos;
2. $A_1 = Q_1$, y para $1 < j \leq n$ se tiene que

$$(3.25) \quad A_j = Q_j + \sum_{i=1}^{j-1} r_{ij} Q_i$$

con

$$(3.26) \quad r_{ij} = \frac{A_j \cdot Q_i}{Q_i \cdot Q_i}, \quad 1 \leq i < j.$$

3. para $k = 1, \dots, n$, los primeros k vectores de \mathcal{Q} forman una base del subespacio generado por los primeros k vectores de \mathcal{A} .

La demostración de esta proposición es inductiva sobre el número de vectores en la familia.

Ejercicio 3.52. Demostrar la proposición 3.16 (si el lector necesita inspiración sobre argumentos inductivos puede consultar la monografía [13]).

Ejercicio 3.53. Investigar qué ocurre cuando el algoritmo de Gramm-Schmidt se aplica a una familia que no es linealmente independiente.

Ahora estamos en condiciones de demostrar que cualquier subespacio \mathbb{S} de \mathbb{R}^n , distinto del subespacio trivial $\{O\}$, tiene bases ortonormales (proposición 3.8, página 86).

Demostración de la proposición 3.8. Aplicando el algoritmo de Gramm-Schmidt a una base cualquiera de \mathbb{S} se obtiene una base ortogonal, que produce una base ortonormal luego de ser normalizada. \square

3.3.2 Descomposición QR y sistemas lineales

Cualquier matriz M puede factorizarse como el producto QR de una matriz Q cuyas columnas forman una familia ortogonal, y una matriz R cuadrada, triangular superior. Esta *descomposición* QR no es otra cosa que la expresión matricial del método de Gramm-Schmidt. Su sentido geométrico explica muchas de sus propiedades y el interés que tiene para algunas aplicaciones.

Ejemplo 3.12. Las matrices

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ -1 & -2 & 1 \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & -1/2 & 1/3 \\ 0 & 1 & 1/3 \\ -1 & -1/2 & 1/3 \end{bmatrix}$$

tienen, respectivamente, como columnas a los vectores de las bases \mathcal{A} en (3.22), y \mathcal{Q} en (3.23), del ejemplo 3.11. Introduciendo la matriz

$$R = \begin{bmatrix} 1 & r_{12} & r_{13} \\ & 1 & r_{23} \\ & & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3/2 & -1/2 \\ & 1 & -1/3 \\ & & 1 \end{bmatrix}.$$

las fórmulas (3.24) que permiten expresar las columnas de A como combinaciones lineales de las columnas de Q se escriben matricialmente como $A = QR$.

El resultado del ejemplo anterior es general.

Proposición 3.17. Descomposición QR . Sea M una matriz $n \times k$ cuyas columnas son linealmente independientes. Entonces existe una matriz R triangular superior, $k \times k$, con unos en su diagonal, y una matriz Q $n \times k$, cuyas columnas forman una familia ortogonal en \mathbb{R}^n , tales que

$$(3.27) \quad M = QR.$$

La factorización (3.27) de una matriz M como el producto QR recibe el nombre de *descomposición QR* de M .

Ejercicio 3.54. Completar los detalles de la demostración de la existencia de la descomposición QR . Investigar acerca de la unicidad de tal descomposición. Extender los resultados al caso en que las columnas de M no sean linealmente independientes.

Ejercicio 3.55. Mostrar que si las columnas de M son linealmente independientes la matriz Q en la descomposición QR de M es tal que $Q^\top Q$ es invertible.

Observación 3.8. Para hallar la descomposición QR de M no es necesario aplicar el algoritmo de Gramm-Schmidt y luego escribir matricialmente los resultados. Si se va escribiendo el algoritmo en forma matricial desde un principio se obtiene directamente la factorización QR . Ver el ejemplo 3.13.

Igual que el método de eliminación gaussiana, la descomposición QR permite reducir a un sistema triangular cualquier sistema lineal de ecuaciones $MX = Y$. Si $M = QR$ podemos escribir el sistema en la forma

$$QRX = Y.$$

Multiplicando a la izquierda por Q^\top obtenemos

$$(3.28) \quad Q^\top QRX = Q^\top Y.$$

Cuando las columnas de Q son linealmente independientes la matriz $Q^\top Q$ es invertible (ver el ejercicio 3.55, por lo que (3.28) resulta entonces equivalente al sistema

$$(3.29) \quad RX = (Q^\top Q)^{-1} Q^\top Y.$$

La matriz R es triangular con unos en la diagonal, de modo que (3.29) este nuevo sistema tiene solución única y ésta, es fácil de encontrar.

Observación 3.9. El vector $Z = (Q^\top Q)^{-1} Q^\top Y$ y las columnas de R son respectivamente las coordenadas de Y y de las columnas de M respecto a la base de $\text{im}(M)$ formada por las columnas de Q .

Ejercicio 3.56. La ecuación 3.29 es la expresión de $MX = Y$ en coordenadas referidas a la base formada por las columnas de Q . Justificar esta afirmación.

Veamos todo esto funcionando en un ejemplo, en el que implementaremos la idea de que todas las matrices pueden ir calculándose a medida que avanza el proceso de escalerización.

Ejemplo 3.13. El sistema $MX = Y$ que se representa por la matriz ampliada

$$[M|Y] = \left[\begin{array}{cc|c} 1 & 3 & 4 \\ -3 & 1 & -2 \\ 2 & -4 & -2 \end{array} \right].$$

tiene como única solución $X = (1, 1)$. Llamemos M_1 y M_2 a las columnas de M . Para resolverlo calculando QR en el primer paso fijamos $Q_1 = M_1$ y buscamos las

componentes de M_2 e Y según Q_1 , con los que comenzamos a armar la matriz R , ampliada por una columna en la que aparecerá $Z = (Q^\top Q)^{-1} Q^\top Y$:

$$(3.30) \quad \left[\begin{array}{cc|c} 1 & -\frac{4}{7} & \frac{3}{7} \\ 0 & 1 & z_2 \end{array} \right].$$

Estos coeficientes permiten restar de M_1 e Y sus proyecciones sobre Q_1 . Al hacerlo actualizamos la matriz $[M|Y]$ a

$$(3.31) \quad \left[\begin{array}{cc|c} 1 & \frac{25}{7} & \frac{25}{7} \\ -3 & -\frac{5}{7} & -\frac{5}{7} \\ 2 & \frac{20}{7} & \frac{20}{7} \end{array} \right].$$

Notar que las columnas segunda y tercera de (3.31) son ortogonales a la primera. Actualizamos (3.30) calculando el coeficiente de la tercera columna de (3.31) respecto a la segunda, para obtener

$$(3.32) \quad \left[\begin{array}{cc|c} 1 & -\frac{4}{7} & \frac{3}{7} \\ 0 & 1 & 1 \end{array} \right].$$

La solución del sistema $RX = Z$ en (3.32) es, efectivamente, $X = (1, 1)$. Todavía podemos actualizar (3.31) con el último coeficiente que hemos calculado. El resultado es

$$\left[\begin{array}{cc|c} 1 & \frac{25}{7} & 0 \\ -3 & -\frac{5}{7} & 0 \\ 2 & \frac{20}{7} & 0 \end{array} \right].$$

Ejercicio 3.57. ¿Qué significado tiene esta tercera columna de ceros?

Ejercicio 3.58. Identificar la descomposición QR de M , y usarla junto con la fórmula (3.29) para hallar el sistema $RX = Z$ que corresponde a este ejemplo.

Ejercicio 3.59. Resolver usando el algoritmo de la descomposición QR el sistema

$$[M|Y] = \left[\begin{array}{ccc|c} 1 & 1 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ -1 & -2 & 1 & -2 \end{array} \right].$$

Ejercicio 3.60. El sistema representado por la matriz ampliada

$$\left[\begin{array}{cc|c} 1 & 3 & 4,1 \\ -3 & 1 & -1,9 \\ 2 & -4 & -1,9 \end{array} \right]$$

es incompatible. Pero al resolverlo usando QR se obtiene la solución $X = (1, 1)$. ¿Cuál es la explicación? Volveremos sobre este problema en la sección 3.4.3.

Ejercicio 3.61. ¿Qué ocurre al utilizar el método basado en QR para resolver un sistema compatible de ecuaciones $MX = Y$ cuando las columnas de M no son linealmente independientes?

Ejercicio 3.62. Investigar en la literatura qué ventajas y desventajas tiene el algoritmo de resolución de sistemas usando QR con respecto al algoritmo clásico de eliminación gaussiana, ¿cuál de ellos considera más fácil de implementar?

3.4 Mínimos cuadrados

Un sistema lineal $MX = Y$ puede no tener solución, es lo que llamamos un *sistema incompatible*. El método de mínimos cuadrados transforma $MX = Y$ en un sistema aproximado $MX = \hat{Y}$ que siempre tiene solución. Este procedimiento, que en principio puede parecer arbitrario, tiene significado en diversos campos del análisis de datos: ajuste de modelos a observaciones experimentales, recuperación de señales contaminadas por ruido, problemas de inteligencia artificial, etcétera. No discutiremos aquí los detalles ni las referencias históricas, que son apasionantes, ni profundizaremos en su justificación, pero remitimos al lector a [15, 10] para mayor información.

3.4.1 Proyecciones sobre la imagen de M

Dada una matriz M de tamaño $m \times n$, los vectores Y que hacen compatible

$$(3.33) \quad MX = Y$$

son justamente ¡los que pueden escribirse en la forma MX ! Cuando el sistema es incompatible, el *método de mínimos cuadrados* propone considerar en vez del vector Y a su mejor aproximación (en el sentido del módulo $\|\cdot\|$ en \mathbb{R}^m) por vectores de la forma MX . El conjunto de todos estos vectores no es otra cosa que la imagen $\text{im}(M)$ de la matriz M . Por lo tanto, este método nos lleva a resolver el sistema compatible

$$(3.34) \quad MX = P_{\text{im}(M)}Y,$$

donde $P_{\text{im}(M)}Y$ es la proyección ortogonal de Y sobre $\text{im}(M)$.

Ejemplo 3.14. El sistema $MX = Y$ con matriz ampliada

$$\left[\begin{array}{cc|c} 1 & 3 & 4, 1 \\ -3 & 1 & -1, 9 \\ 2 & -4 & -1, 9 \end{array} \right].$$

es incompatible. La proyección ortogonal de Y sobre $\text{im}(M)$ es $(4, -2 - 2)$.

Ejercicio 3.63. Completar los detalles de este cálculo.

Resolvemos entonces el sistema compatible

$$\left[\begin{array}{cc|c} 1 & 3 & 4 \\ -3 & 1 & -2 \\ 2 & -4 & -2 \end{array} \right]$$

que tiene solución $X = (1, 1)$.

Observación 3.10. Si las columnas de M no son linealmente independientes el sistema (3.34) es indeterminado. En la mayor parte de las aplicaciones del método el número m de ecuaciones es mucho mayor que el de incógnitas n , y la matriz M es $m \times n$ y tiene sus columnas linealmente independientes. Por lo tanto, su rango es n . En lo sucesivo nos concentraremos en este caso.

Si M es una matriz $m \times n$ de rango n el sistema (3.34) es compatible y determinado. Su solución X es lo que llamaremos la *solución de $MX = Y$ por mínimos cuadrados*.

Observación 3.11. Cuando un sistema $MX = Y$ es compatible el vector Y está en $\text{im}(M)$. Por lo tanto $Y = P_{\text{im}(M)}Y$ y el sistema (3.34) no es otra cosa que el mismo sistema original (3.33). Lo que implica que la solución de mínimos cuadrados es una generalización de la noción de solución de un sistema lineal.

La solución de $MX = Y$ en el sentido de mínimos cuadrados es el vector $X \in \mathbb{R}^n$ que hace mínimo $|MX - Y|$. Esta es una caracterización variacional de X , porque cualquier variación respecto a la solución hace crecer $|MX - Y|$.

Observemos que X también minimiza $|MX - Y|^2$, lo que justifica el nombre del método.

3.4.2 Ecuaciones normales

Las relaciones entre los cuatro subespacios asociados a una matriz M , permiten derivar un sencillo conjunto de ecuaciones para hallar la solución de mínimos cuadrados del sistema $MX = Y$.

Buscamos un vector X tal que vector $MX = P_{\text{im}(M)}Y$, por lo tanto, debe satisfacer

$$Y - MX \in \text{im}(M)^\perp = \ker(M^\top),$$

lo que implica

$$M^\top(MX - Y) = O.$$

Desarrollando obtenemos el sistema

$$(3.35) \quad M^\top MX = M^\top Y.$$

Este sistema lineal de ecuaciones recibe el nombre de *ecuaciones normales*.

Ejercicio 3.64. Mostrar que si M es $m \times n$ y de rango n la matriz $M^\top M$ es cuadrada e invertible.

Por el ejercicio 3.64, si M tiene rango n entonces (3.35) tiene una única solución, que además admite la expresión matricial

$$(3.36) \quad X = (M^\top M)^{-1} M^\top Y.$$

Ejemplo 3.15. Para la matriz M y el vector Y del ejemplo 3.14 tenemos

$$M^\top M = \begin{bmatrix} 14 & -8 \\ -8 & 26 \end{bmatrix}, \quad M^\top Y = \begin{bmatrix} 6 \\ 18 \end{bmatrix}.$$

Las ecuaciones normales son el sistema

$$\left[\begin{array}{cc|c} 14 & -8 & 6 \\ -8 & 26 & 18 \end{array} \right],$$

en cuya solución $X = (1, 1)$ reencontramos el resultado del ejemplo 3.14.

La fórmula (3.36) para la solución X del sistema $MX = P_{\text{im}(M)}Y$ implica que para todo Y en \mathbb{R}^n se tiene

$$(3.37) \quad M(M^\top M)^{-1}M^\top Y = P_{\text{im}(M)}Y.$$

Por lo tanto, cuando M es $m \times n$ y de rango n

$$(3.38) \quad M(M^\top M)^{-1}M^\top$$

es la matriz de la proyección ortogonal sobre la imagen de M .

Ejercicio 3.65. Verificarlo para la matriz M de los ejemplos 3.14 y 3.15.

Observación 3.12. Seudoinversa. Cuando las columnas de M son linealmente independientes la matriz

$$M^+ = (M^\top M)^{-1}M^\top$$

recibe el nombre de *seudoinversa* de M .

Ejercicio 3.66. Mostrar que $M^+M = I$.

Volveremos sobre esta noción cuando en la sección 4.3 discutamos algunas aplicaciones de la descomposición en valores singulares. Ver los ejercicios 4.51 y 4.52 en la página 139.

Observación 3.13. Formar las ecuaciones normales no es un método conveniente para resolver problemas de mínimos cuadrados. Una de las razones es que este procedimiento aumenta el *número de condición* del problema, que es una medida de la sensibilidad a los errores en los datos. Como los datos de un problema real siempre se adquieren con errores, y la resolución numérica siempre introduce problemas de redondeo, esta cuestión no puede obviarse. Para más detalles, el lector puede consultar [15].

3.4.3 Mínimos cuadrados y descomposición QR

La descomposición QR provee un método de resolución de problemas de mínimos cuadrados. Al emplear la descomposición $M = QR$ el sistema $MX = Y$ se reduce a

$$(3.39) \quad RX = (Q^\top Q)^{-1}Q^\top Y,$$

(ver (3.29), página 100), cuya solución satisface

$$MX = QRX = Q(Q^\top Q)^{-1}Q^\top Y.$$

El miembro de la derecha es la proyección ortogonal de Y sobre $\text{im}(Q) = \text{im}(M)$. En conclusión, cuando el sistema $MX = Y$ es incompatible su solución por el método

QR es justamente la solución en el sentido de mínimos cuadrados. Esta observación explica el resultado del ejercicio 3.60, página 101. Lo veremos en el próximo ejemplo.

Ejemplo 3.16. Aplicaremos el método QR al sistema

$$\left[\begin{array}{cc|c} 1 & 3 & 2,1 \\ -3 & 1 & 1,1 \\ 2 & -4 & -2,9 \end{array} \right].$$

de los ejemplos 3.14 y 3.15. En el primer paso conseguimos los coeficientes para calcular la primera fila de la matriz ampliada del sistema (3.39):

$$(3.40) \quad \left[\begin{array}{cc|c} 1 & -4/7 & 3/7 \\ 0 & 1 & z_2 \end{array} \right].$$

La entrada z_2 todavía es desconocida, porque representa a la componente de Y según la segunda columna de Q , que aún no ha sido calculada. Actualizamos el cálculo de Q como

$$(3.41) \quad \left[\begin{array}{cc|c} 1 & 25/7 & 257/70 \\ -3 & -5/7 & -43/70 \\ 2 & -20/7 & -193/70 \end{array} \right].$$

Determinamos ahora z_2 y completamos (3.40):

$$\left[\begin{array}{cc|c} 1 & -4/7 & 3/7 \\ 0 & 1 & 1 \end{array} \right].$$

Resolviendo este sistema podemos encontrar que $X = (1, 1)$ es la solución del problema de mínimos cuadrados. La actualización de (3.41) restando de la tercera columna su componente según la segunda arroja

$$(3.42) \quad \left[\begin{array}{cc|c} 1 & 25/7 & 1/10 \\ -3 & -5/7 & 1/10 \\ 2 & -20/7 & 1/10 \end{array} \right].$$

En la tercera columna aparece la diferencia $Y - MX$, el vector ortogonal a las columnas de M que es la diferencia entre Y y su mejor aproximación por vectores en la imagen de M .

Cuando el sistema $MX = Y$ se resuelve por mínimos cuadrados su solución satisface $MX = P_{\text{im}(M)}Y$. Por lo tanto

$$(3.43) \quad Y - MX = Y - P_{\text{im}(M)}Y \in \text{im}(M)^\perp.$$

A este vector se le llama el *residuo* de la solución. .

Ejercicio 3.67. Usar el método de la descomposición QR para hallar la solución de mínimos cuadrados y su residuo para el sistema

$$\left[\begin{array}{cc|c} 4 & -3 & 6 \\ 0 & -5 & -4 \\ 1 & -2 & -4 \end{array} \right].$$

3.4.4 Ejercicios adicionales

Ejercicio 3.68. Supongamos que dos variables x e y están relacionadas por una relación lineal del tipo $y = mx$, donde m es una constante, y que disponemos de un conjunto de observaciones

$$(x_i, y_i), \quad i = 1, \dots, n,$$

de las variables x e y , con el que pretendemos averiguar el valor de m . Encontrarlo de dos maneras diferentes:

1. resolviendo el sistema lineal $mX = Y$, con n ecuaciones e incógnita m , en el sentido de mínimos cuadrados;
2. empleando técnicas de cálculo para minimizar en m la expresión

$$\sum_{i=1}^m (y_i - mx_i)^2.$$

Ejercicio 3.69. Mostrar que la media aritmética $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ puede interpretarse como la solución en el sentido de mínimos cuadrados de una ecuación

$$x\mathbf{1} = X,$$

donde X es el vector que contiene los n datos x_i , y $\mathbf{1}$ es un vector de n unos.

Ejercicio 3.70. Investigar qué ocurre si en los problemas de ajuste de una recta, ejercicio 3.68, y de hallar un número \bar{x} que indique la tendencia de un conjunto de datos x_i , ejercicio 3.69, se modifica el criterio de aproximación a uno basado en $\|\cdot\|_1$ en vez de $|\cdot|$. Es decir, en el primer caso buscamos m que minimice $\|mX - Y\|_1$, y en el segundo \bar{x} que minimice $\|x\mathbf{1} - X\|_1$.

Si M es una matriz real $m \times n$ de rango n , se puede mostrar directamente que la matriz

$$(3.44) \quad P = M(M^\top M)^{-1}$$

es la matriz de una proyección ortogonal.

Ejercicio 3.71. Sea M una matriz $m \times n$ de rango n , Mostrar que P en (3.44) es una matriz simétrica que satisface

$$P^2 = P, \quad \text{im}(P) = \text{im}(M), \quad \text{im}(P) = \ker(P)^\perp.$$

Concluir que P es la proyección ortogonal sobre la imagen de M .

Capítulo 4: Teorema espectral y descomposición en valores singulares



En este capítulo presentamos dos resultados importantes, con enorme contenido geométrico: el *teorema espectral para matrices simétricas* y la *descomposición en valores singulares*, válida para matrices cualesquiera. Ambos aportan descripciones acerca de cómo actúan las matrices al transformar vectores, pueden representarse también como teoremas de *factorización* de matrices, y tienen gran cantidad de aplicaciones y múltiples extensiones.

4.1 Teorema espectral para matrices simétricas

El principal objetivo de esta sección es demostrar el siguiente teorema.

Teorema 4.1. Teorema espectral.

Sea M una matriz real $n \times n$. Entonces M es simétrica si y sólo si existe una base ortonormal de \mathbb{R}^n formada por vectores propios de M .

En la sección 4.1.2 aplicaremos el teorema 4.1 a las formas cuadráticas. Luego mostraremos una extensión a matrices normales, que usaremos en la sección 4.1.4 para estudiar las isometrías de \mathbb{R}^n . Pero el Teorema Espectral tiene muchas más aplicaciones, en los dominios más variados.

4.1.1 Prueba del teorema espectral para matrices simétricas

Para una matriz M la existencia de una base de vectores propios es equivalente a la existencia de una factorización $M = ADA^{-1}$, con D diagonal (teorema 2.7, página 56). Cuando las bases son ortonormales este resultado puede refinarse.

Lema 4.2. *Sea M una matriz real $n \times n$. Son equivalentes*

1. *existe una base ortonormal formada por vectores propios de M ;*
2. *existen una matriz ortogonal Q y una diagonal D tales que $M = QDQ^T$.*

Ejercicio 4.1. Demostrar el lema 4.2. Extender el resultado para matrices complejas.

Ejercicio 4.2. Mostrar que si M es una matriz real $n \times n$ y \mathbb{R}^n tiene una base ortonormal formada por vectores propios de M entonces M es simétrica.

El ejercicio 4.2 demuestra una de las implicaciones en el enunciado del teorema 4.1. La otra requiere algo más de trabajo.

Lema 4.3. *Una matriz simétrica M tiene un valor propio real.*

Demostración. La matriz M tiene un valor propio complejo λ (lema 2.2, página 52), por lo tanto existe un vector propio $Z \in \mathbb{C}^n$ asociado a λ . Como M es simétrica

$$(4.1) \quad MZ \cdot Z = Z \cdot M^\top Z = Z \cdot MZ.$$

Por otra parte, simplemente invirtiendo el orden en el producto escalar, tenemos

$$(4.2) \quad MZ \cdot Z = \overline{Z \cdot MZ}.$$

Combinando (4.1) y (4.2) concluimos que $MZ \cdot Z$ es un número real. Formando el producto escalar de $MZ = \lambda Z$ con Z obtenemos

$$MZ \cdot Z = \lambda Z \cdot Z = \lambda |Z|^2.$$

Como $|Z|^2$ es no nulo resulta que

$$\lambda = \frac{MZ \cdot Z}{|Z|^2}$$

es real, por ser el cociente de dos reales. \square

Demostración del teorema 4.1 La demostración es inductiva sobre n . Para matrices 1×1 el resultado es trivialmente cierto. Supongamos entonces demostrado el teorema para matrices $k \times k$, para cualquier valor de $k \leq n - 1$.

Sabemos que M tiene un valor propio real λ . Si $\ker(M - \lambda I)$ es todo \mathbb{R}^n entonces $M = \lambda I$ y es una matriz diagonal. En caso contrario

$$\dim(\ker(M - \lambda I)) = k < n,$$

y

$$\ker(M - \lambda I)^\perp = \text{im}((M - \lambda I)^\top) = \text{im}(M - \lambda I),$$

es un subespacio no trivial, invariante para M . Si \mathcal{O}_1 y \mathcal{O}_2 son bases ortonormales de $\ker(M - \lambda I)$ y de $\text{im}(M - \lambda I)$ respectivamente, entonces $\mathcal{O} = \mathcal{O}_1 \cup \mathcal{O}_2$ es una base ortonormal de \mathbb{R}^n (ver el ejercicio 3.45, página 94). Si O es la matriz ortogonal cuyas columnas son los vectores en \mathcal{O} entonces

$$(4.3) \quad M = O \begin{bmatrix} \lambda I_k & \\ & N \end{bmatrix} O^\top,$$

donde I_k es la matriz identidad $k \times k$ y N es una matriz simétrica $(n - k) \times (n - k)$. Por la hipótesis inductiva

$$N = Q_1 D_1 Q_1^\top,$$

con Q_1 ortogonal y D_1 diagonal, ambas $(n - k) \times (n - k)$.

Las matrices

$$Q_2 = \begin{bmatrix} I_k & \\ & Q_1 \end{bmatrix}, \quad D = \begin{bmatrix} \lambda I_k & \\ & D_1 \end{bmatrix}$$

son respectivamente una matriz ortogonal y una matriz diagonal que satisfacen

$$(4.4) \quad \begin{bmatrix} \lambda I_k & \\ & N \end{bmatrix} = Q_2 D Q_2^\top.$$

Combinando (4.3) y (4.4) obtenemos

$$M = O Q_2 D Q_2^\top O^\top = O Q_2 D (O Q_2)^\top.$$

Esta factorización de M completa la demostración. \square

Ejercicio 4.3. Justificar por qué la matriz N en (4.3) es simétrica.

Ejemplo 4.1. Consideremos

$$M = \begin{bmatrix} 25 & -15 \\ -15 & 25 \end{bmatrix}.$$

Los valores propios de M son 40, con un subespacio propio generado por $(1, -1)$ y 10, cuyo subespacio asociado está generado por $(1, 1)$. Una base ortonormal que diagonaliza esta matriz es

$$\mathcal{U} = \left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right), \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right) \right).$$

En correspondencia con esto, las matrices

$$(4.5) \quad D = \begin{bmatrix} 40 & \\ & 10 \end{bmatrix}, \quad U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

factorizan M como $M = U D U^\top$.

Ejercicio 4.4. Hallar una base ortonormal que diagonalice a

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

4.1.2 Formas cuadráticas y cónicas

Una forma cuadrática en \mathbb{R}^n es un polinomio homogéneo de segundo grado en las variables x_1, x_2, \dots, x_n .

Ejemplo 4.2. La función $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}$ definida para cada $X = (x_1, x_2)$ por la fórmula

$$(4.6) \quad \varphi(X) = 25x_1^2 - 30x_1x_2 + 25x_2^2.$$

es un ejemplo de forma cuadrática.

En general, una forma cuadrática es una suma de productos $x_i x_j$, multiplicados por coeficientes a_{ij} . Por esta razón, cualquier forma cuadrática φ definida en \mathbb{R}^n puede expresarse para cada $X \in \mathbb{R}^n$ en la forma

$$(4.7) \quad \varphi(X) = X^\top M X,$$

donde M es una matriz simétrica.

Ejemplo 4.3. La forma cuadrática del ejemplo 4.2 puede escribirse como

$$\varphi(X) = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}^\top \begin{bmatrix} 25 & -15 \\ -15 & 25 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

Observemos que la matriz que apareció es la del ejemplo 4.1

Ejercicio 4.5. Hallar matrices que permitan escribir las formas cuadráticas

1. $x_1^2 + 2x_1x_2 + 3x_2^2$,
2. $x_1^2 - 2x_1x_2 + x_2^2$,
3. $2x_1^2 - x_1x_2 + x_2^2$,

en la forma (4.7).

Las formas cuadráticas aparecen en diversos dominios de la matemática y otras ciencias. Una de sus aplicaciones más importantes es el estudio de puntos críticos de funciones de varias variables. En este problema, como en muchos otros, interesa especialmente determinar el signo de los valores de la función φ . Este problema es sencillo de resolver, si se conoce una diagonalización de M en la forma $M = UDU^\top$, con D diagonal y U ortogonal. Se tiene

$$(4.8) \quad \varphi(X) = X^\top MX = X^\top UDU^\top X = Y^\top DY = \sum_{i=1}^n \lambda_i y_i^2,$$

donde $[y_1, y_2, \dots, y_n]^\top = Y = U^\top X$, no es otra cosa que las coordenadas de X respecto a la base formada por las columnas de U y los números λ_i son los valores propios de M . Entonces los signos de los valores propios de M determinan los posibles signos de $\varphi(X)$.

Ejemplo 4.4. Usando la diagonalización de la matriz M en el ejemplo 4.1, la igualdad (4.8) adopta para (4.6) la forma

$$(4.9) \quad \varphi(X) = 40 \left(\frac{x_1 - x_2}{\sqrt{2}} \right)^2 + 10 \left(\frac{x_1 + x_2}{\sqrt{2}} \right)^2,$$

que revela $\varphi(X) > 0$ siempre que $X \neq O$, porque los dos valores propios de M son positivos.

Ejercicio 4.6. Desarrollar (4.9) y verificar que se recupera (4.6).

Ejercicio 4.7. Estudiar en el plano (x_1, x_2) el signo de las formas cuadráticas asociadas con las siguientes matrices.

$$\begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}.$$

Este tipo de técnicas permite reconocer conjuntos del plano caracterizados por ecuaciones cuadráticas, entre los que se encuentran las cónicas: elipses, parábolas e hipérbolas.

Ejemplo 4.5. Consideremos el conjunto del plano formado por las parejas (x_1, x_2) que satisfacen la ecuación

$$(4.10) \quad 25x_1^2 - 30x_1x_2 + 25x_2^2 - 90x_1 + 70x_2 + 84 = 0.$$

Se trata de la elipse en la figura 4.1. A continuación consideraremos una estrategia general para reconocer este tipo de figuras.

La ecuación (4.10) puede escribirse en la forma

$$(4.11) \quad X^\top M X + X^\top A + c = 0,$$

con

$$M = \begin{bmatrix} 25 & -15 \\ -15 & 25 \end{bmatrix}, \quad A = \begin{bmatrix} -90 \\ 70 \end{bmatrix}, \quad c = 84.$$

La ecuación (4.11) se simplifica introduciendo las coordenadas $Y = U^\top X$ que diagonalizan M , operación que corresponde a un giro de ejes en el plano. El resultado es

$$(4.12) \quad Y^\top D Y + Y^\top U^\top A + c = 0,$$

Ejemplo 4.6. Para los valores numéricos del ejemplo (4.10) la matriz M es una vieja conocida, y el cambio de base que la diagonaliza está definido por la matriz U en (4.5). Las líneas punteadas en la figura 4.1 corresponden a los ejes coordenados (y_1, y_2) del

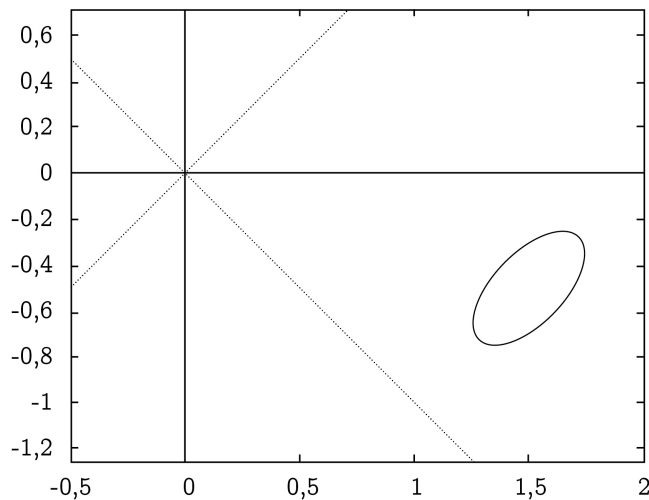


FIGURA 4.1. La elipse definida por (4.10)

sistema ortogonal de coordenadas definido por las columnas de U . Para este ejemplo

concreto la ecuación (4.12) toma la forma

$$Y^\top \begin{bmatrix} 40 & \\ & 10 \end{bmatrix} Y - Y^\top \begin{bmatrix} 80\sqrt{2} \\ 10\sqrt{2} \end{bmatrix} + 84 = 0,$$

y describe a la elipse en el sistema de coordenadas Y . La representación de la elipse en este nuevo sistema de coordenadas aparece en la figura 4.2.

Buscaremos deshacernos del término lineal por medio de una traslación del origen de coordenadas. Esto es equivalente a introducir una nueva coordenada

$$Z = Y - Y_0.$$

Por lo tanto $Y = Z + Y_0$. Al substituir, (4.12) se transforma en

$$(Z + Y_0)^\top D(Z + Y_0) + (Z + Y_0)^\top U^\top A + c = 0.$$

Desarrollamos los cálculos y obtenemos

$$Z^\top DZ + Z^\top (2DY_0 + U^\top A) + Y_0^\top DY_0 + Y_0^\top U^\top A + c = 0.$$

Para eliminar el término lineal buscamos Y_0 tal que

$$(4.13) \quad 2DY_0 + U^\top A = O.$$

Si podemos resolver (4.13), la ecuación (4.11) finalmente toma la forma

$$(4.14) \quad Z^\top DZ + d = 0,$$

donde d es la constante

$$d = Y_0^\top DY_0 + Y_0^\top U^\top A + c.$$

Ejemplo 4.7. Para el ejemplo (4.10) la solución de (4.13) es $Y_0 = (\sqrt{2}, 1/\sqrt{2})$, y la forma (4.14) es

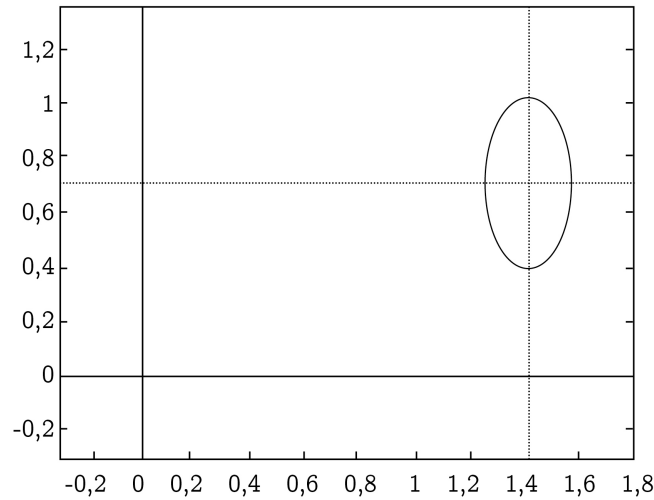
$$(4.15) \quad Z^\top DZ - 1 = 0.$$

La variable Z es sólo una traslación de la Y . Los nuevos ejes de coordenadas (z_1, z_2) son los que aparecen con líneas punteadas en la figura 4.2. Al escribir (4.15) haciendo aparecer explícitamente las variables z_1 y z_2 obtenemos

$$40z_1^2 + 10z_2^2 = 1.$$

Reconocemos en esta fórmula la ecuación de una elipse centrada en $(0, 0)$, con semiejes de longitud $1/\sqrt{40}$ y $1/\sqrt{10}$.

En resumen, el procedimiento adoptado consiste en girar los ejes de coordenadas para alinearlos con los vectores propios de la matriz M (esto hace desaparecer todos los términos de segundo orden que no son cuadráticos), y luego hacer una traslación que absorba los términos lineales. Esto último no siempre se consigue, porque la ecuación (4.13) puede no tener solución, pero en ese caso la traslación de ejes puede usarse para hacer desaparecer el término independiente.

FIGURA 4.2. La elipse definida por (4.10) vista en los ejes (y_1, y_2)

Ejemplo 4.8. Para la ecuación

$$x_1^2 + 2x_1x_2 + x_2^2 - 4x_1 - 5y_2 + 4 = 0$$

la forma (4.12) es

$$(4.16) \quad Y^\top \begin{bmatrix} 2 & \\ & 0 \end{bmatrix} Y - Y^\top \begin{bmatrix} 9/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} + 4 = 0,$$

que en coordenadas (y_1, y_2) toma el aspecto

$$(4.17) \quad 2y_1^2 - \frac{9}{\sqrt{2}}y_1 - \frac{1}{\sqrt{2}}y_2 + 4 = 0.$$

Ejercicio 4.8. Completar los detalles del cálculo.

En este caso la ecuación (4.13) no tiene solución. Pero podemos absorber el término de (4.17) que es lineal en y_1 completando el cuadrado en y_1 . Obtenemos

$$2 \left(y_1 - \frac{9}{4\sqrt{2}} \right)^2 - \frac{81}{16} - \frac{1}{\sqrt{2}}y_2 + 4 = 0.$$

Un poco más de manipulación transforma esta ecuación en

$$2 \left(y_1 - \frac{9}{4\sqrt{2}} \right)^2 - \frac{1}{\sqrt{2}} \left(y_2 + \frac{17}{8\sqrt{2}} \right) = 0.$$

Escogiendo nuevas variables

$$z_1 = y_1 - \frac{9}{4\sqrt{2}}, \quad z_2 = y_2 + \frac{17}{8\sqrt{2}},$$

lo que equivale a trasladar el origen de coordenadas sin girar los ejes. La ecuación final, en las nuevas variables $Z = (z_1, t_2)$ es

$$z_2 = 2\sqrt{2}z_1^2,$$

que corresponde a una parábola. En el primer esquemas de la figura 4.3 aparece la

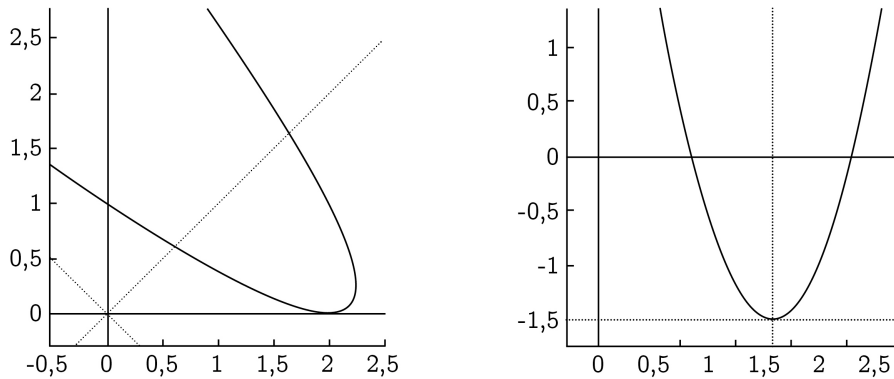


FIGURA 4.3. La parábola definida por (4.10), y los ejes correspondientes a los distintos sistemas de coordenadas usados para su reconocimiento.

parábola en el plano (x_1, x_2) y, en trazo punteado, los ejes que corresponden a las variables (y_1, y_2) . En el segundo ya hemos girado los ejes para representar la parábola en el plano (y_1, y_2) , y se indican los ejes que corresponden a las coordenadas (z_1, z_2) .

Ejercicio 4.9. Reconocer las figuras planas definidas por las ecuaciones:

1. $x_1^2 + 2x_1x_2 + 6x_2^2 + 8x_2 + 2 = 0$;
2. $x_1^2 - 2x_1x_2 + x_2^2 + 6x_1 + 1 = 0$;
3. $2x_1^2 - x_1x_2 - x_2^2 + 2x_1 + x_2 + 3 = 0$.

Describir los movimientos de sistemas de coordenadas empleados en el reconocimiento.

Ejercicio 4.10. Extender los procedimientos de reconocimiento de cónicas en el plano al reconocimiento de cuádricas (superficies definidas por ecuaciones cuadráticas) en el espacio.

Otro problema interesante es determinar los valores máximo y mínimo que sobre S^{n-1} puede alcanzar una forma cuadrática.

Proposición 4.4. Sea $\varphi : \mathbb{R}^n \mapsto \mathbb{R}$ la forma cuadrática en \mathbb{R}^n definida por la matriz simétrica M y la fórmula $\varphi(X) = X^\top MX$. Sean $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ los valores propios de M , ordenados en forma decreciente. Entonces φ alcanza sobre S^{n-1} un valor máximo igual a λ_1 , y un mínimo igual a λ_n .

Demostración. Escribamos $\varphi(X)$ en la forma (4.8). El vector $Y = U^\top X$ tiene módulo 1. Entonces

$$\varphi(X) = \sum_{i=1}^n \lambda_i y_i^2 \leq \sum_{i=1}^n \lambda_1 y_i^2 = \lambda_1.$$

Además $\lambda_1 = \varphi(U_1)$, donde U_1 es la primera columna de U .

Ejercicio 4.11. Completar la demostración probando los resultados para el valor mínimo. \square

Corolario 4.5. Sea M una matriz $m \times n$. Entonces el módulo $|MX|$ alcanza un valor máximo sobre S^{n-1} , que es igual a $\sqrt{\lambda_1}$, donde $\lambda_1 \geq 0$ es el valor propio de $M^\top M$ con mayor módulo.

Demostración. Que el módulo $|MX|$ alcance su valor máximo es equivalente a que

$$(4.18) \quad |MX|^2 = (MX) \cdot MX = (MX)^\top MX = X^\top M^\top MX.$$

alcance su máximo. Como (4.18) es una forma cuadrática con matriz simétrica $M^\top M$ su valor máximo sobre S^{n-1} es igual a λ_1 , que no puede ser negativo porque es el cuadrado del módulo de un vector. El máximo de $|MX|$ es entonces $\sqrt{\lambda_1}$. \square

Observación 4.1. El corolario implica que la norma $\|\cdot\|_2$ para las matrices que introdujimos en la sección 1.3.4 está correctamente definida, y además da una expresión para su valor.

Ejemplo 4.9. Los valores máximo y mínimo de la forma cuadrática (4.6) sobre S^1 son 40 y 10. Se alcanzan en $\pm(1/\sqrt{2}, -1/\sqrt{2})$ y $\pm(1/\sqrt{2}, 1/\sqrt{2})$.

Ejercicio 4.12. Hallar los valores máximo y mínimo sobre S^1 de las formas cuadráticas del ejercicio 4.7. Encontrar también el máximo y el mínimo sobre la circunferencia de centro O y radio 2.

4.1.3 Teorema espectral para matrices normales

En esta sección presentamos una versión del teorema espectral para matrices complejas y damos las pautas para una demostración. En la sección 4.1.4 lo aplicaremos al estudio de las matrices ortogonales reales, cuya estructura puede elucidarse completamente a partir de su diagonalización sobre \mathbb{C} .

Definición 4.6. Matrices normales. Llamaremos *matrices normales* a las matrices complejas cuadradas M que conmutan con su traspuesta conjugada \overline{M}^\top , en el sentido de que se satisface la igualdad $M\overline{M}^\top = \overline{M}^\top M$.

Teorema 4.7. Teorema espectral para matrices normales.

Una matriz compleja M es normal, si y sólo si existe una base ortonormal de \mathbb{C}^n formada por vectores propios de M .

Ejercicio 4.13.

1. Mostrar que si una matriz compleja se diagonaliza en una base ortonormal de \mathbb{C}^n entonces es normal.
2. Mostrar que si las matrices M y N conmutan entonces $\text{im}(M)$ y $\text{ker}(M)$ son subespacios invariantes para N .
3. Mostrar que si un subespacio \mathbb{S} es invariante para M , su complemento ortogonal \mathbb{S}^\perp es invariante para \overline{M}^\top .
4. Completar la demostración del teorema 4.7. Sugerencia: adoptar la demostración del teorema 4.1.

Ejemplo 4.10. La matriz

$$M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

es una matriz ortogonal que satisface $MM^\top = M^\top M = I$. Como es una matriz real $\overline{M}^\top = M^\top$, por lo que M es normal. Los valores propios de M son $\pm i$ y una base ortonormal que diagonaliza M sobre \mathbb{C} es

$$((i, 1), (-i, 1)).$$

Tal como ocurre para cualquier matriz real, los valores propios complejos vienen en parejas de un número λ y su conjugado $\bar{\lambda}$, y los vectores propios correspondientes a λ y $\bar{\lambda}$ son conjugados.

Ejercicio 4.14. Mostrar que cualquier matriz de la forma

$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

es normal y encontrar una base ortonormal de \mathbb{C}^2 que la diagonalice.

4.1.4 Forma canónica real de matrices ortogonales

Las matrices ortogonales reales son matrices normales, porque

$$Q = \overline{Q}, \quad Q^\top Q = QQ^\top = I.$$

Por lo tanto, se diagonalizan sobre \mathbb{C} , como la matriz del ejemplo 4.10. Mostraremos que de esta forma diagonal compleja puede deducirse una descomposición de \mathbb{R}^n en subespacios ortogonales sobre los que Q actúa como la identidad, como una simetría o como un giro.

Lema 4.8. Si Q es ortogonal y $\lambda \in \mathbb{C}$ es un valor propio entonces $|\lambda| = 1$.

Demostración. Si Z es un vector propio asociado al valor propio λ entonces $QZ = \lambda Z$, por lo que $|QZ| = |\lambda||Z|$. Por ser Q ortogonal $|Z| = |QZ|$. De estas dos igualdades se deduce $|\lambda| = 1$. \square

Los únicos valores propios reales de Q pueden ser entonces 1 y -1 . Los valores propios con parte imaginaria no nula son de la forma

$$\lambda = \cos \theta - i \sin \theta,$$

para algún valor de θ que no es un múltiplo de π . Llamaremos

$$Z = \Re(Z) + i\Im(Z)$$

al vector propio correspondiente. De acuerdo con los resultados de la sección 2.3.3 también $\bar{\lambda}$ es un valor propio de M , \bar{Z} es un vector propio con valor propio $\bar{\lambda}$, y el subespacio de \mathbb{R}^n generado por

$$\mathcal{A} = (\Re(Z), \Im(Z))$$

es invariante para M . Si llamamos \mathbb{S}_λ a este subespacio entonces \mathcal{A} es una base de \mathbb{S}_λ y la acción de M en \mathbb{S}_λ se representa respecto a la base \mathcal{A} por la matriz

$$(4.19) \quad \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

Ésta es la matriz de un giro. Para asegurarnos de que M efectivamente actúa como un giro en \mathbb{S}_λ nos falta ver que la base \mathcal{A} es ortogonal y está formada por vectores que tienen el mismo módulo.

Proposición 4.9. *Sea Q una matriz ortogonal real, λ un valor propio complejo de Q , y*

$$Z = \Re(Z) + i\Im(Z)$$

un vector propio asociado al valor propio λ . Entonces $\Re(Z)$ e $\Im(Z)$ son vectores ortogonales que tienen el mismo módulo.

Demostración. Z y \bar{Z} son vectores ortogonales que tienen el mismo módulo. Entonces

$$\begin{aligned} |\Re(Z)|^2 &= |(Z + \bar{Z})/2| = (|Z|^2 + |\bar{Z}|^2)/4, \\ |\Im(Z)|^2 &= |(Z - \bar{Z})/(2i)| = (|Z|^2 + |\bar{Z}|^2)/4, \\ \Re(Z) \cdot \Im(Z) &= ((Z + \bar{Z})/2) \cdot ((Z - \bar{Z})/(2i)) = (|Z|^2 - |\bar{Z}|^2)/(4i) = 0. \end{aligned}$$

Dividiendo $\Re(Z)$ e $\Im(Z)$ entre $|\Re(Z)| = |\Im(Z)|$ conseguimos una base ortonormal del subespacio \mathbb{S}_λ . \square

Ejemplo 4.11. Retomemos los cálculos del ejemplo 4.10. La matriz M tiene valores propio $\lambda = -i$ y su conjugado $\bar{\lambda} = i$. El vector propio que corresponde al valor propio $-i$ es $Z = (1, i)$, que puede escribirse separando su parte real e imaginaria como

$$(1, i) = (1, 0) + i(0, 1).$$

Efectivamente, las partes real e imaginaria de Z forman una base ortogonal, que además ya está normalizada: la base canónica de \mathbb{R}^2 .

Ejemplo 4.12. La matriz

$$(4.20) \quad Q = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

es ortogonal. Tiene un valor propio real 1 con vector propio $(1, 1, 1)$, y valores propios complejos conjugados $(-1 \pm \sqrt{3}i)/2$. Los vectores propios correspondientes al valor propio $(-1 - \sqrt{3}i)/2$ están generados por

$$\left(1, -\frac{1 + \sqrt{3}i}{2}, \frac{-1 + \sqrt{3}i}{2}\right) = \left(1, -\frac{1}{2}, -\frac{1}{2}\right) + i \left(0, -\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}\right).$$

Respecto a la base ortonormal

$$\left((1/\sqrt{3})(1, 1, 1), (1/\sqrt{6})(2, -1, -1), (1/\sqrt{2})(0, -1, 1)\right)$$

la matriz Q se representa como

$$J = \begin{bmatrix} 1 & & \\ & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}.$$

Ejercicio 4.15. Interpretar geoméricamente el resultado. Hallar una matriz ortogonal U tal que $Q = UJU^\top$.

Ejercicio 4.16. Para la matriz ortogonal

$$Q = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

hallar un ángulo θ y una base ortonormal de \mathbb{R}^3 en la que la matriz toma la forma

$$\begin{bmatrix} 1 & & \\ & \cos \theta & -\operatorname{sen} \theta \\ & \operatorname{sen} \theta & \cos \theta \end{bmatrix}.$$

Hacerlo de dos maneras:

1. usando los resultados del ejemplo 4.12 y el hecho de que Q es el cuadrado de la matriz que aparece en (4.20);
2. buscando los valores y vectores propios de Q .

Ejercicio 4.17. En este ejercicio Q representa una matriz ortogonal $n \times n$.

1. Mostrar que si $n = 2$ existe una base ortonormal de \mathbb{R}^2 en la que Q toma una de las dos posibles formas siguientes:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} \cos \theta & -\operatorname{sen} \theta \\ \operatorname{sen} \theta & \cos \theta \end{bmatrix}.$$

El parámetro θ es algún número real, que puede escogerse en el intervalo $[0, 2\pi)$. Discutir el significado geométrico de cada una de las posibilidades.

2. Mostrar que si $n = 3$ entonces existe una base ortonormal en la que Q toma una forma diagonal con ± 1 en la diagonal, o una base ortonormal en la que Q toma la forma

$$\begin{bmatrix} \pm 1 & & \\ & \cos \theta & -\operatorname{sen} \theta \\ & \operatorname{sen} \theta & \cos \theta \end{bmatrix}.$$

Interpretar geométricamente las diferentes posibilidades.

3. ¿Cómo se generalizan los resultados de esta sección a matrices ortogonales reales $n \times n$, para n cualquiera?

En los ejercicios 3.13 y 3.14, página 84, aprendimos que toda isometría f en \mathbb{R}^n es de la forma

$$(4.21) \quad f(X) = P + QX,$$

donde P es la imagen por f del origen O , y Q es una matriz ortogonal. Si f tiene un punto fijo X_0 tal que $f(X_0) = X_0$ su expresión se simplifica cambiando a las coordenadas $Y = X - X_0$. Llamemos $G(Y) = F(X) - X_0$ a la nueva coordenada de $F(X)$. Entonces

$G(Y) = F(X) - X_0 = P + Q(X) - X_0 = P + Q(Y + X_0) - X_0 = QY + F(X_0) - X_0$, como X_0 es un punto fijo, entonces

$$G(Y) = QY.$$

Por lo tanto existe un sistema de coordenadas ortonormal, con origen X_0 , en el que la isometría f está representada por una matriz Q en alguna de las formas canónicas que discutimos en el ejercicio 4.17.

Ejercicio 4.18. Hallar la condición que deben satisfacer P y Q en (4.21) para que la isometría f no tenga puntos fijos.

Nota Histórica 4.1. *Los antecedentes más antiguos del teorema espectral aparecen ya en los inicios de la geometría analítica. Pierre de Fermat y René Descartes, conocían la posibilidad de rotar los ejes del plano para simplificar la expresión de una forma cuadrática. En el contexto de buscar formas normales para formas cuadráticas Agustín Cauchy mostró entre 1826 y 1830 que toda matriz simétrica es diagonalizable, con valores propios reales. Las versiones matriciales de estos resultados tuvieron que esperar la aparición de las matrices y su cálculo, y recién en 1858 Arthur Cayley formuló los resultados sobre formas cuadráticas como un resultado acerca de la diagonalización de una matriz.*

Las versiones más fascinantes del teorema espectral para matrices simétricas son las que corresponden a sus extensiones a espacios de dimensión infinita. Grandes

avances en esta teoría se deben a los trabajos David Hilbert y Erhard Schmidt. Justamente fue Schmidt quien extendió a espacios de dimensión infinita el método de ortogonalización que estudiamos en la sección 3.3. En la década de 1920 esta teoría tuvo un papel importante en la descripción unificada de la mecánica cuántica de Heisenberg y Schrödinger. John von Neumann dio en 1929 una versión del teorema espectral que permite describir a todos los observables de la mecánica cuántica. El espectro, que es el análogo en esta teoría del conjunto de los valores propios de una matriz, tiene, efectivamente, una correspondencia con los espectros de átomos y moléculas.

Los incansables matemáticos no se detuvieron en este resultado de Von Neumann. Aparecieron luego las versiones para los operadores que extienden a las matrices normales, y nuevas extensiones y reinterpretaciones, a través de los trabajos de la escuela de Gelfand, que no describiremos.

4.1.5 Ejercicios adicionales

Ejercicio 4.19. Discutir en función del valor de \mathbf{a} qué conjunto de puntos del plano describen las ecuaciones

1. $x_1^2 + x_2^2 + 2\mathbf{a}x_1x_2 + 2x_1 + 1 = 0$;
2. $x_1^2 - x_2^2 - 2x_1 + \mathbf{a} = 0$

Ejercicio 4.20. Mostrar que una forma cuadrática queda completamente determinada por sus valores sobre la esfera unidad S^{n-1} de \mathbb{R}^n .

Ejercicio 4.21. Mostrar que dos matrices cuadradas simétricas M y N conmutan si y sólo si existe una base ortonormal que diagonaliza a ambas simultáneamente. Sugerencia: mostrar que los subespacios propios de M son invariantes para N .

Ejercicio 4.22. El teorema espectral para matrices simétricas, teorema 4.1, tiene consecuencias, a veces sorprendentes, en las más variadas áreas de la matemática y sus aplicaciones. Una razón es que las matrices simétricas aparecen naturalmente en muchos contextos. Buscar información sobre las aplicaciones de las matrices simétricas y del teorema 4.1

4.2 Descomposición en valores singulares

Presentaremos un resultado general acerca de la estructura de matrices reales o complejas cualesquiera, la descomposición en valores singulares. Nos referiremos a ella por su sigla en inglés SVD, de *singular value decomposition*.

Nota Histórica 4.2. *La descomposición en valores singulares fue descubierta para matrices cuadradas en la segunda mitad del siglo XIX por Beltrami y Jordan. A pesar de esto, no llegó a ser ampliamente conocida hasta los años 60 del siglo XX, en que Golub y otros autores mostraron que la SVD puede emplearse eficazmente en el análisis numérico. De hecho, la SVD interviene en algoritmos para calcular el rango*

de una matriz, encontrar bases de su núcleo e imagen, resolver problemas de mínimos cuadrados, etcétera. En la actualidad continúa cobrando importancia, de la mano de sus aplicaciones para comprender la estructura de grandes conjuntos de datos.

Ejemplo 4.13. Como hemos visto reiteradas veces, una matriz M real 2×2 define una transformación en el plano \mathbb{R}^2 :

$$X \in \mathbb{R}^2 \mapsto MX \in \mathbb{R}^2.$$

Esta transformación queda determinada por su acción sobre la circunferencia unidad S^1 formada por los vectores de módulo 1 (ver el ejercicio 3.17, página 85). En la figura 4.4 aparecen representadas S^1 , y su imagen por la matriz

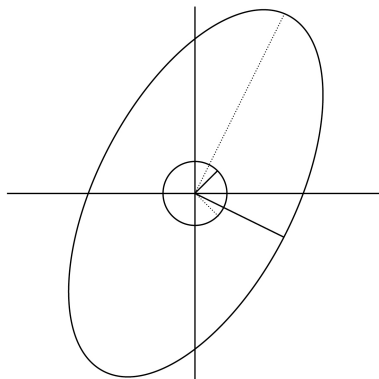


FIGURA 4.4. S^1 y su imagen por M

$$(4.22) \quad M = \begin{bmatrix} 4 & 0 \\ 3 & -5 \end{bmatrix}.$$

Esta imagen, el conjunto formado por todos los vectores MX con $X \in S^1$, es una elipse, cuyos semiejes mayores son

$$(4.23) \quad \pm \begin{bmatrix} 2\sqrt{2} \\ 4\sqrt{2} \end{bmatrix} = \pm M \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix},$$

en tanto que los menores son

$$(4.24) \quad \pm \begin{bmatrix} 2\sqrt{2} \\ -\sqrt{2} \end{bmatrix} = \pm M \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}.$$

Los semiejes de la elipse son un par de vectores ortogonales, que provienen de transformar un par de vectores ortogonales de \mathbb{R}^2 . Esto no es para nada casual, como discutiremos con detalle en breve.

Tal vez la manera menos sofisticada de llegar a las conclusiones del ejemplo 4.13 sea representar los transformados por M de muchos vectores de S^1 . Así se obtuvo la elipse en la figura 4.4. Un segundo procedimiento está esbozado en el siguiente ejercicio, que nos remite al mundo del cálculo diferencial.

Ejercicio 4.23. Usar que cada vector $X \in S^1$ es de la forma $(\cos \theta, \sin \theta)$ para algún valor de $\theta \in \mathbb{R}$, y hallar el módulo $|MX|$ en función de θ . Encontrar los valores de θ en los que $|MX|$ alcanza sus valores máximo y mínimo e identificar cuáles son los vectores $X \in S^1$ a los que corresponden esos valores.

Los valores y vectores propios de M poco ayudan a entender la geometría de la figura 4.4.

Ejercicio 4.24. Hallar los valores y vectores propios de M . Identificar los vectores propios de módulo 1, representarlos y representar sus transformados por M en la figura 4.4.

La clave está en los valores y vectores propios de la matriz simétrica $M^\top M$, tal como se discute en nuestro próximo ejemplo.

Ejemplo 4.14. Los semiejes mayores y menores de la elipse en la figura 4.4 son los más “largos” y los más “cortos” entre los transformados MX de vectores de S^1 . Al calcular los cuadrados $|MX|^2$ de las longitudes $|MX|$ reencontramos la forma cuadrática del ejemplo 4.3, página 110, con matriz simétrica

$$M^\top M = \begin{bmatrix} 25 & -15 \\ -15 & 25 \end{bmatrix},$$

que alcanza sus valores máximo 40 y mínimo 10 sobre los vectores propios de $M^\top M$, que aparecen en los miembros de la derecha de 4.23 y 4.24 respectivamente. Observemos que $\|M\|_2 = 4\sqrt{10}$.

Los resultados de los ejemplos (4.13) y (4.14) se extienden a matrices reales cualesquiera.

Proposición 4.10. *Sea M una matriz real $m \times n$. Entonces existe una base ortonormal $\mathcal{U} = (U_1, U_2, \dots, U_n)$ de \mathbb{R}^n tal que la familia*

$$(4.25) \quad (MU_1, MU_2, \dots, MU_n)$$

es ortogonal.

Demostración. La matriz $M^\top M$ es simétrica, por lo que tiene una base ortonormal \mathcal{U} de vectores propios U_i , $i = 1, \dots, n$, con valores propios λ_i . Entonces

$$(4.26) \quad (MU_i) \cdot (MU_j) = (M^\top MU_i) \cdot U_j = \lambda_i U_i \cdot U_j = \lambda_i \delta_{ij}, \quad i, j = 1, \dots, n.$$

Estas igualdades implican que los vectores MU_i son dos a dos ortogonales. \square

De (4.26) deducimos también $0 \leq |MU_i|^2 = \lambda_i$. Por lo tanto

$$(4.27) \quad |MU_i| = \sqrt{\lambda_i}, \quad i = 1, \dots, n.$$

La familia ortogonal (4.25) genera a la imagen de M . Si el rango de M es k entonces sólo k de los vectores que la componen pueden ser no nulos y por lo tanto sólo k de los números (4.27) son no nulos. Llamaremos σ_i a estos k números positivos en (4.27). Es estándar elegir \mathcal{U} ordenada de manera tal que los σ_i van decreciendo. Con esta convención, introducimos la siguiente definición:

Definición 4.11. Valores singulares. A los números

$$\sigma_i, \quad i = 1, \dots, k,$$

se les llama los *valores singulares* de la matriz M .

Observación 4.2. Según la definición 4.11 los valores singulares son números positivos. Son justamente las raíces cuadradas positivas de todos los valores propios no nulos de $M^\top M$. Algunas referencias, por ejemplo [9], incluyen al cero entre los valores singulares cuando el rango k de M es menor que n . Las dos opciones son posibles y pueden encontrarse en la literatura.

Llamaremos *multiplicidad* de un valor singular σ_i de M a la multiplicidad de σ_i^2 como valor propio de $M^\top M$.

Ejercicio 4.25. ¿Es necesario especificar si nos estamos refiriendo a la multiplicidad algebraica o a la multiplicidad geométrica de los valores propios de $M^\top M$? ¿Por qué?

La discusión que precede a la definición 4.11 implica la siguiente proposición.

Proposición 4.12. Valores singulares y rango. *Una matriz tiene tantos valores singulares, contados con su multiplicidad, como su rango.*

Ejemplo 4.15. Tomemos la matriz 2×3 de rango 1

$$M = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix}.$$

Los valores propios de $M^\top M$ son 15 y 0, un valor propio doble. Una base ortonormal que diagonaliza $M^\top M$, es

$$(U_1, U_2, U_3) = \left((1/\sqrt{3})(1, 1, 1), (1/\sqrt{2})(1, -1, 0), (1/\sqrt{6})(1, 1, 2) \right).$$

El único valor singular de M es

$$\sigma_1 = \sqrt{15} = |MU_1| = |(2\sqrt{3}, \sqrt{3})|.$$

La imagen por M de cualquier vector ortogonal a U_1 es el vector nulo de \mathbb{R}^2 .

Teorema 4.13. Versión vectorial de la SVD.

Sean M una matriz real $m \times n$ de rango k y σ_i , $i = 1, \dots, k$, sus valores singulares. Entonces existen bases ortonormales

$$\mathcal{U} = (U_1, U_2, \dots, U_n), \quad \mathcal{V} = (V_1, V_2, \dots, V_m)$$

de \mathbb{R}^n y \mathbb{R}^m respectivamente, tales que

$$(4.28) \quad MU_i = \begin{cases} \sigma_i V_i, & i = 1, 2, \dots, k, \\ 0, & i = k + 1, \dots, n. \end{cases}$$

Demostración. Si el rango de M es k , consideremos una base ortonormal \mathcal{U} de \mathbb{R}^n como en la proposición 4.10, ordenada en forma decreciente según $|MU_i|$. Entonces, los primeros k vectores U_i no están en el núcleo de M y satisfacen

$$\sigma_i = |MU_i| > 0.$$

Normalizando definimos los vectores

$$V_i = \sigma_i^{-1} MU_i.$$

Por su construcción, los vectores V_i forman una base ortonormal de la imagen de M , que puede extenderse a una base ortonormal \mathcal{V} de \mathbb{R}^m . Las bases \mathcal{U} y \mathcal{V} satisfacen el enunciado del teorema. \square

Ejemplo 4.16. Para la matriz M en (4.22) podemos elegir

$$\mathcal{U} = \left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right), \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right) \right), \quad \mathcal{V} = \left(\left(\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}} \right), \left(\frac{2}{\sqrt{5}}, -\frac{1}{\sqrt{5}} \right) \right).$$

Los valores singulares de M son $\sigma_1 = 10\sqrt{2}$ y $\sigma_2 = 5\sqrt{2}$.

Ejercicio 4.26. Mostrar que las únicas bases ortonormales de \mathbb{R}^2 que son transformadas por M en conjuntos ortonormales son las que se obtienen de \mathcal{U} haciendo modificaciones triviales, como multiplicar vectores por ± 1 o intercambiar el orden de los vectores de la base.

4.2.1 Expresión matricial de la SVD

El teorema 4.13 admite una expresión matricial, como una factorización de la matriz M .

Teorema 4.14. Descomposición en valores singulares.

Sea M una matriz real $m \times n$ de rango k . Entonces existen matrices ortogonales U y V , y una matriz $m \times n$

$$\Sigma = \begin{bmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_k & \\ & & & \end{bmatrix},$$

tales que M admite la factorización

$$(4.29) \quad M = V \Sigma U^\top.$$

Observación 4.3. La matriz Σ tiene sus coeficientes nulos, salvo las primeras k entradas de la diagonal, en la que aparecen los valores singulares σ_i de M .

Demostración. Sean U y V las matrices cuyas columnas son los vectores de las bases ortonormales \mathcal{U} y \mathcal{V} del teorema 4.13. Las relaciones 4.28 pueden resumirse en una única expresión matricial

$$(4.30) \quad MU = V\Sigma.$$

Multiplicando (4.30) a la derecha por la matriz ortogonal U^\top se obtiene (4.29). \square

Ejemplo 4.17. La escritura matricial de los ejemplos 4.13 y 4.14, es

$$(4.31) \quad \begin{bmatrix} 4 & 0 \\ 3 & -5 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ 2/\sqrt{5} & -1/\sqrt{5} \end{bmatrix} \begin{bmatrix} 2\sqrt{10} & \\ & \sqrt{10} \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}.$$

Ejercicio 4.27. Verificar los detalles, realizando los cálculos.

Ejercicio 4.28. Hallar la expresión matricial de la SVD para

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1/\sqrt{5} & -2/\sqrt{5} \\ 2/\sqrt{5} & 1/\sqrt{5} \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 4 & 3 \\ 0 & -5 \end{bmatrix},$$

para la matriz

$$\begin{bmatrix} 4 & -3 \\ 0 & -5 \\ 1 & -2 \end{bmatrix},$$

del ejercicio 3.67, página 105, y para la matriz M del ejemplo 4.15.

Ejercicio 4.29. ¿Es única la descomposición (4.29) de una matriz M ? Si no lo es, ¿es posible dar una descripción de todas las posibilidades?

Observación 4.4. Los procedimientos de cálculo de la SVD que empleamos en este texto sólo funcionan eficientemente para matrices M de rango 1 o 2, o con un buen número de valores propios de $M^\top M$ evidentes. En la práctica hay que trabajar de otra manera. Recomendamos al lector interesado consultar algún texto de álgebra lineal numérica, como, por ejemplo, [17].

4.2.2 La imagen de S^{n-1} por una matriz cualquiera

Para recuperar el significado geométrico de estos resultados estudiaremos como una matriz M transforma a la esfera unidad S^{n-1} formada por todos los vectores de módulo 1 de \mathbb{R}^n . Encontraremos que S^{n-1} se transforma en un elipsoide, o en un elipsoide y su interior. Nuestro tratamiento general incluye los casos particulares $n = 2$ y $n = 3$ que corresponden al plano y al espacio, donde la geometría del problema es más evidente.

Teorema 4.15. *Sea M una matriz $m \times n$ de rango k . Sea \mathcal{V} la base ortonormal de \mathbb{R}^n que aparece en el enunciado del teorema 4.13. Sea $E \subset \mathbb{R}^m$ la imagen por M de S^{n-1} . Indicaremos con $Z = (z_1, \dots, z_m)$ los vectores de coordenadas de los vectores de \mathbb{R}^m respecto a la base \mathcal{V} . Entonces*

1. Si $k = n$ el conjunto E es el elipsoide en \mathbb{R}^n cuyos semiejes principales son los primeros n vectores de \mathcal{V} , y caracterizado por la ecuación

$$(4.32) \quad \frac{z_1^2}{\sigma_1^2} + \frac{z_2^2}{\sigma_2^2} + \cdots + \frac{z_n^2}{\sigma_n^2} = 1;$$

2. Si $k < n$ el conjunto E es la unión del elipsoide contenido en $\text{im}(M)$, cuyos semiejes principales son los primeros k vectores de \mathcal{V} , con su interior. En este caso E está formado por los vectores de \mathbb{R}^n cuyas primeras k coordenadas respecto a \mathcal{V} satisfacen la inecuación

$$(4.33) \quad \frac{z_1^2}{\sigma_1^2} + \frac{z_2^2}{\sigma_2^2} + \cdots + \frac{z_k^2}{\sigma_k^2} \leq 1,$$

y cuyas últimas $n - k$ coordenadas son nulas:

$$(4.34) \quad z_{k+1} = \cdots = z_n = 0.$$

Demostración. Un vector Y pertenece a E si y sólo si existe un vector $X \in S^{n-1}$ tal que

$$Y = MX = V\Sigma U^\top X.$$

Lo que es equivalente a que

$$(4.35) \quad V^\top Y = \Sigma U^\top X.$$

Llamando $Z = V^\top Y$ y $T = U^\top X$ a las coordenadas de Y y X respecto a \mathcal{V} y \mathcal{U} , la igualdad (4.35) toma la forma

$$(4.36) \quad Z = \Sigma T.$$

Al variar X en S^{n-1} los vectores T también recorren S^{n-1} , porque el cambio de coordenadas es invertible. Concluimos que un vector $Y \in E$ si y sólo si existe $T \in S^{n-1}$ tal que satisface (4.36). Si $k = n$,

$$(4.37) \quad z_1 = \sigma_1 t_1, \dots, z_n = \sigma_n t_n.$$

Entonces

$$\frac{z_1^2}{\sigma_1^2} + \cdots + \frac{z_n^2}{\sigma_n^2} = t_1^2 + \cdots + t_n^2 = 1.$$

Recíprocamente, si las coordenadas Z de Y respecto a \mathcal{V} satisfacen (4.32), entonces Y es la imagen del punto $X \in S^{n-1}$ cuyas coordenadas T respecto a \mathcal{U} satisfacen (4.37).

Si $k < n$ tenemos

$$(4.38) \quad z_1 = \sigma_1 t_1, \dots, z_k = \sigma_k t_k, z_{k+1} = 0, \dots, z_n = 0$$

por lo que

$$\frac{z_1^2}{\sigma_1^2} + \cdots + \frac{z_k^2}{\sigma_k^2} = t_1^2 + \cdots + t_k^2 \leq 1.$$

Recíprocamente, si las coordenadas Z de Y respecto a \mathcal{V} satisfacen (4.33) y (4.34), entonces cualquier elección de

$$T = (t_1, \dots, t_k, t_{k+1}, \dots, t_n)$$

que haga que se satisfagan (4.38) y que T esté en S^{n-1} corresponde a las coordenadas respecto a \mathcal{U} de un vector $X \in S^{n-1}$ tal que $MX = Y$. \square

Ejemplo 4.18. En este ejemplo daremos los detalles que están por detrás de la figura 4.4, que muestra la imagen de la circunferencia unidad $S^1 \subset \mathbb{R}^2$ por la matriz M en (4.22). Al escribir el producto MX en la forma (4.35), a partir de la descomposición (4.31) obtenemos

$$\begin{bmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ 2/\sqrt{5} & -1/\sqrt{5} \end{bmatrix} \begin{bmatrix} 4 & 0 \\ 3 & -5 \end{bmatrix} X = \begin{bmatrix} 2\sqrt{10} & \\ & \sqrt{10} \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix},$$

que puede escribirse en forma de las dos ecuaciones escalares

$$(4.39) \quad \begin{cases} z_1 = 2\sqrt{10}t_1, \\ z_2 = \sqrt{10}t_2, \end{cases}$$

donde $Z = (z_1, z_2)$ y $T = (t_1, t_2)$ son, respectivamente, coordenadas de $Y = MX$ y de X respecto a las bases en que se obtiene la SVD de la matriz M . Tenemos entonces que los vectores MX satisfacen

$$(4.40) \quad \frac{z_1^2}{40} + \frac{z_2^2}{10} = t_1^2 + t_2^2 = 1.$$

Esto se puede escribir en la variable Y , usando que

$$Z = \begin{bmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \end{bmatrix} Y \Rightarrow \begin{cases} z_1 = \frac{1}{\sqrt{5}}y_1 + \frac{2}{\sqrt{5}}y_2, \\ z_2 = \frac{2}{\sqrt{5}}y_1 - \frac{1}{\sqrt{5}}y_2. \end{cases}$$

Sustituyendo encontramos que en las variables (y_1, y_2) la ecuación (4.40) toma el aspecto

$$(4.41) \quad (y_1 + 2y_2)^2 + 4(2y_1 - y_2)^2 = 200.$$

Todavía pueden desarrollarse los cuadrados en (4.41) para pasar a la fórmula

$$(4.42) \quad 17y_1^2 - 12y_1y_2 + 8y_2^2 = 200,$$

tan sencilla como inconveniente, porque dificulta el reconocimiento de que el conjunto de puntos que describe es una elipse.

Ejercicio 4.30. Mostrar que los vectores

$$Y = \pm(2\sqrt{2}, 4\sqrt{2}), \quad Y = \pm(2\sqrt{2}, -\sqrt{2}),$$

de las fórmulas (4.23) y (4.24), y los vectores $Y = Me_1$ e $Y = Me_2$, satisfacen las ecuaciones (4.41)-(4.42). Con e_1 y e_2 indicamos a los vectores de la base canónica de \mathbb{R}^2 .

Ejemplo 4.19. La matriz

$$M = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix}$$

tiene una descomposición en valores singulares $M = V\Sigma U^\top$, con

$$V = \begin{bmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{bmatrix}, \quad \Sigma = M = \begin{bmatrix} \sqrt{15} & & \\ & & \end{bmatrix}, \quad U = \begin{bmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & -\frac{2}{\sqrt{6}} \end{bmatrix}.$$

Los vectores $Y = MX$ satisfacen entonces

$$(4.43) \quad \begin{cases} \frac{2}{\sqrt{5}}y_1 + \frac{1}{\sqrt{5}}y_2 = z_1 = \sqrt{15}t_1, \\ \frac{1}{\sqrt{5}}y_1 - \frac{2}{\sqrt{5}}y_2 = z_2 = 0. \end{cases}$$

La primera ecuación en (4.43) implica que están en el subespacio $y_1 = 2y_2$, generado por cualquiera de las columnas $[1 \ 2]^\top$ de la matriz M . Dado que t_1 toma valores en $[-1, 1]$, la segunda ecuación tiene como consecuencia que para cualquier vector (y_1, y_2) en la imagen de S^1 se tiene

$$-5\sqrt{3} \leq 2y_1 + y_2 = 5y_2 = 5y_1/2 \leq 5\sqrt{3}.$$

La imagen de S^1 es entonces el segmento sobre la recta de ecuación $y_1 = 2y_2$, con extremos $\pm(2\sqrt{3}, \sqrt{3})$.

Ejercicio 4.31. Hallar los vectores X tales que $MX = \pm(2\sqrt{3}, \sqrt{3})$.

Ejercicio 4.32. Hallar las imágenes de la esfera unidad para las matrices del ejercicio 4.28. Para la matriz M del ejemplo 4.15 encontrar para cada vector en la imagen de S^2 todas sus preimágenes en S^2 .

4.2.3 Ejercicios adicionales

Ejercicio 4.33. Para cada valor de ϵ hallar la descomposición en valores singulares de

$$M = \begin{bmatrix} 2 + 2\epsilon & -2 + 2\epsilon \\ 4 - \epsilon & -4 - \epsilon \end{bmatrix}.$$

Estudiar cómo varía con ϵ la imagen de S^1 en el plano \mathbb{R}^2 .

El próximo ejercicio muestra lo inestable que pueden ser las soluciones de un problema tan sencillo como es un sistema lineal de dos ecuaciones con dos incógnitas.

Ejercicio 4.34.

1. Resolver el sistema de ecuaciones lineales

$$\begin{cases} 2,002x_1 - 1,998x_2 = 4, \\ 3,998x_1 - 4,001x_2 = 8. \end{cases}$$

2. Resolver el sistema de ecuaciones lineales

$$\begin{cases} 2,002x_1 - 1,998x_2 = 4,4, \\ 3,998x_1 - 4,001x_2 = 7,8, \end{cases}$$

pero antes de hacer los cálculos conjeturar una aproximación para los valores de su solución, a partir de los resultados de la parte 1.

3. Comparar la estimación hecha en la parte 2 con la verdadera solución. ¿Puede explicar lo que ha observado? Buscar interpretaciones algebraicas y geométricas. Sugerencia: la matriz de los sistemas de ecuaciones de este ejercicio es la matriz M del ejercicio 4.33 con $\epsilon = 10^{-3}$.

Los resultados del ejercicio 4.34 están relacionados con el *número de condición* de la matriz del sistema, un importante concepto que el lector puede encontrar desarrollado en la monografía [15].

Ejercicio 4.35. Hallar dos matrices 2×2 diferentes tales que su imagen de la esfera unidad sea la elipse de ecuación $3x^2 + 3y^2 + 2xy = 1$.

Ejercicio 4.36. Sea M una matriz $n \times n$. Mostrar que M es ortogonal si y sólo si la imagen por M de S^{n-1} es S^{n-1} .

Ejercicio 4.37. DESCOMPOSICIÓN POLAR. Demostrar que toda matriz cuadrada M se puede factorizar en la forma $M = RU$, donde R es una matriz simétrica con todos sus valores propios mayores o iguales que cero, y U una matriz ortogonal.

4.3 Extensiones y aplicaciones de la SVD

El principal objetivo de esta sección es mostrar las ideas básicas que subyacen en algunas variantes y en importantes aplicaciones de la SVD. Ilustraremos con una familia de ejemplos en dimensiones muy bajas, como las ideas geométricas contenidas en la SVD, pueden dar luz sobre transformaciones que tienen lugar en el plano o en el espacio tridimensional. Luego veremos como esas mismas ideas geométricas pueden extrapolarse para comprender diversos problemas en espacios de dimensión arbitrariamente alta.

Ejemplo 4.20. Para cada valor de $\epsilon \in [0, 1]$ la descomposición en valores singulares de la matriz

$$(4.44) \quad M = \begin{bmatrix} -1 + 2\epsilon & 2 + \epsilon \\ -1 - 2\epsilon & 2 - \epsilon \\ 2 & -4 \end{bmatrix}$$

es $M = V\Sigma U^\top$ con

$$(4.45) \quad \Sigma = \begin{bmatrix} \sqrt{30} & 0 \\ 0 & \epsilon\sqrt{10} \\ 0 & 0 \end{bmatrix}, \quad U = \begin{bmatrix} -\frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \end{bmatrix}, \quad V = \begin{bmatrix} \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ -\frac{2}{\sqrt{6}} & 0 & \frac{1}{\sqrt{3}} \end{bmatrix},$$

Ejercicio 4.38. Completar los detalles del cálculo de la descomposición en valores singulares de M .

En la figura 4.5 ilustramos como al cambiar ϵ varía en \mathbb{R}^3 la imagen por M de la circunferencia unidad $S^1 \subset \mathbb{R}^2$, representándola para los valores $\epsilon = 1, 1/4, 1/10, 0$.

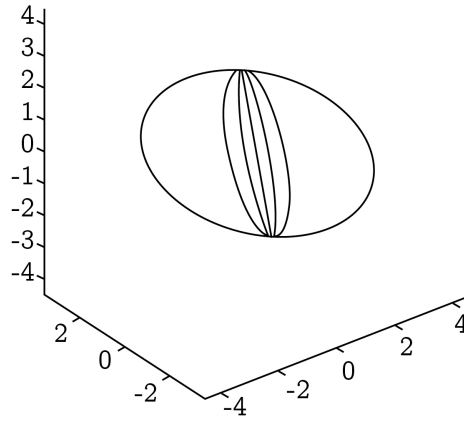


FIGURA 4.5. La imagen de S^1 variando con ϵ .

4.3.1 Formas reducidas de la SVD

Al calcular la SVD de las matrices M en (4.44), en los productos $V\Sigma$ la tercera columna de V siempre aparece multiplicada por ceros. Si eliminamos de Σ la fila de ceros y de V su tercera columna obtenemos

$$\tilde{\Sigma} = \begin{bmatrix} \sqrt{30} & 0 \\ 0 & \epsilon\sqrt{10} \end{bmatrix}, \quad \tilde{V} = \begin{bmatrix} 1/\sqrt{6} & 1/\sqrt{2} \\ 1/\sqrt{6} & -1/\sqrt{2} \\ -2/\sqrt{6} & 0 \end{bmatrix}.$$

Esto es suficiente para reconstruir M como

$$A = \tilde{V}\tilde{\Sigma}U^\top.$$

Las dos columnas de \tilde{V} bastan para generar $\text{im}(M)$. La tercera columna de V está en $\text{im}(M)^\perp$ y no aporta nada al conocimiento de M . Esta discusión se puede generalizar a una nueva factorización de matrices cualesquiera.

Ejercicio 4.39. Sea M una matriz $m \times n$ de rango k . Mostrar que existen matrices \tilde{U} y \tilde{V} , $n \times k$ y $m \times k$ respectivamente, cuyas columnas forman familias ortonormales en \mathbb{R}^n y \mathbb{R}^m , y una matriz cuadrada $k \times k$, diagonal, de rango k ,

$$\tilde{\Sigma} = \begin{bmatrix} \sigma_1 & & \\ & \ddots & \\ & & \sigma_k \end{bmatrix}$$

que tiene en su diagonal a los valores singulares de M , tales que

$$(4.46) \quad M = \tilde{V}\tilde{\Sigma}\tilde{U}^\top.$$

La descomposición (4.46) recibe el nombre de *forma reducida* de la SVD.

Ejercicio 4.40. Hallar la forma reducida de la SVD para la matriz que se obtiene tomando $\epsilon = 0$ en (4.44).

Observación 4.5. SVD Y LOS CUATRO SUBESPACIOS. En la forma

$$M = V\Sigma U^\top$$

de la SVD con matrices U y V ortogonales, las primeras k columnas de V forman una base ortogonal de $\text{im}(M)$ y las últimas $n - k$ una base ortonormal de $\text{im}(M)^\perp$. Las últimas $m - k$ columnas de U forman una base del núcleo de M , y las primeras k una base de $\ker(M)^\perp$. Cuando la SVD se escribe en su forma reducida las columnas que se eliminan de U y V están en el núcleo y en el complemento ortogonal de la imagen de M , por lo que no aportan a la reconstrucción de M .

Ejercicio 4.41. A partir de las descomposiciones de M hallar la SVD y la SVD reducida de M^\top . Investigar que relación tiene este resultado, la observación 4.5 y las relaciones entre los subespacios asociados con M que se discuten en la sección 3.2.4, página 92.

4.3.2 Aproximaciones por matrices de menor rango y $\|\cdot\|_2$

El mayor valor singular de una matriz $m \times n$ es la mayor dilatación que la matriz produce sobre los vectores de \mathbb{R}^n al multiplicarlos y transformarlos en vectores de \mathbb{R}^m . Vimos en la sección 1.3.4 que la máxima dilatación define una norma, la norma $\|\cdot\|_2$, en el espacio de las matrices. Relacionando estos conceptos obtenemos nuestra próxima proposición (ver también el corolario 4.5, página 115).

Proposición 4.16. $\|M\|_2 = \sigma_1$, donde σ_1 es el mayor valor singular de M .

Ejemplo 4.21. Las matrices (4.44) están escritas de una forma que hace evidente que cuando ϵ es pequeño pueden aproximarse por

$$(4.47) \quad M_1 = \begin{bmatrix} -1 & 2 \\ -1 & 2 \\ 2 & -4 \end{bmatrix},$$

que es una matriz de rango 1.

Para matrices cualesquiera es difícil conseguir un resultado de este tipo por una inspección directa, pero puede obtenerse de la SVD. Lo mostraremos primero para M . La SVD de M es $M = V\Sigma U^\top$ con la matriz

$$\Sigma = \begin{bmatrix} \sqrt{30} & 0 \\ 0 & \epsilon\sqrt{10} \\ 0 & 0 \end{bmatrix}$$

en (4.45). La SVD de M_1 es $M_1 = V\Sigma_1U^\top$, donde

$$\Sigma_1 = \begin{bmatrix} \sqrt{30} & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

se obtiene de Σ conservando sólo el primer valor singular $\sigma_1 = \sqrt{30}$, que para $\epsilon \simeq 0$ es mucho más grande que $\sigma_2 = \epsilon\sqrt{10}$.

Notemos además que

$$M - M_1 = V(\Sigma - \Sigma_1)U^\top$$

es esencialmente la SVD de la diferencia entre M y M_1 , y que $\epsilon\sqrt{10}$ es el mayor valor singular de esta diferencia. Por lo tanto

$$\|M - M_1\|_2 = \epsilon\sqrt{10}.$$

En la proposición 4.17 veremos que no hay una mejor aproximación de M respecto a $\|\cdot\|_2$ por matrices de rango 1.

La SVD sugiere un procedimiento para aproximar una matriz M de rango k por matrices de rango menor, conservando en la matriz Σ de su SVD sólo algunos valores singulares. Para $j \leq k$ definimos entonces

$$(4.48) \quad \Sigma_j = \begin{bmatrix} \sigma_1 & & & \\ & \ddots & & \\ & & \sigma_j & \\ & & & \end{bmatrix},$$

y $M_j = V\Sigma_jU^\top$

Proposición 4.17. *Sea M una matriz $m \times n$ de rango k . Para cada $j \leq k$, la matriz M_j es la mejor aproximación de M entre las matrices de rango menor o igual que j , en el sentido de que si N es una matriz de rango menor o igual que j se tiene*

$$\sigma_{j+1} = \|M - M_j\|_2 \leq \|M - N\|_2$$

Demostración. Que $\sigma_{j+1} = \|M - M_j\|_2$ es una consecuencia directa de

$$M - M_j = V(\Sigma - \Sigma_j)U^\top$$

y la proposición 4.16.

Supongamos ahora que existe una matriz N de rango menor o igual que j tal que $\|M - N\|_2 < \sigma_{j+1}$. Comencemos por observar que en el subespacio \mathbb{S}_{j+1} generado por las primeras $j+1$ columnas de U

$$|MX| \geq \sigma_{j+1}|X|.$$

Este espacio tiene dimensión $j+1$. Por otra parte el núcleo de N tiene dimensión mayor o igual que $n-j$. Debe haber entonces un vector X no nulo que pertenezca a la vez a $\ker(N)$ y a \mathbb{S}_{j+1} . Para ese vector se tiene

$$\sigma_{j+1}|X| > \|M - N\|_2|X| \geq |(M - N)X| = |MX| \geq \sigma_{j+1}|X|.$$

Esta contradicción completa la prueba. \square

Hay situaciones en que los valores singulares decaen rápidamente, y bastan unos pocos de ellos para conseguir una muy buena aproximación M_j a M . Observemos que para conocer M completamente hace falta conocer sus $m \times n$ coeficientes. Para reconstruir M_j solo hacen falta $j(m + n + 1)$ datos. Si m y n son grandes y j es pequeño, entonces $j(m + n + 1)$ es mucho más pequeño que mn , y se logra entonces una compresión significativa del volumen de información necesario para tener una buena reconstrucción de M .

Ejemplo 4.22. Ilustraremos la proposición 4.17 con un ejemplo del área de procesamiento de imágenes. La figura 4.6 es una representación en valores de gris de los coeficientes de una matriz 100×200 . En la figura 4.7 aparece el gráfico de los 100

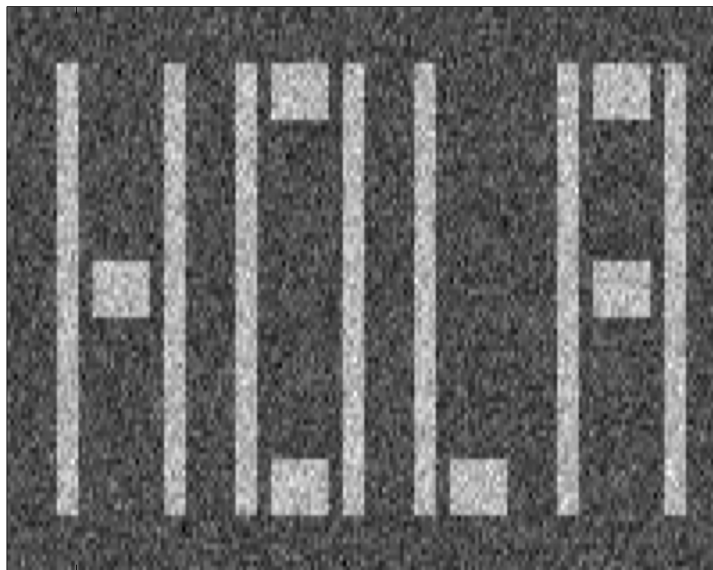


FIGURA 4.6. Un “HOLA” algo ruidoso

valores singulares de la matriz. Los cuatro primeros valores singulares son significativamente mayores que el resto. Con ellos generamos una aproximación de rango 4 de la matriz original, que representamos como imagen en la figura 4.8. Observemos que la reconstrucción de rango 4 devuelve con nitidez la estructura de la imagen original, eliminando buena parte del ruido que contenía. El procedimiento puede verse a la vez como un mecanismo de compresión (en la matriz original están almacenados $100 \times 200 = 20,000$ números, pero para la reconstrucción de rango 4 sólo hace falta conocer $4 \times (1 + 100 + 200) = 1204$) y de filtrado de ruido.

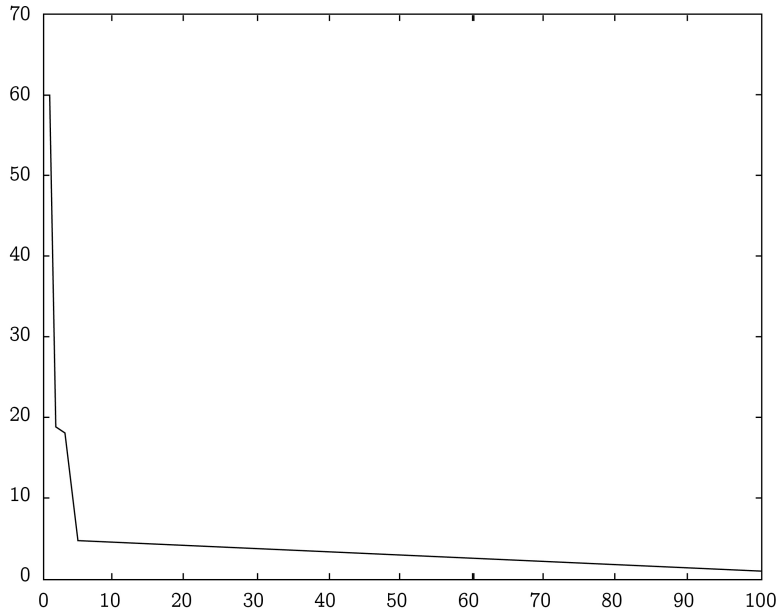


FIGURA 4.7. Los valores singulares del “HOLA” algo ruidoso

Ejercicio 4.42. ¿Puede explicar en términos de las imágenes por qué los valores singulares decaen abruptamente luego del cuarto?, ¿qué ha ocurrido en el proceso de aproximación de la imagen a partir de la SVD?

4.3.3 SVD y reducción de dimensionalidad

En esta sección y la siguiente aportaremos nuevas miradas sobre la SVD, para interpretarla como un procedimiento que ayuda a poner en claro la estructura de conjuntos de datos. Volvamos sobre nuestro ejemplo básico.

Ejemplo 4.23. Para $\epsilon > 0$ pero pequeño las columnas de las matrices

$$M = \begin{bmatrix} -1 + 2\epsilon & 2 + \epsilon \\ -1 - 2\epsilon & 2 - \epsilon \\ 2 & -4 \end{bmatrix}$$

generan un espacio de dimensión 2 en \mathbb{R}^3 , pero están muy cerca de estar alineadas en un espacio de dimensión 1. La descomposición en valores singulares refleja esto. Escribamos la descomposición en valores singulares $M = V\Sigma U^T$ en la forma de la

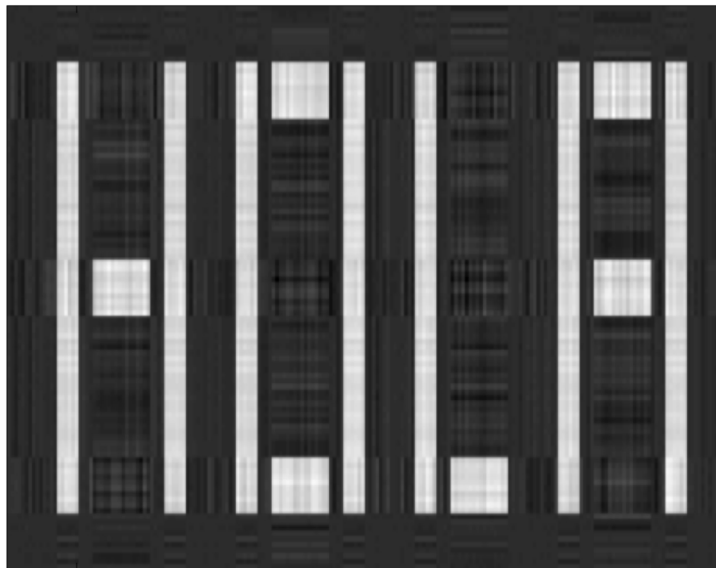


FIGURA 4.8. Reconstrucción de rango 4 del “HOLA” ruidoso

factorización $M = VW$, con

$$(4.49) \quad W = \Sigma U^\top = \begin{bmatrix} -\sqrt{6} & 2\sqrt{6} \\ 2\epsilon\sqrt{2} & \epsilon\sqrt{2} \\ 0 & 0 \end{bmatrix},$$

y llamemos $\mathcal{V} = (V_1, V_2, V_3)$ a la base de \mathbb{R}^3 formada por las columnas de V . La fórmula (4.49) contiene la expresión de las columnas de M como combinaciones lineales de \mathcal{V} . La contribución de V_3 es nula, y cuando $\epsilon \simeq 0$ la de V_2 es despreciable frente a la de V_1 . El grueso de la información de las columnas de M está entonces almacenado en V_1 y en la primera fila de W .

Cuando los primeros r valores singulares de una matriz M son mucho más grandes que los siguientes, sus columnas están concentradas cerca del subespacio de dimensión r generado por las r primeras columnas de la matriz V en la SVD de M . Cuando r es mucho menor que m y n la SVD permite explicar en términos de un número relativamente pequeño de parámetros, r , datos que en principio pueden tener una dimensionalidad muy alta.

Observación 4.6. En un mundo lleno de un enorme volumen de datos (información estadística de todo tipo, resultados de observaciones de experimentos, imágenes, grabaciones de sonido, etcétera) que se almacenan en registros gigantescos, la búsqueda

de herramientas para comprimir e interpretar esta información es un problema candente de la ciencia contemporánea. Es así que las técnicas que hemos presentado en esta sección tienen un papel importante en áreas tan diversas como la estadística, el procesamiento de imágenes, el reconocimiento del habla, el estudio de proteínas y la inteligencia artificial. Estas ideas de *reducción de dimensionalidad* están fuertemente relacionadas con el *análisis de componentes principales*, que se discute en la monografía [10].

4.3.4 SVD y problemas de mínimos cuadrados

La descomposición en valores singulares también permite tratar problemas de mínimos cuadrados.

Ejemplo 4.24. Volvamos al sistema $MX = Y$, con

$$M = \begin{bmatrix} 1 & 3 \\ -3 & 1 \\ 2 & -4 \end{bmatrix}, \quad Y = \begin{bmatrix} 4, 1 \\ -1, 9 \\ -1, 9 \end{bmatrix},$$

que estudiamos en los ejemplos 3.14, 3.15 y 3.16 de la sección 3.4. La matriz M es (4.44) con $\epsilon = 1$. Por lo tanto conocemos su SVD $M = V\Sigma U$. Escribimos entonces el sistema $MX = Y$ como

$$V\Sigma U^T X = Y,$$

que es equivalente a

$$\Sigma U^T X = V^T Y.$$

Notemos que $U^T X$ son las coordenadas de X en la base \mathcal{U} , que podemos representar por $X_{\mathcal{U}}$. El producto $V^T Y$ son las coordenadas $Y_{\mathcal{V}}$ de Y en la base \mathcal{V} formadas por las columnas de V . El nuevo sistema puede escribirse

$$\Sigma X_{\mathcal{U}} = Y_{\mathcal{V}}.$$

Como Σ e $Y_{\mathcal{V}}$ son conocidos, llamando $Z = X_{\mathcal{U}}$, tenemos

$$\begin{cases} \sqrt{30}z_1 &= 3\sqrt{6}, \\ \sqrt{10}z_2 &= 4\sqrt{2}, \\ 0 &= -\sqrt{3}. \end{cases}$$

Este sistema es incompatible, a causa de la última ecuación. La explicación es que la tercera columna V_3 de V es ortogonal a la imagen de M , y no hay manera de generar la componente de Y según V_3 haciendo combinaciones lineales de las columnas de M . Este número revela el residuo de nuestra solución. Como el tercer vector de la base \mathcal{V} está normalizado el módulo del residuo será $\sqrt{3}$. Para determinar el vector residuo multiplicamos su coordenada $-\sqrt{3}$ por el tercer vector de la base \mathcal{V} :

$$-\sqrt{3} \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right) = (-1, -1, -1).$$

Los números $3\sqrt{6}$ y $4\sqrt{2}$ son las coordenadas de la proyección de Y sobre la imagen de M . Resolvemos entonces

$$\begin{cases} \sqrt{30}z_1 = 3\sqrt{6}, \\ \sqrt{10}z_2 = 4\sqrt{2}, \end{cases}$$

que tiene como única solución $Z = \left(\frac{3}{\sqrt{5}}, \frac{4}{\sqrt{5}}\right)$. El producto

$$X = UZ = (1, 2)$$

es la solución de $MX = Y$ en el sentido de mínimos cuadrados. Observemos que

$$MX = (7, -1, -6)$$

y el residuo es

$$Y - MX = (-1, -1, -1),$$

un vector ortogonal a las columnas de M , tal como habíamos encontrado.

Ejercicio 4.43. Calcular la solución de mínimos cuadrados de los sistemas

$$M = \left[\begin{array}{cc|c} 4 & -3 & 6 \\ 0 & -4 & -4 \\ 1 & -4 & -4 \end{array} \right], \quad M = \left[\begin{array}{cc|c} 1 & 2 & 3 \\ 1 & 2 & 3, 1 \\ 1 & 2 & 2, 9 \end{array} \right]$$

usando el método basado en la SVD.

Ejercicio 4.44. ¿Qué relación hay entre la SVD como herramienta para resolver problemas de mínimos cuadrados y la observación 4.5, página 131?, ¿qué ocurre al resolver con la SVD un problema $MX = Y$ cuando las columnas de M no son linealmente independientes?

4.3.5 Ejercicios adicionales

Ejercicio 4.45. Sea M una matriz cuadrada e invertible. Dar una expresión para $\|M^{-1}\|_2$ en término de los valores singulares de M .

Ejercicio 4.46. Sea M una matriz $m \times n$ de rango k y $M = V\Sigma U^\top$ su SVD. Llamemos V_i , $i = 1, \dots, n$ a las columnas de V , U_i , $i = 1, \dots, m$ a las columnas de U , y σ_i , $i = 1, \dots, k$, a los valores singulares de M .

1. Mostrar que

$$(4.50) \quad M = \sum_{i=1}^k \sigma_i V_i U_i^\top.$$

2. Mostrar que cada una de las matrices $\sigma_i V_i U_i^\top$ tiene rango 1.

3. Para las matrices M en (4.44) hallar las matrices $\sigma_i V_i U_i^\top$.

4. Mostrar que para cada $j = 1, \dots, k$, la matriz

$$M_j = \sum_{i=1}^j \sigma_i V_i U_i^\top$$

tiene rango j .

Ejercicio 4.47. A partir de (4.50), dar una nueva demostración de que toda matriz M admite una forma reducida de la SVD como en (4.46), con $\tilde{\Sigma}$ cuadrada $k \times k$ e invertible.

Ejercicio 4.48.

1. Mostrar que toda matriz $m \times n$ de rango 1 puede escribirse en la forma VU^\top , donde V y U son vectores de \mathbb{R}^n y \mathbb{R}^m respectivamente. Investigar si esta descomposición es única.
2. Mostrar que una matriz M de rango k puede escribirse como

$$M = \sum_{i=1}^k V_i U_i^\top,$$

donde V_i y U_i son vectores de \mathbb{R}^n y \mathbb{R}^m .

Ejercicio 4.49. Sea M una matriz cuadrada $n \times n$ e invertible y σ_i , $i = 1, \dots, n$ sus valores singulares. Mostrar que si una matriz N cuadrada $n \times n$ no es invertible entonces $\|M - N\|_2 \geq \sigma_n$ y que existe una matriz N no invertible para la que se satisface la igualdad (este resultado significa que el menor valor singular σ_n de una matriz invertible es la distancia, medida en $\|\cdot\|_2$, a las matrices singulares).

Nuestro próximo ejercicio permite demostrar el teorema 4.14 sin recurrir al teorema espectral para matrices simétricas, por medio de un argumento muy geométrico, basado en estudiar la dilatación que M produce sobre los vectores de \mathbb{R}^n .

Ejercicio 4.50. Consideremos una matriz M no nula y $m \times n$.

1. Sea $X \in S^{n-1}$ tal que $|MX| = \|M\|_2$. Mostrar que

$$(4.51) \quad MX \cdot MY = \|M\|_2^2 X \cdot Y$$

se satisface para todo $Y \in \mathbb{R}^n$. Sugerencia: considerar la función auxiliar

$$\varphi(\epsilon) = \frac{|M(X + \epsilon Y)|^2}{|X + \epsilon Y|^2},$$

y usar que tiene un máximo en $\epsilon = 0$.

2. Deducir que si X es como en la parte 1 e Y es ortogonal a X , entonces MY es ortogonal a MX .
3. Completar la demostración del teorema 4.29 usando un argumento inductivo sobre el tamaño de la matriz A , similar al empleado en la demostración del teorema espectral.

Observación 4.7. El argumento empleado en la parte 1 del ejercicio 4.50 es un *argumento variacional*, una técnica estándar para extraer conclusiones acerca de las propiedades de un máximo (mínimo) de una función: consiste en perturbar ligeramente el valor del argumento de la función donde se alcanza el máximo (mínimo) y estudiar qué ocurre. Un ejemplo de este tipo de argumentos es la demostración de que en un máximo (mínimo) local de una función real de variable real diferenciable, la derivada debe anularse. Pero el cálculo de variaciones va mucho más allá de ser una herramienta de demostración de algunos resultados, es un área de la matemática en sí misma, con importantes implicaciones en dominios diversos. Una hermosa referencia que puede permitir al lector acercarse a este mundo es [12].

Ejercicio 4.51. SVD y pseudoinversa. A partir de la forma reducida (4.46) de la SVD de una matriz M definimos

$$M^+ = \tilde{U} \tilde{\Sigma}^{-1} \tilde{V}^\top.$$

A esta matriz se le llama la *pseudoinversa* de M .

1. Mostrar que si M es invertible entonces $M^+ = M^{-1}$;
2. Mostrar que si M es de rango n entonces $M^+ = M(M^\top M)^{-1} M^\top$.

Ejercicio 4.52. Pseudoinversa y mínimos cuadrados. Sean M una matriz $m \times n$ y M^+ su pseudoinversa.

1. Mostrar que si el rango de M es n entonces $X = M^+ Y$ es la única solución de $MX = Y$, en el sentido de mínimos cuadrados.
2. Mostrar que si el rango de M es menor que n entonces $X = M^+ Y$ es la solución de $MX = Y$, en el sentido de mínimos cuadrados, que tiene el menor módulo.
3. Resolver los problemas del ejercicio 4.43 haciendo uso de la pseudoinversa.

Capítulo 5: Cadenas de Markov



El principal objetivo de esta sección es mostrar como la estructura lineal de \mathbb{R}^n interactúa con la geometría inducida por la norma $\|\cdot\|_1$. Los resultados obtenidos pueden aplicarse a las cadenas de Markov, de las que presentamos una introducción en la sección 5.1. En la sección 5.2 usamos un teorema de punto fijo para probar un importante teorema sobre cadenas de Markov, y lo aplicamos al problema del ordenamiento de las páginas de Internet que ya introdujimos y discutimos en la sección 2.1.1.

5.1 Cadenas de Markov

En esta sección presentamos una introducción a las cadenas de Markov, un modelo para fenómenos de evolución. Comenzamos por un ejemplo.

Ejemplo 5.1. Consideremos una población que se divide en dos clases c_1 y c_2 , de la que nos interesa estudiar la evolución en el tiempo del número de individuos en cada clase. Supondremos que medimos el tiempo a intervalos regulares (por ejemplo, cada hora, o cada mes, o cada año), por lo que tomaremos una variable discreta $k = 0, 1, \dots$, para representarlo. En cada instante k el *estado* de la población será un vector

$$X_k = (x_{k,1}, x_{k,2})$$

cuyos coeficientes son, respectivamente, la fracción de individuos en las clases c_1 y c_2 sobre el total de individuos de la población.

El principal ingrediente del modelo son las reglas que regulan las transiciones entre clases. Para este ejemplo, supondremos que en cada unidad de tiempo $1/5$ de los individuos de la clase c_1 pasa a c_2 , y $3/5$ de los de la clase c_2 pasa a c_1 . Por lo tanto $4/5$ y $2/5$ de los de las clases c_1 y c_2 , respectivamente, permanecen en sus clases de origen. Estos datos pueden esquematizarse en la tabla de la figura 5.1. Si

clases	1	2
1	$4/5$	$3/5$
2	$1/5$	$2/5$

FIGURA 5.1. Transiciones en una población.

la distribución $X_k = (x_{k,1}, x_{k,2})$ entre las clases c_1 y c_2 al tiempo k es conocida, ¿cuál será la distribución $X_{k+1} = (x_{k+1,1}, x_{k+1,2})$ una unidad de tiempo después? El producto $(4/5)x_{k,1}$ representa la fracción de individuos en el total de la población que

estaban originalmente en la clase A y permanecieron en ella. En tanto que $(3/5)x_{k,1}$ es la fracción de los que cambiaron a la clase A desde la B . La fracción total $x_{k+1,1}$, de individuos en la clase A al cabo de una unidad de tiempo es la suma

$$x_{k+1,1} = (4/5)x_{k,1} + (3/5)x_{k,1}.$$

Un razonamiento análogo implica

$$x_{k+1,2} = (1/5)x_{k,1} + (2/5)x_{k,1}.$$

El lector reconocerá que ambas ecuaciones pueden resumirse en la igualdad matricial

$$(5.1) \quad X_{k+1} = \begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix} X_k.$$

Los coeficientes de la matriz M que regula las transiciones son justamente las entradas de la tabla 5.1. Las reglas algebraicas del cálculo matricial se adecuan perfectamente a la escritura de este modelo, y originan una ecuación de recurrencia.

Sabemos que una ecuación como (5.1) determina completamente la sucesión X_k si el *estado inicial* X_0 es conocido. Por ejemplo, si para $k = 0$ la población está igualmente distribuida en las dos clases entonces

$$X_0 = (1/2, 1/2).$$

Al tiempo $k = 1$ tendremos

$$X_1 = (7/10, 3/10),$$

y para $k = 2$ el estado de la población es

$$X_2 = (74/100, 26/100).$$

Ejercicio 5.1. Calcular X_3 .

Continuar estos cálculos manualmente es tedioso e innecesario: una computadora rápidamente genera para los estados de esta población la sucesión

$$\begin{bmatrix} 0,5 \\ 0,5 \end{bmatrix}, \begin{bmatrix} 0,7 \\ 0,3 \end{bmatrix}, \begin{bmatrix} 0,74 \\ 0,26 \end{bmatrix}, \begin{bmatrix} 0,748 \\ 0,252 \end{bmatrix}, \begin{bmatrix} 0,7496 \\ 0,2504 \end{bmatrix}, \begin{bmatrix} 0,74992 \\ 0,25008 \end{bmatrix}, \dots,$$

que se aproximan al límite $(3/4, 1/4)$. La razón es que $X_k = M^k X_0$, y las potencias de M son

$$M^k = \begin{bmatrix} 3 + 5^{-k} & 3 - \frac{3}{5^k} \\ 1 - \frac{1}{5^k} & 1 + \frac{3}{5^k} \end{bmatrix} \rightarrow \frac{1}{4} \begin{bmatrix} 3 & 3 \\ 1 & 1 \end{bmatrix},$$

tal como aprendimos en el ejemplo 2.23, página 67. Por lo tanto

$$(5.2) \quad X_k = M^k \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} \rightarrow \frac{1}{4} \begin{bmatrix} 3 & 3 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} = \begin{bmatrix} 3/4 \\ 1/4 \end{bmatrix}.$$

Ejercicio 5.2. Mostrar que desde cualquier condición inicial X_0 se tiende al mismo límite. Sugerencia: si $X_0 = (x_{0,1}, x_{0,2})$ entonces $x_{0,1} + x_{0,2} = 1$, porque sus coeficientes son fracciones sobre el total de la población.

Una característica notable del estado límite $X_* = (3/4, 1/4)$ en (5.2) es que es un estado de equilibrio, o *estado estacionario* para la población. En efecto

$$\begin{bmatrix} 4/5 & 3/5 \\ 1/5 & 2/5 \end{bmatrix} \begin{bmatrix} 3/4 \\ 1/4 \end{bmatrix} = \begin{bmatrix} 3/4 \\ 1/4 \end{bmatrix},$$

por lo que si la población empieza en este estado permanece en él.

Observación 5.1. Equilibrio dinámico. El equilibrio en el estado X_* es dinámico. El modelo predice que una fracción de

$$(3/5) \times (1/4) = 3/20$$

del total de individuos de la población pasa de la clase c_1 a c_2 en cada unidad de tiempo. En tanto

$$(1/5) \times (3/4) = 3/20$$

lo hacen de c_2 a la c_1 . Tal como corresponde a una situación de equilibrio, ambos flujos se cancelan.

En el ejemplo anterior escogimos trabajar sólo con dos clases para obtener mayor simplicidad, pero la situación puede extenderse a un número n cualquiera de clases. En este caso, los estados X_k serán vectores de \mathbb{R}^n . Como sus coeficientes representan fracciones sobre el total de la población deben ser no negativas, y sumar 1.

Definición 5.1. Llamaremos *vectores de probabilidad* a los vectores $X = (x_1, \dots, x_n)$ de \mathbb{R}^n tales que

1. $x_i \geq 0$, para $i = 1, 2, \dots, n$;
2. $x_1 + x_2 + \dots + x_n = 1$.

Indicaremos con \mathcal{P} al subconjunto de \mathbb{R}^n formado por todos los vectores de probabilidad.

En el lenguaje de la definición 5.1, diremos que los estados serán vectores de \mathcal{P} .

Ejercicio 5.3. Representar geométricamente \mathcal{P} en los casos $n = 2$ y $n = 3$.

Cuando hay n clases, la matriz M que gobierna las transiciones entre ellas es una matriz real $n \times n$ con entradas no negativas, cuyas columnas suman 1. Esto es así porque cada coeficiente m_{ij} de la columna j indica que fracción de los individuos de la clase j va a pasar a la clase i . Llamaremos *matriz de transición* a una matriz que tiene estas dos propiedades. Observemos que las columnas de una matriz de transición son vectores de probabilidad.

Definición 5.2. Cadena de Markov. Una *cadena de Markov* es una sucesión de X_k , $k = 0, 1, \dots$, de vectores de probabilidad que satisfacen

$$(5.3) \quad X_{k+1} = MX_k, \quad k = 0, 1, 2, \dots,$$

para una matriz de transición M .

Observación 5.2. El tipo de problemas que estamos tratando aparece naturalmente en epidemiología o dinámica de poblaciones, pero la definición abstracta (5.2) resulta útil en situaciones muy variadas. Aunque hemos escogido presentarla en términos de “frecuencias”, “individuos” y “clases” porque esto facilita la exposición, el modelo es mucho más amplio. Por ejemplo, en la sección 5.2.1 lo usaremos para describir un paseo al azar sobre una red. El contexto más adecuado para interpretar a los vectores de probabilidad, las matrices de transición y las cadenas de Markov es el del cálculo de probabilidades. Por detalles en este sentido, ampliaciones del concepto y más aplicaciones remitimos al lector a [5]. En particular, en ese texto se considera el caso en que la matriz M de transición entre estados puede ir cambiando de un paso al otro, y tiene una dependencia explícita en k . En las cadenas de Markov que aquí tratamos la matriz M es constante, independiente de k , y por eso reciben el nombre de *estacionarias*.

Nota Histórica 5.1. *Las cadenas de Markov fueron formuladas por Andrei Markov alrededor de 1910. Markov, aficionado a la poesía, aplicó su modelo al poema de Pushkin Evgueni Onegin, estudiando las transiciones entre consonantes y vocales. Encontró la tabla que aparece en la figura 5.2, y a partir de estos valores predijo pro-*

	<i>vocal</i>	<i>consonante</i>
<i>vocal</i>	0,128	0,872
<i>consonante</i>	0,663	0,337

FIGURA 5.2. Transiciones entre consonantes y vocales en *Evgueni Onegin*

porciones de consonantes y vocales que mostraban un buen acuerdo con los valores reales.

Las cadenas de Markov admiten diversas generalizaciones. Una de ella es el paseo al azar: vamos caminando por la ciudad, y en cada esquina a la que llegamos sorteamos si vamos hacia el este, oeste, norte o sur. El paseo podría llevarnos muy lejos, de modo que para poder formalizarlo requiere infinitos posibles estados, pero incorpora la idea básica de los procesos de Markov: en cada paso el sorteo es independiente de la historia previa.

Un límite continuo de los paseos al azar es el proceso de Wiener, que provee un modelo para el movimiento browniano. Un fenómeno presumiblemente observado por primera vez por el botánico Robert Brown en 1827 (aunque ha habido controversia acerca de lo que si Brown realmente observó se trataba de lo que hoy llamamos un movimiento browniano).

También Albert Einstein trabajó sobre el movimiento browniano, realizando contribuciones que fueron tenidas en cuenta a la hora de otorgarle en 1921 el Premio Nobel de Física.

Ejercicio 5.4. En una población con dos clases A y B al cabo de una unidad de tiempo el 25% de los individuos de la clase A pasa a la B , y el 25% de los de la clase B pasa a la A . El resto permanece en su clase de origen. Hallar la matriz de transición que corresponde a esta población. Hallar los vectores de estado X_k cuando en el instante inicial toda la población es clase A . Mostrar que hay un único estado límite al que se converge desde cualquier estado inicial.

Para las cadenas de Markov del ejemplo 5.1 y el ejercicio 5.4 hay un vector límite al que se converge desde cualquier condición inicial. Esto no siempre ocurre.

Ejemplo 5.2. La matriz de transición

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

tiene $(1/2, 1/2)$ como estado de equilibrio. Cualquier otro estado inicial $(p, q) \in \mathcal{P}$ da lugar a un ciclo

$$\begin{bmatrix} p \\ q \end{bmatrix}, \begin{bmatrix} q \\ p \end{bmatrix}, \begin{bmatrix} p \\ q \end{bmatrix}, \begin{bmatrix} q \\ p \end{bmatrix}, \begin{bmatrix} p \\ q \end{bmatrix}, \begin{bmatrix} q \\ p \end{bmatrix}, \begin{bmatrix} p \\ q \end{bmatrix}, \begin{bmatrix} q \\ p \end{bmatrix}, \dots,$$

que no se aproxima a $(1/2, 1/2)$.

Uno de los principales resultados de este capítulo es el siguiente teorema.

Teorema 5.3. *Si M es una matriz de transición con todos sus coeficientes positivos entonces existe un único $X_* \in \mathcal{P}$ que tiene la propiedad de que cualquier cadena X_k generada por M , a partir de cualquier estado inicial $X_0 \in \mathcal{P}$, converge a X_* . Además X_* es un estado de equilibrio para M .*

La condición de que todas los coeficientes sean positivos no es necesaria. Ver el siguiente ejercicio, y también el ejercicio 5.19 en la página 150.

Ejercicio 5.5. Mostrar que la cadena de Markov generada por la matriz

$$\begin{bmatrix} 0 & 1/2 \\ 1 & 1/2 \end{bmatrix}$$

tiene un estado límite $(1/3, 2/3)$ al que se converge desde cualquier condición inicial E_0 . Si $E_0 = (1, 0)$, ¿cuántas unidades de tiempo hay que esperar hasta que la fracción de individuos en la segunda clase comience a mantenerse mayor que 0,65?

Aunque pueden no existir estados límites que atraen a la evolución desde cualquier condición inicial, siempre hay estados de equilibrio.

Proposición 5.4. *Si M es una matriz de transición existe $E_* \in \mathcal{P}$ que es un estado estacionario para M , en el sentido de que $ME_* = E_*$.*

Las demostraciones del teorema 5.3 y de la proposición 5.4 aparecen en la sección 5.2.

Ejercicio 5.6. Mostrar que $X \in \mathcal{P}$ es un estado de equilibrio para una matriz de transición M si y sólo si es un vector propio de M con valor propio 1. Mostrar que cualquier matriz de transición M tiene a 1 como un valor propio. Sugerencia: demostrar que 1 es un valor propio de M^\top , ¿por qué este resultado no es suficiente para demostrar por sí sólo la proposición 5.4?

5.1.1 Ejercicios adicionales

Ejercicio 5.7. Para cada una de las cadenas de Markov generadas por las matrices

$$\begin{bmatrix} 0 & 0 & \frac{3}{4} \\ \frac{1}{2} & 0 & \frac{1}{4} \\ \frac{1}{2} & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

1. calcular E_{10} a partir del estado inicial con todos los individuos en la primera clase;
2. investigar la existencia de estados límite.

Ejercicio 5.8. ¿Cuál es la proporción de vocales y consonantes que, según la tabla 5.2, predice el modelo de Markov para *Evgueni Onegin*?

Ejercicio 5.9. Escoger un texto no muy corto (poema, letra de canción, página de una novela, carta de amor, etcétera) y calcular las frecuencias de las transiciones entre vocales y consonantes. Con esta información calcular la proporción de vocales y consonantes que según esa tabla de transiciones predice el modelo de Markov, la proporción real de vocales y consonantes, y comparar los resultados.

Ejercicio 5.10. Para las cadenas de los ejercicios 5.4 y 5.5 determinar las fracciones de individuos que en el equilibrio, pasan de una clase a la otra en cada unidad de tiempo.

Ejercicio 5.11. En la cadena del ejemplo 5.1 las proporciones van convergiendo en forma monótona hacia sus valores límite, pero en la del ejercicio 5.5 aparecen oscilaciones, ¿puede explicar este fenómeno?

5.2 Métrica $\|\cdot\|_1$ y matrices de transición

Para demostrar el teorema 5.3 acerca de la existencia de estados límite para cadenas de Markov, probaremos que las matrices de transición con todos sus coeficientes positivos definen, en el conjunto \mathcal{P} de los vectores de probabilidad, aplicaciones contractivas respecto a $\|\cdot\|_1$. La información necesaria sobre aplicaciones contractivas aparece en el apéndice C. Un resultado preliminar para el lema 5.5 está contenido en el siguiente ejercicio.

Ejercicio 5.12. Mostrar que si M es una matriz de transición $n \times n$, entonces el subespacio

$$\mathbb{S} = \{X \in \mathbb{R}^n; x_1 + x_2 + \cdots + x_n = 0\}$$

es invariante para M .

La idea principal en la prueba de nuestro próximo lema es que cualquier vector no nulo en \mathbb{S} tiene algunas entradas positivas y algunas negativas. Por lo tanto, si M tiene todos sus coeficientes positivos, al formar el producto MX debe producirse cierta cancelación entre sumandos positivos y negativos.

Lema 5.5. Si M es una matriz de transición con todos sus coeficientes positivos existe una constante $\eta < 1$ tal que la desigualdad

$$(5.4) \quad \|MX\|_1 \leq \eta \|X\|_1$$

se satisface para todo vector $X \in \mathbb{S}$.

Demostración. Escribimos

$$(5.5) \quad \|MX\|_1 = \sum_{i=1}^n \left| \sum_{j=1}^n m_{ij} x_j \right| = \sum_{i=1}^n \sigma_i \sum_{j=1}^n m_{ij} x_j,$$

donde

$$\sigma_i = \begin{cases} 1 & \text{si } \sum_{j=1}^n m_{ij} x_j \geq 0, \\ -1 & \text{si } \sum_{j=1}^n m_{ij} x_j < 0. \end{cases}$$

Como $MX \in \mathbb{S}$ algunos de los números σ_i tomarán el valor 1, y otros -1 . Salvo en el caso trivial en que $MX = O$, para el que (5.4) es obvia. Reordenamos ahora la suma en (5.5) como

$$(5.6) \quad \|MX\|_1 = \sum_{j=1}^n \sum_{i=1}^n \sigma_i m_{ij} x_j \leq \sum_{j=1}^n \left| \sum_{i=1}^n \sigma_i m_{ij} \right| |x_j|.$$

Tenemos

$$\sum_{i=1}^n \sigma_i m_{ij} = \sum_{\{i; \sigma_i=1\}} m_{ij} - \sum_{\{i; \sigma_i=-1\}} m_{ij}$$

Si llamamos δ al más pequeño de los coeficientes de la matriz M entonces

$$\begin{aligned} \delta &\leq \sum_{\{i; \sigma_i=1\}} m_{ij} \leq 1, \\ \delta &\leq \sum_{\{i; \sigma_i=-1\}} m_{ij} \leq 1. \end{aligned}$$

Restando la segunda cadena de desigualdades de la primera encontramos

$$-1 + \delta \leq \sum_{\{i; \sigma_i=1\}} m_{ij} - \sum_{\{i; \sigma_i=-1\}} m_{ij} \leq 1 - \delta,$$

lo que es equivalente a

$$\left| \sum_{i=1}^n \sigma_i m_{ij} \right| \leq 1 - \delta.$$

Combinando esta última desigualdad con (5.6) conseguimos acotar

$$\|MX\|_1 \leq (1 - \delta) \sum_{j=1}^n |x_j|,$$

que es justamente (5.4) con $\eta = 1 - \delta < 1$. \square

Lema 5.6. *Si M es una matriz de transición con todas sus entradas positivas la correspondencia $X \mapsto MX$ define una contracción en el conjunto \mathcal{P} formado por los vectores de probabilidad.*

Demostración. M transforma vectores de probabilidad en vectores de probabilidad, por lo que efectivamente define una aplicación de \mathcal{P} en \mathcal{P} . Además, si X e Y son vectores de probabilidad las entradas de su diferencia $X - Y$ suman cero. El lema 5.5 implica

$$\|MX - MY\|_1 = \|M(X - Y)\|_1 \leq \eta \|X - Y\|_1$$

para alguna constante $\eta < 1$ que no depende de X e Y . \square

Demostración. (del teorema 5.3.) La matriz M define una aplicación contractiva respecto a la norma $\|\cdot\|_1$ en el conjunto \mathcal{P} de los vectores de probabilidad, que es un conjunto cerrado (ver el ejercicio C.2, en la sección C.1 de los apéndices). El teorema C.8, página 180 implica el teorema. \square

El siguiente ejercicio propone probar la proposición 5.4. Utilizaremos el siguiente teorema de cálculo de varias variables.

Teorema 5.7. *Toda sucesión X_k acotada en \mathbb{R}^n tiene una subsucesión convergente.*

Ejercicio 5.13. Consideremos una matriz de transición M , de tamaño $n \times n$.

1. Mostrar que para cada $\epsilon > 0$ existe una matriz de transición M_ϵ que tiene todos sus coeficientes $m_{\epsilon,ij}$ positivos, y tal que $|m_{ij} - m_{\epsilon,ij}| < \epsilon$.
2. Mostrar que para cualquier vector X se satisface $\|(M - M_\epsilon)X\|_1 \leq \epsilon \|X\|_1$.
3. Usar el teorema 5.7 para mostrar que existe una sucesión ϵ_j tal que los vectores X_{ϵ_j} que satisfacen $M_{\epsilon_j}X_{\epsilon_j} = X_{\epsilon_j}$ tienden a un límite X_* .
4. Mostrar que X_* es un vector de probabilidad y que $MX_* = X_*$. Sugerencia: considerar

$$MX_* - X_\epsilon = M(X_* - X_\epsilon) + (M - M_\epsilon)X_\epsilon,$$

y pasar al límite

5.2.1 Paseos al azar en grafos, Google y PageRank

Cada matriz de transición $n \times n$ admite una interpretación como el modelo de un paseo al azar sobre una red con n nodos $(1, \dots, n)$. Llamemos M a la matriz. Podemos interpretar cada una de sus entradas m_{ij} como la probabilidad de pasar desde el nodo j al nodo i recorriendo la conexión entre j e i . Los coeficientes m_{jj} representan las probabilidades de permanecer en el nodo j . Una coeficiente nulo implica la ausencia de conexión, o que esa conexión no será recorrida. Por ejemplo, si un coeficiente m_{jj} es nulo significa que si estamos en el nodo j lo abandonaremos, sorteando el posible destino con probabilidad m_{ij} para cada uno de los $n - 1$ nodos restantes en la red. Si el lector desea seguir pensando en términos de una población dividida en clases e individuos pasando de una clase a otra puede imaginar millones de insectos saltando de un nodo a otro de una red. Cada clase en la población corresponde a un nodo.

Ejercicio 5.14. Representar redes que correspondan a las matrices de transición del ejercicio 5.7, página 146.

Ejemplo 5.3. En el ejemplo 2.5, página 48 introdujimos la matriz

$$(5.7) \quad N = \begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{bmatrix}$$

como una matriz de conectividad “normalizada” que describía una estructura de enlaces. Podemos reinterpretarla ahora como una matriz de transición, según la cual vamos viajando por la red siguiendo enlaces. Desde una página pasamos a otra, sorteando entre todos los enlaces que contiene.

Si usamos una matriz de transición M para describir el paseo al azar sobre una red, la proposición 5.4 asegura que existe un vector de probabilidad X que es un estado de equilibrio. Satisface entonces $MX = X$, lo que implica que es un vector propio con valor propio 1. Los coeficientes de X , no negativos, pueden usarse para definir un puntaje para las páginas de la web, como hicimos en la sección 2.1.1. Pero si entre los coeficientes de la matriz M hay ceros, el vector X no tiene por qué ser único. Para evitar este posible problema X , podemos modificar ligeramente la matriz. Por ejemplo, a partir de la matriz N en (5.7), consideramos

$$(5.8) \quad \begin{bmatrix} 0,01 & 0,49 & 0,49 & 0,005 \\ 0,49 & 0,01 & 0,01 & 0,005 \\ 0,01 & 0,49 & 0,01 & 0,98 \\ 0,49 & 0,01 & 0,49 & 0,01 \end{bmatrix}.$$

En términos de la web, los coeficientes positivos que no corresponden a enlaces pueden interpretarse como la probabilidad de saltar a cualquier otra página sin seguir un enlace (por ejemplo, cargando una dirección nueva en el navegador). Los coeficientes

positivos en la diagonal como la probabilidad de prolongar la visita a la página en la que se está, simplemente quedándose, o recorriendo un enlace interno. El vector

$$P \simeq (0, 2355, 0, 1216, 0, 3513, 0, 2916) \in \mathcal{P}$$

es un vector propio de (5.8) con valor propio 1, que propone el siguiente orden de importancia para los nodos (páginas): 3, 4, 1, 2. El teorema 5.3 asegura que es el único en \mathcal{P} . Tampoco puede haber otros vectores propios que tengan todos sus coeficientes no negativos (ver la parte ejercicio 3 del ejercicio 5.16). Además de la interpretación como un vector de puntajes, P tiene significado probabilístico: su i -ésima entrada es la probabilidad de estar en el nodo i de la red luego de haber estado vagabundeando por ella un tiempo suficientemente largo, muy largo, como para que el efecto de la condición inicial (dada por nuestra página de partida) ya se haya olvidado. Recomendamos al lector consultar [3] para una explicación más detallada y nuevas referencias.

5.2.2 Ejercicios adicionales

Ejercicio 5.15. Si M es una matriz de transición mostrar que la desigualdad

$$(5.9) \quad \|MX\|_1 \leq \|X\|_1$$

se satisface para cualquier vector X en \mathbb{R}^n .

Ejercicio 5.16. M representa una matriz de transición.

1. Mostrar que todos los valores propios de M , reales o complejos, que sean distintos de 1 tienen módulo estrictamente menor que 1. Sugerencia: usar el teorema de los círculos de Gerschgorin.
2. Mostrar que si M tiene todas sus coeficientes positivos entonces la dimensión de $\ker(M - I)$ es igual a 1. Sugerencia: cualquier vector $X \in \mathbb{R}^n$ puede descomponerse de manera única como $X = \lambda E + Y$ donde E es un estado estacionario para M , y los coeficientes de Y suman 0.
3. Mostrar que si M tiene todos sus coeficientes positivos y X es un vector propio de M con coeficientes mayores o iguales que cero, entonces el valor propio que corresponde a X es 1.

Ejercicio 5.17. Completar una prueba del teorema 2.20, página 75 para el caso particular de matrices de transición.

Ejercicio 5.18. Si M es una matriz de transición con todos sus coeficientes positivos y E un estado de equilibrio para M , mostrar que todos los coeficientes de E son positivos, ¿es cierto el resultado para matrices de transición cualesquiera?

Ejercicio 5.19. Diremos que una matriz de transición es *regular* si alguna potencia M^k tiene la propiedad de que todos sus coeficientes son positivos.

1. Mostrar que el teorema 5.3 también es cierto para matrices de transición regulares.

2. Mostrar que para una matriz M de transición regular

$$\dim(\ker(M - I)) = 1.$$

Ejercicio 5.20. Una matriz de transición se llama *doblemente aleatoria* si también los coeficientes de cada fila suman 1. Si los coeficientes de una matriz doblemente aleatoria son positivos, ¿cuál es su único estado estacionario?

Capítulo 6: Códigos correctores de errores



Cuando se almacena o transmite información siempre se corre el riesgo de cometer un error o perder una parte de los datos a lo largo del proceso. Por esta razón, toda la tecnología de la información incorpora procedimientos automáticos de corrección de errores. La idea básica es simple: tal como una persona guarda muchas copias de una información importante o repite varias veces algo que desea transmitir con precisión, la información se almacena y procesa con cierta redundancia. Esta redundancia artificial se administra inteligentemente gracias al uso de estructuras matemáticas adecuadas. En este capítulo ofrecemos al lector una breve introducción a esta área de las matemáticas contemporáneas, que nació cuando comenzaba la segunda mitad del siglo veinte.

En la sección 6.1 introduciremos esta idea de redundancia y mostramos los primeros ejemplos de códigos detectores y correctores de errores. La sección 6.2 presenta una interpretación geométrica de los procesos de codificación y recuperación de la información. Por último, en la sección 6.3 dejamos que las estructuras geométricas y algebraicas interactúen. Terminamos presentando los importantes códigos de Reed-Solomon, que, aunque no lo notemos, todos los días trabajan para hacer nuestra vida más agradable.

Un aspecto a destacar es que en esta sección prácticamente toda el álgebra se hará sobre cuerpos finitos, esencialmente sobre \mathbb{Z}_2 . En el apéndice B hemos incluido la información sobre cuerpos finitos necesaria para este capítulo, que en realidad es muy poca. El lector interesado puede consultar también la monografía [8].

6.1 Detección y corrección de errores

Presentamos en esta sección la noción de *dígito de control*, su uso para dar distintos niveles de protección a la información, y la idea de que emplear dígitos de control es equivalente a imponer ecuaciones algebraicas sobre los registros de ceros y unos.

6.1.1 Control de paridad y otros dígitos de control

La información digitalizada se representa usando dos caracteres, el cero y el uno. Cada carácter almacena un *bit* de información. Los bits se agrupan en unidades de mayor tamaño. Por ejemplo, en las listas de ocho bits denominadas *bytes*¹, pero consideraremos listas de cualquier longitud formadas por ceros y unos.

Una manera de proteger las listas $X = (x_1, \dots, x_n)$ de longitud n contra posibles alteraciones o pérdidas de información es convenir en utilizar sólo aquellas que tengan una cantidad par de unos. Esta condición admite la representación algebraica

$$(6.1) \quad x_1 + x_2 + \dots + x_n = 0, \quad (\text{mód } 2).$$

Ejercicio 6.1. Supondremos que todos los *bytes* de este ejercicios satisficían una ecuación como (6.1) cuando fueron almacenados.

1. Se recuperan los *bytes* $(1, 0, 1, 0, 0, 0, 1, 1)$ y $(1, 0, 1, 1, 1, 0, 0, 1)$, ¿de cuál de ellos podemos asegurar que ha sido alterado?, ¿podemos estar seguros de que el otro no ha sufrido modificaciones?
2. Al intentar recuperar un *byte* se lee $(0, 1, 1, 1, \quad, 0, 1, 1)$ donde falta la información de la tercera posición, ¿qué conjeturamos que habrá que poner?, ¿podemos tener certeza de nuestra respuesta?

Imponer sobre X la condición (6.1) significa que sólo podemos usar $n - 1$ de los n bits para almacenar información. El restante quedará determinado por (6.1). Es usual referirse a los caracteres extra, que no agregan nueva información pero introducen una redundancia que protege a la información contra pérdidas y alteraciones como a *caracteres de control*, o *dígitos de control*, cuando se trata de números. Una ecuación como (6.1), que fuerza una cantidad par de unos se llama *control de paridad*. Al dígito que se agrega para satisfacer un control de paridad le llamaremos *dígito de control de paridad*, o simplemente *control de paridad*.

Ejercicio 6.2. Hallar el dígito de control que hay que agregar a la información $(1, 0, 0, 1, 1, 0, 0)$ para producir un *byte* que satisfaga el control de paridad (6.1).

Observación 6.1. Controles de paridad y \mathbb{Z}_2 . La aritmética módulo 2 es la aritmética del cuerpo finito \mathbb{Z}_2 y se adapta perfectamente a nuestro propósito: permite manejar los dos símbolos 0 y 1 necesarios para representar la información digital, y expresar la condición (6.1) como una sencilla ecuación lineal homogénea. Por lo tanto, consideraremos a partir de ahora las listas X de longitud n como elementos del espacio vectorial \mathbb{Z}_2^n , y utilizaremos la aritmética módulo 2 sin hacer mención explícita de ello.

¹El término español para *byte* es “octeto”, pero conservaremos la forma inglesa, de uso más extendido.

Observación 6.2. A partir de un único control de paridad en un *byte* no podemos detectar un número par de errores. Pero esta situación problemática requiere al menos dos errores, lo que es, en general, más improbable que sufrir uno sólo. Todas las técnicas de protección contra errores tienen esta característica: no pueden evitar que haya errores indetectados, pero disminuyen la probabilidad de que ocurran hasta un nivel en que las comunicaciones se vuelven fiables.

Observación 6.3. Dígitos de control y la vida cotidiana. Los dígitos y caracteres de control están incorporados a muchos números de identificación de uso corriente. Por ejemplo, en el sistema EAN13 que genera los códigos de barras que aparecen en el exterior de los envases de los artículos de consumo, en el ISBN que sistematiza los registros bibliográficos, y en los números de los documentos de identidad. Se determinan por ecuaciones algebraicas como (6.1), pero usando otras aritméticas, por ejemplo, módulo 10, módulo 11, módulo 23, etcétera. Son una posible fuente de inspiración para actividades en el aula, razón por la recomendamos hacer el siguiente ejercicio.

Ejercicio 6.3. Investigar sobre el uso de dígitos de control en la vida corriente, y sobre las propiedades matemáticas de los distintos sistemas.

Un poco de jerga:

- utilizaremos la palabra *error* para indicar la sustitución de un carácter por otro diferente;
- cuando un carácter se pierde en una posición conocida (como en la parte 2 del ejercicio 6.1) hablaremos de una *borradura*;
- Llamaremos *palabras* a los elementos de \mathbb{Z}_2^n .

Observación 6.4. Para representar los elementos de \mathbb{Z}_2^n emplearemos en muchos lugares de este capítulo una notación concisa que omite las comas y paréntesis. Haciendo uso de ella escribimos, por ejemplo, $(1, 0, 1, 0)$ como 1010 y $(0, 0, 0, 0, 0, 0, 0)$ como 0000000.

6.1.2 El código de repetición

¿Cuántas veces hemos repetido algo hasta el cansancio para asegurarnos de que es entendido? Si queremos comunicar una de dos alternativas, como NO o SÍ, podemos representarlas por un bit de información, 0 o 1. Luego, en vez de transmitir 0 o 1, transmitiremos uno de los dos vectores

$$(6.2) \quad 00 \dots 0 \quad 11 \dots 1$$

de \mathbb{Z}_2^n , en los que simplemente repetimos n veces el mensaje 0 o 1. El conjunto formado por las dos palabras en (6.2) recibe el nombre de *código de repetición de longitud n* .

Ejercicio 6.4. Supongamos que A acuerda con B que le transmitirá el mensaje 0 o 1 usando el código de repetición de longitud n .

1. Mostrar que si en la transmisión se producen menos de n errores B notará que hubo problemas en la transmisión, pero que si se producen exactamente n errores B recibirá el mensaje equivocado.
2. Mostrar que si n es impar, de la forma $n = 2e + 1$ con e natural, y en la transmisión se producen no más de e errores entonces B puede interpretar correctamente el mensaje.
3. Mostrar que si se producen menos de n borraduras B puede interpretar el mensaje.
4. Analizar cuáles son las combinaciones de errores y borraduras que pueden producirse sin que B pierda su capacidad de interpretar correctamente el mensaje.

6.1.3 Los códigos de Hamming

Los controles de paridad sólo permiten detectar errores o corregir borraduras, y los códigos de repetición son ineficientes, porque prácticamente toda la información es redundante. Los códigos de Hamming son un primer ejemplo de códigos con una estructura y propiedades interesantes, y permiten corregir un error.

Observación 6.5. La expresión “corregir un error” significa que si en la transmisión se produce un error el mensaje puede recuperarse correctamente, pero no asegura que si se producen dos se recuperará un mensaje con un error sólo. En general, cuando digamos que un código es capaz de “corregir e errores” la expresión significará que si se producen hasta e errores en un mensaje será correctamente decodificado. Pero, en principio, para más de e errores puede pasar cualquier cosa.

Nota Histórica 6.1. *Richard Hamming, pionero en el área de la corrección automática de errores, introdujo los códigos de Hamming hacia fines de la década de 1940. Una discusión detallada de su construcción y propiedades apareció en 1950, en un artículo titulado Error detecting and error correcting codes. En esos años nacían los códigos correctores, y también la teoría de la información, que esencialmente tomó forma a partir del celebrado artículo de Claude Shannon, A mathematical theory of information, publicado en 1948. La teoría de Shannon constituye uno de los fundamentos de toda nuestra tecnología de comunicaciones y almacenamiento de datos, por lo que su impacto en la vida moderna es de una dimensión difícil de aquilatar. Un teorema central de su teoría asegura que es posible transmitir información con una probabilidad de error tan baja como se desee, con tal de codificarla adecuadamente. Este resultado, que aparece en el artículo de 1948 junto con una breve noticia de los códigos de Hamming, continúa estimulando hasta el día de hoy la búsqueda de buenos códigos que hagan realidad la promesa que contiene.*

Un único control de paridad, que puede satisfacerse o no, no aporta información suficiente para más que decidir entre una de dos posibilidades. Por ejemplo, permite distinguir entre que no se produzca ningún error o haya exactamente uno, pero en este caso no nos dice dónde se produjo. La idea de Hamming fue aplicar sobre una lista

$X \in \mathbb{Z}_2^n$ varios controles de paridad simultáneamente, cada uno de ellos actuando sólo sobre algunos de los bits de X , de modo de que aporten informaciones independientes unas de otras.

La primera pregunta que debió responder fue ¿cuántos controles de paridad son necesarios para identificar los posibles patrones de error que se quiere corregir?

Como nuestro propósito es corregir **un** error (sin preocuparnos de lo que puede ocurrir cuando aparezcan más errores) en una lista de longitud n , debemos ser capaces de distinguir los siguientes casos:

1. para cada valor de i entre 1 y n , que haya un error en el lugar i . Esto hace un total de n posibilidades;
2. el caso adicional de que no exista error alguno.

Completamos así $n + 1$ alternativas diferentes. Por otra parte, un control de paridad puede arrojar dos resultados posibles: satisfacerse o fallar. Dos controles tienen cuatro posibilidades, y si se usan m pueden generar hasta 2^m patrones diferentes de aciertos y fallos. Por tanto, si deseamos poder distinguir entre $n + 1$ posibilidades diferentes a partir de la aplicación de m controles de paridad necesitamos que m y n sean tales que se satisfaga

$$(6.3) \quad 2^m \geq n + 1.$$

Cada control de paridad que impongamos sobre posiciones de una lista implica forzar el valor de un bit, que hará las veces de dígito de control. Si queremos m controles de paridad sobre una lista de longitud n nos quedarán

$$k = n - m$$

bits de información. Los valores en los otros m se calcularán a partir de los k con información. Para cada valor de m dado, escogeremos

$$n = 2^m - 1,$$

que es el valor de n más grande que satisface (6.3). Quedan entonces

$$n - m = 2^m - m - 1$$

bits de información.

Mostraremos cómo distribuir eficientemente los controles de paridad analizando el caso

$$m = 3, \quad n = 2^3 - 1 = 7, \quad k = 7 - 3 = 4,$$

con 3 bits de control y 4 con información. La observación clave es la siguiente: cada uno de los números del 1 al 7 que identifican las posiciones de una lista

$$X = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{Z}_2^7$$

puede representarse en notación binaria por medio de un patrón de tres dígitos:

$$1 = 001, \quad 2 = 010, \quad 3 = 011, \quad 4 = 100, \quad 5 = 101, \quad 6 = 110, \quad 7 = 111.$$

Aplicaremos los controles de paridad para que sus fallos vayan revelando las cifras de la escritura en base 2 del lugar del error. El caso 000 en que todos los controles se satisfacen corresponderá a la situación en que no hay error.

El primer control que impondremos es la condición

$$(6.4) \quad x_4 + x_5 + x_6 + x_7 = 0.$$

Si se produce un error en las posiciones 4, 5, 6 o 7 este control devolverá el valor 1 en vez de 0, indicando que la primera cifra del lugar de error es un 1. Siguiendo la misma lógica, pero ahora con la segunda cifra del lugar del error, el segundo control es

$$(6.5) \quad x_2 + x_3 + x_6 + x_7 = 0.$$

El tercero,

$$(6.6) \quad x_1 + x_3 + x_5 + x_7 = 0,$$

define si el hipotético error está en una posición identificada por un número par o por un impar.

En resumen, las listas X en nuestro código son las soluciones del sistema de ecuaciones

$$(6.7) \quad \begin{cases} x_1 + x_3 + x_5 + x_7 = 0, \\ x_2 + x_3 + x_6 + x_7 = 0, \\ x_4 + x_5 + x_6 + x_7 = 0. \end{cases}$$

Es directo ver que del sistema (6.7) se pueden despejar fácilmente x_1 , x_2 y x_4 , que quedan expresadas en términos de x_3 , x_5 , x_6 y x_7 como

$$(6.8) \quad \begin{aligned} x_1 &= x_3 + x_5 + x_7, \\ x_2 &= x_3 + x_6 + x_7, \\ x_4 &= x_5 + x_6 + x_7. \end{aligned}$$

Esto sugiere emplear los lugares 3, 5, 6 y 7 para guardar cuatro bits con información, y usar las posiciones 1, 2 y 4 como los dígitos de control que aseguren (6.7).

A continuación presentamos las 16 elecciones posibles para x_3, x_5, x_6, x_7 , junto a la palabra $X \in \mathbb{Z}_2^7$ que cada elección genera

	(x_3, x_5, x_6, x_7)	$(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$
	0000	0000000
	1000	1110000
	0100	1001100
	0010	0101010
	0001	1101001
	1100	0111100
	1010	1011010
(6.9)	1001	0011001
	0110	1100110
	0101	0100101
	0011	1000011
	1110	0010110
	1101	1010101
	1011	0110011
	0111	0001111
	1111	1111111

Ejemplo 6.1. Transmitiendo una “ñ”. La letra **ñ** tiene el número 164 en la codificación **Latín 1**. La expresión binaria de 164 es 10100100, que podemos dividir en los bloques 1010 y 0100 para su transmisión con la ayuda del código de Hamming. Codificamos 1010 como 1011010, y 0100 con 1001100, según la tabla (6.9).

Si en la transmisión del primer bloque el mensaje se adultera en 1001010, cuando el receptor aplica los controles de paridad (6.7) obtiene

$$\begin{aligned}
 (6.10) \quad & 1 + 0 + 1 + 0 = 0, \\
 & 0 + 0 + 1 + 0 = 1, \\
 & 1 + 0 + 0 + 0 = 1.
 \end{aligned}$$

Concluye que ha habido un error en el lugar con expresión binaria 011, el tercero. Corrige este error modificando la tercera entrada en la lista, y recupera 1011010. Al eliminar los dígitos de control el mensaje se interpreta como 1010, que fue lo que se intentó transmitir.

Supongamos ahora que el segundo bloque se ve contaminado por dos errores, y quien espera el mensaje recibe 1111100. Ahora los controles de paridad arrojan el resultado

$$\begin{aligned}
 (6.11) \quad & 1 + 1 + 1 + 0 = 1, \\
 & 1 + 1 + 0 + 0 = 0, \\
 & 1 + 1 + 0 + 0 = 0,
 \end{aligned}$$

que sugiere corregir el primer lugar de la lista. Al hacerlo obtenemos erróneamente 0111100, que a su vez es mal decodificado como 1100. En este caso el código no es capaz de recuperar correctamente el mensaje. Más aún, al intentar eliminar los errores todavía agregamos un error más en la lista de siete números. Esto ocurre porque hemos superado la capacidad de corrección del código. El diseño de este código de Hamming es capaz de corregir un error. Cuando hay dos errores el código todavía es capaz de alertarnos, pero ya no tiene capacidad de recuperar la palabra correcta.

Ejercicio 6.5. Suponiendo que se emplea el código de Hamming para codificar mensajes de cuatro bits en palabras de siete bits, usando las fórmulas (6.8) o la tabla (6.9), hallar las palabras de cuatro bits que corresponden a la recepción de cada una de los siguientes mensajes de siete bits:

1. 0111100;
2. 1000110;
3. 1000010;
4. 11_0110, en que se ha perdido el tercer bit.
5. 11_1_11.

¿Siempre es posible interpretar correctamente un mensaje con dos borraduras?

Ejercicio 6.6. Mostrar que el código de Hamming que corresponde a $m = 2$ es el código de repetición que consiste en repetir 3 veces cada bit, ¿qué código se obtiene para $m = 1$?

6.1.4 La noción de código y un poco de jerga

Definición 6.1. Códigos, palabras código y codificación Un *código* de longitud n sobre \mathbb{Z}_2 es un subconjunto \mathcal{C} no vacío de \mathbb{Z}_2^n . Llamaremos *palabras código*, o simplemente *palabras* a cada uno de los elementos del código. Una *codificación* de \mathbb{Z}_2^k es una función biyectiva entre \mathbb{Z}_2^k y un código $\mathcal{C} \subset \mathbb{Z}_2^n$.

Ejemplo 6.2. Al agregar un dígito de control de paridad a cada palabra de \mathbb{Z}_2^n se genera un código formado por la mitad de los vectores en \mathbb{Z}_2^{n+1} . Sus palabras código son las listas X con un número par de unos. La codificación simplemente consiste en agregar el dígito de control.

Ejemplo 6.3. El código de repetición de longitud 3 es

$$\{000, 111\} \subset \mathbb{Z}_2^3.$$

Su codificación es $0 \mapsto 000$, $1 \mapsto 111$.

Ejemplo 6.4. El código de Hamming de longitud 7 está formado por la lista de palabras código que aparece en la segunda columna de (6.9). La función de codificación copia la palabra original en los lugares 3, 5, 6 y 7, e intercala en los lugares 1, 2 y 4 los dígitos de control que producen las fórmulas (6.8).

Observación 6.6. La definición 6.1 de código puede extenderse a cualquier conjunto de símbolos. Las palabras no tienen por qué estar en \mathbb{Z}_2^n . Por ejemplo, en la sección 6.3.3 daremos ejemplos de códigos construidos sobre otros cuerpos finitos.

El diccionario del idioma español puede verse como un ejemplo de código: es un subconjunto de todas las posibles palabras formadas con letras de nuestro alfabeto. El hecho de que no todas las palabras estén en el diccionario permite corregir automáticamente algunos errores. ¿Lo ha notado el lector?

6.1.5 Ejercicios adicionales

Ejercicio 6.7. Buscar información sobre Shannon, los aspectos matemáticos de la teoría de la información y el impacto de esta teoría sobre nuestra vida cotidiana.

Ejercicio 6.8. Además de la corrección automática de errores, otras dos grandes áreas del procesamiento de la información son la *compresión* y la *criptografía*. Buscar información sobre las matemáticas involucradas en ellas. La referencia [2] puede ser un buen comienzo.

Recordemos que la distancia de Hamming entre dos palabras de la misma longitud no es otra cosa que la cantidad de lugares en que difieren (ver la definición 1.8, en la página 40).

6.2 La distancia de Hamming en \mathbb{Z}_2^n

Cuando se transmiten palabras de un código los errores resultan evidentes porque producen palabras extrañas al código. Se corrigen volviendo a la palabra código más cercana, en el sentido de la distancia de Hamming.

6.2.1 Decodificación por el vecino más próximo

Cuando en una transmisión de palabras de un código \mathcal{C} se recibe una palabra X que no pertenece a \mathcal{C} adoptaremos el siguiente *criterio del vecino más próximo* para su decodificación: interpretaremos que se ha transmitido la palabra $Y \in \mathcal{C}$ que hace mínima la distancia de Hamming $d(X, Y)$ entre todas las palabras código. Notemos que Y es la palabra código que coincide con X en la mayor cantidad posible de posiciones. La distancia de Hamming dota de sentido geométrico a este criterio de sentido común, que también tiene sentido estadístico como estimador bayesiano o de máxima verosimilitud. Por nociones de inferencia estadística ver la monografía [10].

Ejercicio 6.9. Verificar que la decodificación de las palabras con errores en el ejemplo 6.1 siguió el criterio del vecino más próximo.

Ejercicio 6.10. Mostrar que el criterio del vecino más próximo aplicado a la decodificación de un código de repetición de longitud $n = 2e + 1$ implica que el receptor entenderá que se le ha transmitido el símbolo que aparece más veces. ¿Qué puede ocurrir si $n = 2e$?

El sentido de codificar las palabras es aumentar la distancia de Hamming entre ellas: cuanto más se separan más difícil es confundirlas.

Ejemplo 6.5. La distancia de Hamming entre 0100. y 0000 es 1, en tanto que entre 01001 y 00000 es igual a 2. Aumentó en una unidad al agregar un bit de control de paridad.

Ejemplo 6.6. La distancia entre los símbolos 0 y 1 es igual a 1. Al codificarlos con un código de repetición de longitud n estamos aumentando su distancia a n .

Ejercicio 6.11. Buscar información sobre alfabetos telefónicos como **alpha**, **bravo**, **charlie**, ..., o **alicia**, **beatriz**, **carolina**, ..., e interpretar su uso en términos de los conceptos de esta sección.

Ejercicio 6.12. Verificar que al usar el código de Hamming (6.9) para codificar palabras de \mathbb{Z}_2^4 como palabras código en \mathbb{Z}_2^7 la distancia entre palabras siempre aumenta entre 1 y 3 unidades, ¿puede el lector detectar los casos extremos?

La distancia entre las palabras código diferentes más próximas entre sí, es un parámetro que caracteriza la capacidad de corrección de un código.

Definición 6.2. Distancia mínima de un código. La *distancia mínima* d entre las palabras de un código \mathcal{C} es

$$d = \min \{d(X, Y); X, Y \in \mathcal{C}, X \neq Y\}.$$

Ejemplo 6.7. Un posible código en \mathbb{Z}_2^n es todo \mathbb{Z}_2^n . Su distancia mínima es 1. Este código es inútil para detectar o corregir errores.

Ejemplo 6.8. El código $\mathcal{C} \subset \mathbb{Z}_2^{n+1}$ que resulta de agregar un dígito de control de paridad a las palabras de \mathbb{Z}_2^n tiene distancia mínima 2.

Ejemplo 6.9. La distancia mínima del código de Hamming (6.9) es 3. Puede mostrarse examinando el código pero es trabajoso. En la sección 6.3 lo mostraremos haciendo uso de su estructura lineal.

Proposición 6.3. Capacidad de corrección de un código.

Un código \mathcal{C} con distancia mínima $d = 2e + 1$ puede corregir e errores.

Demostración. Supongamos que en una palabra código X se introducen $m \leq e$ errores que producen otra palabra X' . Entonces $d(X', X) = m \leq e$. Si hubiera una palabra $Y \in \mathcal{C}$ tal que $d(X', Y) \leq d(X', X)$ tendríamos

$$d(X, Y) \leq d(X, X') + d(X', Y) \leq e + e = 2e < 2e + 1 = d,$$

en contradicción con que d es la distancia mínima del código. Por lo tanto el criterio del vecino más próximo decodifica correctamente X' como X . \square

Aumentar la distancia mínima tiene su costo: puede aumentar a lo sumo una unidad por cada dígito de control que se agregue en la codificación.

Proposición 6.4. Cota de Singleton.

Cuando las palabras de \mathbb{Z}_2^k se codifican usando un código $\mathcal{C} \subset \mathbb{Z}_2^n$ la distancia mínima d de \mathcal{C} satisface

$$(6.12) \quad d \leq n - k + 1.$$

Demostración. Consideremos las primeras $k-1$ posiciones en las palabras del código. El código contiene 2^k palabras, pero estas primeras $k-1$ posiciones sólo dan lugar a 2^{k-1} posibles configuraciones. Entonces hay dos palabras código X e Y diferentes que coinciden completamente en sus primeras $k-1$ posiciones, de modo que X e Y pueden diferir a lo sumo en las restantes $n-k+1$ posiciones. Esto implica

$$d \leq d(X, Y) \leq n - k + 1.$$

□

6.2.2 Ejercicios adicionales

Ejercicio 6.13. Mostrar que la distancia de Hamming es invariante por traslaciones, en el sentido que satisface

$$d(X, Y) = d(X + Z, Y + Z).$$

Ejercicio 6.14. Generalizar la proposición 6.3 a códigos de distancia mínima par $d = 2e$.

Ejercicio 6.15. Reparación de borraduras. Mostrar que si un código tiene distancia mínima d y se borran no más de $d-1$ entradas de una palabra código X , entonces la palabra original puede recuperarse correctamente.

Ejercicio 6.16. Estudiar si el código de Hamming (6.9), los códigos de repetición y los códigos de control de paridad satisfacen con igualdad la cota de Singleton.

Ejercicio 6.17. Mostrar que se puede ser muy torpe y codificar \mathbb{Z}_2^k con un código $\mathcal{C} \subset \mathbb{Z}_2^n$ que tenga distancia mínima 1, ¿se puede hacer algo peor sin violar la condición natural de que la función de codificación sea biyectiva?

Ejercicio 6.18. Escojamos $k-1$ números i_1, \dots, i_{k-1} en $\{1, 2, \dots, n\}$. En las hipótesis de la proposición 6.4, mostrar que \mathcal{C} contiene al menos dos palabras diferentes que coinciden completamente sobre las $k-1$ posiciones $x_{i_1}, x_{i_2}, \dots, x_{i_{k-1}}$. ¿Puede enunciarse un resultado análogo para una posición?, ¿y para un número cualquiera de posiciones?

6.3 Códigos lineales

Los códigos que hemos examinado hasta el momento tienen una estructura lineal: son subespacios vectoriales del espacio vectorial \mathbb{Z}_2^n . En esta sección veremos como la estructura lineal facilita la codificación, la decodificación y el cálculo de la distancia

mínima. La interacción entre las estructuras algebraica y geométrica que generan, respectivamente, las operaciones lineales en \mathbb{Z}_2^n y la distancia de Hamming, es esencial para poner un poco de orden en el pandemonio de ceros y unos de la información digital y crear códigos útiles para las aplicaciones.

Definición 6.5. Un *código lineal* es un subespacio vectorial de \mathbb{Z}_2^n .

La longitud n de las palabras en un código lineal, la dimensión k del código y la distancia mínima d entre sus palabras son parámetros importantes. Llamaremos código lineal $[n, k, d]$ a un código lineal con estos parámetros.

Ejemplo 6.10. Código de Hamming [7,4,3]. El código de Hamming (6.9) está formado por las soluciones en \mathbb{Z}_2^7 del sistema lineal (6.7). Es un código lineal de dimensión 4, que es el núcleo de la matriz

$$(6.13) \quad C = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

que tiene rango 3. Observemos que en las columnas de C aparecen las expresiones binarias de los números del 1 al 7.

Las reglas de codificación especificadas por las fórmulas (6.8) también admiten una expresión matricial, en la forma

$$(6.14) \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_3 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}.$$

El código de Hamming es entonces igual a la imagen de la matriz 7×4 , de rango 4, en (6.14). Ya hemos observado que la distancia mínima de este código es 3 pero aún no lo hemos probado.

Un código lineal $[n, k, d]$ siempre puede caracterizarse por $n - k$ ecuaciones lineales y representarse como el núcleo de una matriz $(n - k) \times n$ de rango $n - k$, a la que llamaremos *matriz de control* del código. También puede representarse como la imagen de cualquier matriz $k \times n$ cuyas k columnas sean una base del código. Llamaremos *matriz de codificación* a cualquiera de estas matrices. Cada matriz de codificación G

define una codificación²

$$\begin{aligned} X &\mapsto GX, \\ \mathbb{Z}_2^k &\rightarrow \mathcal{C} \subset \mathbb{Z}_2^k, \end{aligned}$$

que es una función biyectiva entre \mathbb{Z}_2^k , el conjunto de palabras con k símbolos, y el código \mathcal{C} , formado por todas las palabras código.

Ejemplo 6.11. La matriz C en (6.13) es una matriz de control para el código de Hamming $[7,4,3]$. Es también la matriz 3×7 que aparece en la portada de esta monografía, aunque allí esté representada con unos coeficientes poco convencionales. En el miembro de la derecha de la fórmula (6.14) aparece una matriz de codificación para este mismo código.

Ejemplo 6.12. El conjunto de palabras de longitud $n + 1$ que satisfacen un control de paridad es un código lineal con parámetros $[n + 1, n, 2]$. Una matriz de codificación es

$$(6.15) \quad G = \begin{bmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix},$$

y una matriz de control es $C = [1 \ 1 \ \dots \ 1 \ 1]$. G es $(n + 1) \times n$ y C es $1 \times (n + 1)$.

Ejemplo 6.13. Los códigos de repetición son códigos lineales $[n, 1, n]$.

Ejercicio 6.19. Hallar una matriz de codificación y una matriz de control para los códigos de repetición.

Ejemplo 6.14. El código de Golay La imagen de la matriz

$$G = [I_{12} \ M]^\top,$$

²Lo habitual en la literatura de códigos lineales es escribir a las palabras como matrices fila, y no como columnas. Si hubiéramos adherido a esta convención y abandonado la escritura de vectores como columnas que hemos usado a lo largo de la monografía, la fórmula de codificación habría tomado el aspecto $X \mapsto XG$, con una matriz de codificación G que sería la traspuesta de “nuestra” matriz de codificación.

donde el bloque I_{12} indica a la matriz identidad 12×12 y

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

es un código lineal con parámetros $[23, 12, 7]$ que recibe el nombre de *Código de Golay binario*.

Nota Histórica 6.2. *El código de Golay apareció en una breve nota publicada en 1949, en los albores de la teoría de los códigos correctores de errores. Se le presenta allí directamente, como el resultado de una búsqueda no exhaustiva basada en consideraciones combinatorias. La búsqueda fue exitosa, porque encontró un objeto realmente interesante, con una rica estructura cuyo estudio escapa al objetivo de esta monografía.*

La verificación de que las palabras código tienen longitud 23 y el código dimensión 12 es directa a partir de G . El análisis de su distancia mínima es más complejo, y lo obviaremos.

6.3.1 Distancia mínima en códigos lineales

La estructura lineal permite simplificar el cálculo de la distancia mínima, porque reduce el problema de determinarla a calcular las distancias de las palabras código a la palabra nula O , que tiene ceros en todas las posiciones. La distancia de una palabra X a O es igual a la cantidad de coeficientes no nulos que contiene X . Es habitual llamar *peso* de la palabra a este número, y designarlo con la expresión $w(X)$ (en la que el lector seguramente habrá adivinado la primera letra de la palabra inglesa “weight”).

Proposición 6.6. *Si \mathcal{C} es un código lineal $[n, k, d]$ su distancia mínima d es igual al menor de los pesos $w(X)$ entre las palabras X no nulas de \mathcal{C} .*

Demostración. Para X e Y en \mathcal{C} tenemos

$$d(X, Y) = d(X - Y, Y - Y) = d(X - Y, O) = w(X - Y).$$

Como el código es lineal $X - Y \in \mathcal{C}$, y $X - Y \neq O$ si y sólo si $X \neq Y$. Por lo tanto, el conjunto de las distancias entre palabras código diferentes coincide con el de los pesos de las palabras código diferentes de O . \square

Ejemplo 6.15. Al examinar la lista de las 15 palabras no nulas en el código de Hamming $[7, 4, 3]$ encontramos palabras de pesos 3, 4 y 7. Esto implica que la distancia mínima entre palabras del código es 3.

Ejercicio 6.20. Mostrar que la distancia mínima de un código es igual al menor cardinal de una familia linealmente dependiente formada por columnas de su matriz de control.

Ejercicio 6.21. Los códigos de Hamming $[2^m - 1, 2^m - m - 1, 3]$. Para m natural cada uno de los 2^m vectores en \mathbb{Z}_2^m contiene la expresión binaria de uno de los números naturales $0, 1, \dots, 2^m - 1$. Sea C la matriz $m \times (2^m - 1)$ que tiene como columnas a todos los vectores no nulos de \mathbb{Z}_2^m , ordenados según el número natural que representan. Mostrar que C tiene rango m , y es la matriz de control de un código $[2^m - 1, 2^m - m - 1, 3]$. Sugerencia: usar el ejercicio 6.20 para hallar la distancia mínima de estos códigos.

6.3.2 Decodificación por síndromes

Sea \mathcal{C} un código lineal $\mathcal{C} [n, k, d]$, con matriz de control C . Una palabra X está en \mathcal{C} si y sólo si $CX = O$, donde O tiene longitud $n - k$. Pero si la palabra se ve perturbada por un vector de error Z que hace que el resultado $Y = X + Z$ no esté en el código, al pasarla por la matriz de control resulta

$$(6.16) \quad CY = C(X + Z) = CX + CZ = CZ \neq O,$$

lo que delata la presencia de un error. Observemos que el resultado en (6.16) sólo depende del error Z , no de X . Llamaremos a (6.16) el *síndrome* $s(Y)$ de la palabra Y . Naturalmente, las palabras de \mathcal{C} tienen síndrome O .

Ejemplo 6.16. Los síndromes de

$$1111111, \quad 1001010, \quad 1111100$$

para la matriz de control (6.13) del código de Hamming $[7, 4, 3]$ son, respectivamente,

$$000, \quad 011, \quad 100.$$

La primera palabra está en el código. Las otras dos no.

El criterio del vecino más próximo implica que si $S(Y) \neq 0$ debemos asumir que el error Z es el de peso mínimo que produce el síndrome $s(Y)$.

Para el código de Hamming $[7, 4, 3]$ esto es muy fácil de implementar: cada uno de los siete posibles síndromes no nulos es una de las columnas C_i de la matriz de control (6.13). Para cada columna C_i el error E_i , el i -ésimo vector en la base canónica de \mathbb{Z}_2^7 , tiene peso 1 y síndrome $s(E_i) = C_i$, y no hay palabra de peso menor que pueda producir ese síndrome.

Por lo tanto, si $S(Y) = C_i$ entonces asumimos que $Y = X + E_i$, donde X es una palabra código. Por lo tanto $X = Y + E_i$ se recupera sumando E_i a la palabra contaminada, lo que es exactamente lo mismo que cambiar la posición i de Y .

Ejemplo 6.17. La primera palabra del ejemplo 6.16 ya está en el código de Hamming y no requiere corrección. El síndrome de la segunda sugiere que su error es 0010000 y debe corregirse a la palabra código

$$1001010 + 0010000 = 1011010.$$

Tal como adelantábamos, la corrección consiste en cambiar el 0 de la tercera posición por un 1. Para corregir la tercera modificaremos directamente la posición del error, sin pasar por los cálculos intermedios. El resultado es 0111100.

Ejercicio 6.22. Supongamos que el lector espera mensajes (x_1, x_2, x_3, x_4) codificados con el código de Hamming $[7, 4, 3]$ por medio de la codificación (6.14). Usar el procedimiento de calcular síndromes por medio de C para decodificar los mensajes 0111011 y 1110110.

Ejercicio 6.23. Mostrar que para cada palabra X de \mathbb{Z}_2^7 que no está en el código de Hamming, existe una única palabra código que está a distancia 1 de X . Extender el resultado a la familia de códigos de Hamming $[2^m - 1, 2^m - m - 1, 3]$.

El ejercicio anterior implica que cada código de Hamming es un buen cubrimiento de $\mathbb{Z}_2^{2^m-1}$. Esta es una notable propiedad combinatoria del código de Hamming.

Ejercicio 6.24. Buscar información sobre las propiedades combinatorias y las aplicaciones de los códigos de Hamming y de Golay.

6.3.3 Códigos de Reed Solomon

Los ejemplos de códigos que hemos presentado hasta ahora son insuficientes para la mayoría de las aplicaciones prácticas, pero este no es el caso de los códigos de Reed-Solomon.

Nota Histórica 6.3. *Los códigos de Reed-Solomon fueron introducidos en 1960 por Irving Reed y Gustave Solomon. Para volverse de uso práctico tuvieron que esperar a que en 1968 Elwyn Berlekamp desarrollara un algoritmo de decodificación eficiente. A partir de entonces fueron incorporándose a los estándares de comunicaciones de la NASA y la agencia espacial europea. En 1980 llegaron a nuestras casas, como parte de los procedimientos de codificación de los discos compactos, y allí se quedaron. Porque siguen en nuestros CDs, y también los emplean los DVDs y la telefonía digital.*

Necesitamos un ejercicio preparatorio.

Ejercicio 6.25. Extender la definición de código lineal a subespacios de \mathbb{K}^n , donde \mathbb{K} es cualquier cuerpo finito. Mostrar que las nociones de matriz de control y matriz de codificación siguen teniendo sentido, que también es válida la cota de Singleton (6.12), y que la distancia mínima es igual al peso mínimo de las palabras no nulas.

La construcción de los códigos de Reed-Solomón está basada en asociar a cada palabra

$$P = (a_0, a_1, \dots, a_{k-1}) \in \mathbb{K}^k$$

construida sobre un cuerpo finito \mathbb{K} el polinomio

$$P[x] = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}.$$

Luego P se codifica evaluando $P[x]$ sobre n de los elementos de \mathbb{K} , con $n \geq k$. La idea básica de esta construcción es que k de las n evaluaciones bastarán para recuperar los k coeficientes del polinomio. Las restantes $n - k$ son redundancia, que protege a la información contra errores. Obviamente, n no puede superar el cardinal de \mathbb{K} . Se genera así un código lineal con parámetros $[n, k]$.

Si usamos $\alpha_i \in \mathbb{K}$, $i = 1, 2, \dots, n$, para las evaluaciones, una matriz generadora de este código es

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}^\top.$$

Proposición 6.7. *La distancia mínima de un código de Reed-Solomon $[n, k]$ es*

$$d = n - k + 1.$$

Demostración. Un polinomio no nulo de grado menor o igual a $k - 1$ puede tener a lo sumo $k - 1$ raíces, por lo que al menos $n - k + 1$ evaluaciones de $P[x]$ serán no nulas. Como efectivamente hay polinomios de grado $k - 1$ sobre \mathbb{K} con $k - 1$ raíces en el conjunto $\{\alpha_1, \dots, \alpha_n\}$, concluimos que el peso mínimo para las palabras no nulas del código es $n - k + 1$. \square

Este resultado nos dice que los códigos de Reed-Solomon son óptimos respecto a la cota de Singleton, por lo que cada dígito extra contribuye a la capacidad de corrección del código. Observemos además que hay códigos de Reed-Solomon con distancias mínimas grandes, mucho mayores que 3 o 4.

En su construcción puede emplearse cualquier cuerpo finito, en particular los de la forma $\mathbb{GF}(2^k)$, en la que los símbolos del cuerpo son agrupamientos de k ceros y unos.

Los códigos de Reed-Solomon son adecuados para tratar ráfagas de errores. Si trabajamos directamente con 0 y 1, como en los códigos de Hamming, el deterioro de seis o siete bits consecutivos produce seis o siete errores. Pero si empleamos, por ejemplo, un código construido sobre $\mathbb{GF}(2^8)$ cada símbolo en las palabras código es un *byte*, formado por ocho bits. Una ráfaga de seis o siete errores alterará un *byte*, a lo sumo dos, por lo que este código la verá como uno o dos errores. Esta característica es muy deseable, porque en muchos sistemas de comunicaciones los errores tienden a aparecer en rachas en vez de aislados.

6.3.4 Ejercicios adicionales

Ejercicio 6.26.

1. Si C y G son, respectivamente, matrices de control y de codificación de un código, mostrar que CG es una matriz nula.
2. Mostrar que si C y G son matrices $(n - k) \times n$ y $k \times n$ de rangos $n - k$ y k respectivamente, tales que CG es una matriz nula, entonces C y G son, respectivamente una matriz de control y una matriz de codificación de un código.
3. **Código dual.** Mostrar que si C y G son matrices de control y de codificación de un código \mathcal{C} entonces G^\top y C^\top son las matrices de control y de codificación de otro código. A este código se le llama el *código dual* de \mathcal{C} .

Ejercicio 6.27. Mostrar que todas las palabras no nulas del código dual del código de Hamming $[7,4,3]$ tienen peso 4. Concluir que es un código $[7,3,4]$ en el que todas las palabras están a distancia 4 de las demás. Recibe el nombre de *código simplex*, ¿por qué será?

Ejercicio 6.28. Código de Hamming extendido. Mostrar que cuando a cada palabra del código de Hamming $[7,4,3]$ se le agrega un bit de control de paridad se obtiene un código lineal $[8,4,4]$. Hallar una matriz de control y una matriz de codificación para este código. Encontrar una estrategia de decodificación que permita corregir cuando se produzca un error y detectar cuando se produjeron dos.

Ejercicio 6.29. Códigos extendidos. Mostrar que si a cada palabra de un código $[n, k, d]$, con d impar, se le agrega un bit de control de paridad se obtiene un código $[n + 1, k, d + 1]$. A este código se le llama el código extendido del código original.

Ejercicio 6.30. Usar el hecho de que la matriz de control de un código lineal $[n, k]$ es de rango $n - k$ y el resultado del ejercicio 6.20 para dar una nueva demostración de la cota de Singleton, válida para códigos lineales.

Apéndice A: Preliminares



Asumimos que el lector conoce los resultados básicos del Álgebra Lineal de los espacios \mathbb{R}^n , incluyendo la relación con la resolución de sistemas lineales de ecuaciones, las propiedades más básicas del cálculo de determinantes y nociones sobre el producto escalar en \mathbb{R}^n .

Aunque en esta monografía fundamentalmente trabajamos con el espacio vectorial \mathbb{R}^n , y emplearemos números reales, elementos del conjunto \mathbb{R} , en algunos lugares se hace necesario trabajar sobre el cuerpo \mathbb{C} de los números complejos. En el capítulo 6 se dan algunas aplicaciones sobre cuerpos finitos. Asumimos que el lector está familiarizado con los números complejos. Si no es así puede consultar [1]. Lo necesario sobre cuerpos finitos está apretadamente resumido en el apéndice B.

Vale la pena tener presente que desde el punto de vista de la estructura vectorial, la teoría de todos los espacios \mathbb{K}^n , donde \mathbb{K} designa a un cuerpo cualquiera, es la misma.

A.1 Matrices y álgebra de matrices

Una matriz es un arreglo de números en filas y columnas. Si tiene m filas y n columnas diremos que es una matriz de tamaño $m \times n$, o, simplemente, una matriz $m \times n$. Si $m = n$ diremos que la matriz es cuadrada de orden n .

Supondremos conocidas para el lector las principales propiedades del álgebra de matrices: cuándo y cómo se pueden sumar las matrices; cuándo y cómo se pueden multiplicar, etcétera. Pero deseamos enfatizar algunos conceptos:

- el producto MX de una matriz M por un vector X , es la combinación lineal de las columnas de M con los coeficientes almacenados en el vector X ;
- las columnas del producto MN de dos matrices M y N , son los productos de M por las columnas de N ;
- una matriz M de tamaño $m \times n$ puede pensarse como
 - un único objeto (que a su vez forma parte de diversas estructuras algebraicas);
 - hecha de mn coeficientes;
 - hecha de n columnas;
 - hecha de m filas;
 - hecha de submatrices más chicas (aquí las posibles descomposiciones son muy variadas);
 - la manera de definir una transformación $X \mapsto MX$.

- La suma y el producto de matrices puede reinterpretarse a la luz de cada una de estas maneras de ver las matrices, y todas las posibles reinterpretaciones tienen sentido en distintos contextos.

Hemos optado por representar las matrices en paréntesis rectos $[]$, y reservar los curvos $()$ para conjuntos ordenados. A veces las dos cosas casi se confunden, porque una matriz es un conjunto ordenado de columnas, pero las dos interpretaciones del mismo conjunto de datos son diferentes, y lo hemos marcado en la notación.

Otra convención que hemos adoptado es no escribir los ceros en una matriz cuando por su forma especial, o su construcción, un coeficiente es necesariamente cero. Por ejemplo, representaremos una matriz M triangular superior 2×2 como

$$\begin{bmatrix} m_{11} & m_{12} \\ & m_{22} \end{bmatrix}.$$

Hemos dejado vacío el lugar del coeficiente m_{21} , necesariamente nulo una vez que sabemos que M es triangular superior.

A.2 Vectores y matrices columnas

Representaremos los vectores X de \mathbb{R}^n con la notación

$$X = (x_1, x_2, \dots, x_n).$$

Pero el vector X puede identificarse de manera completamente natural con la columna

$$[x_1 \ x_2 \ \dots \ x_n]^\top.$$

Cuando esta identificación se hace, el producto MX de una matriz $m \times n$ por X cobra sentido dentro del formalismo del producto de matrices. Por lo tanto, **usaremos libremente esta identificación a lo largo de la monografía**. Los vectores de \mathbb{R}^n aparecerán escritos como n -uplas o como matrices columnas, casi indistintamente, sin dar mayores explicaciones.

A.3 Independencia lineal y bases

Cuando manejemos la noción de independencia lineal nos referiremos a conjuntos **ordenados** de vectores. Hacemos esta opción porque deseamos decir que las columnas de la matriz

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

forman una familia linealmente dependiente. Si consideramos el conjunto de sus columnas haciendo abstracción de que hay una primera columna $[1 \ 1]^\top$, y una segunda columna $[1 \ 1]^\top$, entonces este conjunto sólo contiene a la columna $[1 \ 1]^\top$ y es ¡linealmente independiente!

Además es importante considerar a las bases de cualquier subespacio vectorial de \mathbb{R}^n como un conjunto ordenado: si se modifica el orden de los vectores en una base las coordenadas de los vectores cambian. Por lo tanto, los mismos vectores, puestos en distinto orden, generan bases diferentes.

A.4 Coordenadas

Supondremos conocido para el lector que cada base en un subespacio \mathbb{S} de \mathbb{R}^n define un sistema de coordenadas que permite representar los vectores de \mathbb{S} .

Especialmente importante es el caso en que \mathbb{S} es todo \mathbb{R}^n . En este caso, los cambios de coordenadas que resultan de pasar de una base a otra están representados por matrices invertibles.

Ejemplo A.1. Los espacios \mathbb{R}^n tienen una base a la que llamaremos *base canónica*,

$$\mathcal{C} = (e_1, e_2, \dots, e_n)$$

donde el i -ésimo vector e_i tiene todos sus coeficientes nulos salvo el i -ésimo. Esta base puede describirse en términos de la *delta de Kronecker*

$$(A.1) \quad \delta_{ij} = \begin{cases} 1, & j = i, \\ 0, & j \neq i, \end{cases} \quad i, j = 1, 2, \dots, n.$$

por las ecuaciones

$$e_{i,j} = \delta_{ij}, \quad i, j = 1, 2, \dots, n.$$

La base canónica son las columnas de la matriz I_n , la matriz identidad $n \times n$, que tiene todos sus coeficientes nulos salvo los de la diagonal principal que son iguales a uno.

Las dos afirmaciones

- A es invertible;
- las columnas de A forman una base de \mathbb{R}^n ,

son equivalentes. Cuando resolvemos un sistema

$$AX = Y$$

con una matriz A cuadrada e invertible, la solución

$$X = A^{-1}Y$$

es el vector de coordenadas de Y respecto a la base de \mathbb{R}^n formada por las columnas de A .

A.5 Interpretaciones geométricas

Las n -uplas de \mathbb{R}^n tienen una interpretación geométrica en relación con el plano y el espacio usuales de la geometría euclidiana. Hay aquí un punto que nos interesa comentar con cierto cuidado. Una pareja de números (x_1, x_2) puede interpretarse como un punto en un plano provisto de un sistema de coordenadas, y también como un vector. En esta monografía fundamentalmente usaremos esta segunda interpretación, y nos referiremos a los elementos de \mathbb{R}^2 como vectores. La razón es que haremos una y otra vez uso de la estructura vectorial de \mathbb{R}^2 , en la que las dos operaciones básicas de suma y producto por un escalar se corresponden con la suma de vectores y con

el producto de un vector por un escalar, pero no tienen significado en términos de puntos.

Pero para algunos propósitos es conveniente que el lector pueda manejar también la imagen como punto. Por ejemplo, cuando se quiere representar subconjuntos de \mathbb{R}^2 , como se hace en la figura 1.1, página 25, y en la figura 4.4, página 121.

La representación como puntos se conecta con la representación como vector. Porque cuando un vector se representa con su primer extremo en el origen, el segundo extremo (que en forma coloquial podemos llamar su “punta”) determina una ubicación en el plano, que es un punto. Recíprocamente, una vez fijado un origen O , un punto P en el plano determina al vector $P - O$.

Una manera de mirar las cosas es pensar, sólo por un momento, que las parejas de \mathbb{R}^2 son en realidad parejas de números, nada más. Pero como es sumamente conveniente recurrir a la intuición geométrica para manejarlas desearemos interpretarlas como puntos o como vectores. La interpretación que se elija dependerá esencialmente del tipo de relaciones y propiedades que se decida enfatizar.

Como resumen, digamos que el lector debe tratar de usar las distintas representaciones y pasar de una a otra según le convenga¹. Naturalmente, esta discusión se generaliza a cualquier espacio \mathbb{R}^n , en particular para $n = 3$, que modela el espacio físico más cercano a nuestra experiencia directa.

A.6 Producto escalar en \mathbb{R}^n y \mathbb{C}^n

En \mathbb{R}^n está definido el producto escalar $X \cdot Y$ que a cada par X e Y de vectores les asocia el número

$$X \cdot Y = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

El producto escalar se extiende a \mathbb{C}^n por la fórmula

$$X \cdot Y = x_1\bar{y}_1 + x_2\bar{y}_2 + \cdots + x_n\bar{y}_n,$$

donde \bar{z} indica al complejo conjugado de z . Las propiedades de este producto son similares a las del producto en \mathbb{R}^n , incluyendo la desigualdad de Cauchy-Schwarz

$$|X \cdot Y| \leq |X||Y|.$$

Pero el producto escalar en \mathbb{C}^n no es conmutativo, porque $Y \cdot X = \overline{X \cdot Y}$.

La noción de que dos vectores X e Y son ortogonales si y sólo si $X \cdot Y = 0$ también se generaliza a \mathbb{C}^n .

¹Toda esta confusión entre punto y vector desaparece cuando se conoce el concepto de *espacio afín*. Como los espacios afines permiten construir modelos de la geometría euclidiana del plano y el espacio, es recomendable que un profesor de Matemática al menos sepa de su existencia (Ver el Ejercicio 3.3 en la página 78). El problema con \mathbb{R}^2 es que puede dotársele de una estructura de espacio afín en la que los mismos actores, parejas de \mathbb{R}^2 , hacen los dos papeles: puntos y vectores. No es tan grave, de tanto en tanto también ocurre en el cine y en el teatro que el mismo actor interprete dos papeles. También en cine y en teatro puede generar cierta confusión. Pero, igual que ocurre en la Matemática, al rato uno se acostumbra.

Apéndice B: Cuerpos finitos



Un *cuerpo* es una estructura algebraica formada por un conjunto al que llamaremos \mathbb{K} en el que están definidas dos operaciones de *suma* y *producto*, que tienen las mismas propiedades que en el conjunto de los números racionales, reales y complejos: es posible restar, y siempre se puede dividir entre cualquier número diferente de cero. Obviamos presentar aquí la caracterización axiomática detallada de la estructura de cuerpo, pero el lector puede encontrarla en [8].

Hay cuerpos que tienen una cantidad finita de elementos. El ejemplo más simple es el cuerpo \mathbb{Z}_2 , con el que trabajamos en el capítulo 6. Su descripción más sencilla es presentarlo como el conjunto

$$\{0, 1\}$$

formado por los dos símbolos 0 y 1 con las siguientes reglas para la suma y el producto (el producto aparece indicado con el símbolo \times):

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}, \quad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

Estas reglas son las de la suma y el producto módulo 2, en el que del resultado de las operaciones sólo se conserva el resto de dividir entre 2. Vemos que el opuesto de 1 es el propio 1. El único elemento no nulo del cuerpo es 1, número entre el que se puede dividir sin ningún problema y sin ningún esfuerzo.

El cuerpo \mathbb{Z}_2 es un caso particular de los cuerpos \mathbb{Z}_p , con p un número primo. Estos cuerpos pueden describirse como el conjunto

$$\{0, 1, 2, \dots, p-1\}.$$

Se opera en ellos usando la aritmética módulo p , en la que todo lo que es un múltiplo de p se identifica con 0. No damos más detalles sobre esto, pero referimos a [8].

Hay una familia infinita de cuerpos finitos, conocidos como los cuerpos de Galois, cada uno de ellos con p^k símbolos, donde p es un primo, y k un número natural cualquiera. Son interesantes en sí mismos, como objetos matemáticos, pero además tienen aplicaciones en el procesamiento de la información digital. Hay un cuerpo cuyos elementos son las 2^8 listas formadas por ocho ceros y unos, como, por ejemplo

$$00000000, \quad 01010101, \quad 11101101, \dots$$

No daremos los detalles de su estructura, pero a continuación mostramos un ejemplo similar, aunque bastante más pequeño.

Ejemplo B.1. El conjunto de cuatro símbolos $\{00, 10, 01, 11\}$ con las operaciones

+	00	10	01	11	×	00	10	01	11
00	00	10	01	11	00	00	00	00	00
10	10	00	11	01	10	00	10	01	11
01	01	11	00	10	01	00	01	11	10
11	11	01	10	00	11	00	11	10	01

también es un cuerpo, que recibe el nombre de $\mathbb{GF}(4)$. La \mathbb{G} es en honor a Evaristo Galois. La \mathbb{F} proviene de la palabra inglesa *field*, que en este contexto se traduce como “cuerpo”. El 4 alude a que este cuerpo tiene exactamente cuatro elementos. El símbolo $\mathbb{GF}(4)$ puede leerse entonces como “cuerpo de Galois con cuatro elementos”.

Ejercicio B.1. Completar los detalles necesarios para mostrar que $\mathbb{GF}(4)$ es un cuerpo.

El cuerpo “formado por los *bytes*” es $\mathbb{GF}(2^8)$.

Apéndice C: Completitud y puntos fijos



Una propiedad esencial para el análisis matemático dentro del sistema de los números reales es su completitud, noción que admite muchas caracterizaciones. Una de ellas es que toda sucesión de Cauchy de números reales es convergente, concepto que puede extenderse a cualquier conjunto \mathcal{X} en que esté definida una distancia d .

Definición C.1. Sucesiones de Cauchy. Una sucesión x_k , $k = 1, 2, \dots$, de elementos de \mathcal{X} es de Cauchy respecto a la distancia d si para cada $\epsilon > 0$ existe un número natural k_0 tal que la desigualdad

$$d(x_{m+k}, x_k) < \epsilon$$

se satisface para todo $k \geq k_0$ y todo $m \geq 0$.

Definición C.2. Completitud. Sea \mathcal{X} un conjunto en el que está definida una distancia d . Diremos que \mathcal{X} es completo respecto a la distancia d si cualquier sucesión de Cauchy respecto a d , converge, respecto a d , a un límite $x \in \mathcal{X}$.

Un caso particular de esta noción de completitud nos interesará especialmente en el capítulo 5.

Proposición C.3. \mathbb{R}^n es completo respecto a la distancia inducida por $\|\cdot\|_1$.

Demostración. Si X_k es una sucesión de Cauchy respecto a $\|\cdot\|_1$ la desigualdad

$$|x_{k,i} - x_{k+m,i}| \leq \|X_k - X_{k+m}\|_1$$

se satisface para cada $i = 1, \dots, n$, $k \geq 1$ y $m \geq 0$, e implica que cada sucesión de coordenadas $x_{k,i}$ es de Cauchy en \mathbb{R} . Por lo tanto cada sucesión $x_{k,i}$ tiene un límite x_i . La proposición 1.4, página 36, implica que $X = (x_1, x_2, \dots, x_n)$ es el límite de X_k en $\|\cdot\|_1$. \square

C.1 Contracciones y puntos fijos

El principal objetivo de esta sección es presentar un resultado de punto fijo para contracciones, sobre el que descansa la demostración del teorema 5.3, página 145, acerca de las cadenas de Markov.

Una contracción es una función que acerca entre sí los puntos de cualquier conjunto en que esté definida una distancia. Es un concepto aplicable en muchos contextos, que aquí particularizaremos para subconjuntos de \mathbb{R}^n y la norma $\|\cdot\|_1$ que introdujimos en la sección 1.3.

Definición C.4. Contracciones. Sea \mathcal{X} un subconjunto cualquiera de \mathbb{R}^n . Una función $f : \mathcal{X} \rightarrow \mathcal{X}$ es una contracción respecto a la norma $\|\cdot\|_1$ si existe una constante positiva $\eta < 1$ tal que

$$\|f(X) - f(Y)\|_1 \leq \eta \|X - Y\|_1, \quad X, Y \in \mathcal{X}.$$

Teorema C.5. Teorema del punto fijo en \mathbb{R}^n .

Sea $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ una contracción. Entonces existe un único $X \in \mathbb{R}^n$ tal que

$$(C.1) \quad X = F(X).$$

Decimos que el vector X en (C.1) es un *punto fijo* para la transformación f , porque se transforma en sí mismo, “queda fijo”, al aplicarle f .

El teorema C.5 establece que cuando f es una contracción la ecuación (C.1) tiene una única solución. Este tipo de teoremas son herramientas muy poderosas para mostrar la existencia y unicidad de soluciones de diversas ecuaciones en distintos campos de la matemática. A modo de ejemplo, proponemos al lector un resultado de cálculo de una variable.

Ejercicio C.1. Sea $f : \mathbb{R} \rightarrow \mathbb{R}$ una función derivable tal que

$$|f'(x)| \leq \eta < 1$$

se satisface para todo x real. Usar el teorema C.5 para mostrar que la ecuación

$$f(x) = x$$

tiene una única solución.

¿El resultado es cierto si se sabe que $|f'(x)| < 1$ para todo $x \in \mathbb{R}$? Sugerencia: puede ser más fácil atacar el problema gráficamente que comenzar por buscar fórmulas.

En la monografía [5] aparece con su demostración un teorema de punto fijo en \mathbb{R} . Las ideas son las mismas que empleamos aquí pero en un contexto unidimensional. Recomendamos al lector que se familiarice con ese resultado antes de pasar a la demostración del teorema C.5. Ver también en [15] los resultados relacionados.

Demostación del teorema C.5 La idea es tomar un punto X_0 cualquiera en \mathbb{R}^n , y mostrar que la sucesión

$$X_0 = X, \quad X_1 = f(X), \quad X_2 = f(X_1) = f(f(X)), \quad X_3 = f(X_2) = f(f(f(X))), \dots,$$

que se obtiene aplicando recursivamente f a partir de X_0 , tiene límite. En general tendremos

$$(C.2) \quad X_{k+1} = f(X_k), \quad k = 0, 1, 2, \dots$$

La hipótesis de contractividad hace que los términos de la sucesión se vayan acercando entre sí. Ya que

$$\|X_2 - X_1\|_1 = \|f(X_1) - f(X_0)\|_1 \leq \eta \|X_1 - X_0\|_1.$$

Para la diferencia entre los siguientes tenemos

$$\|X_3 - X_2\|_1 = \|f(X_2) - f(X_1)\|_1 \leq \eta \|X_2 - X_1\|_1 \leq \eta^2 \|X_1 - X_0\|_1.$$

Un argumento inductivo muestra entonces

$$(C.3) \quad \|X_{k+1} - X_k\|_1 \leq \eta^k \|X_1 - X_0\|_1, \quad k = 1, 2, \dots$$

Los coeficientes η^k decaen a cero con velocidad exponencial. Esto no sólo implica que dos términos consecutivos de la sucesión X_k se están aproximando, sino que dos cualesquiera de ellos estarán muy próximos, con tal de tomar sus índices suficientemente grandes. En efecto

$$X_{k+m} - X_k = \sum_{j=0}^{m-1} (X_{k+j+1} - X_{k+j}),$$

por lo que

$$\|X_{k+m} - X_k\|_1 \leq \sum_{j=0}^{m-1} \|X_{k+j+1} - X_{k+j}\|_1.$$

Acotamos cada sumando en la sumatoria por (C.3), para obtener

$$(C.4) \quad \|X_{k+m} - X_k\|_1 \leq \|X_1 - X_0\|_1 \eta^k \sum_{j=0}^{m-1} \eta^j \leq \frac{\eta^k}{1 - \eta} \|X_1 - X_0\|_1.$$

Como $\eta < 1$ el último miembro en la cadena de desigualdades tiende a cero cuando k tiende a infinito, lo que implica que la sucesión X_k es de Cauchy y converge a un cierto límite X , en virtud de la proposición C.3.

Pasemos al límite cuando $k \rightarrow \infty$ en ambos miembros de (C.2). En el de la izquierda aparece X_{k+1} , que converge a X . En el de la derecha aparece $f(X_k)$. Como

$$\|f(X_k) - f(X)\|_1 \leq \eta \|X_k - X\|_1 \rightarrow 0$$

resulta

$$f(X_k) \rightarrow f(X),$$

Concluimos entonces que X satisface (C.1).

Si Y también es un punto fijo de f entonces $f(Y) = Y$. Por lo tanto

$$\|Y - X\|_1 = \|f(Y) - f(X)\|_1 \leq \eta \|Y - X\|_1.$$

Como $\eta < 1$ esta desigualdad sólo puede satisfacerse si $\|Y - X\|_1 = 0$, lo que implica que Y es igual a X , y la unicidad del punto fijo para f . \square

La demostración del teorema C.5 implica la siguiente proposición.

Proposición C.6. *Sea $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ una contracción. Entonces existe un único $X \in \mathbb{R}^n$ tal que $f^{(k)} X_0 \rightarrow X$ cuando $n \rightarrow \infty$, para cualquier $X_0 \in \mathbb{R}^n$.*

En muchos casos, como en la aplicación de este tipo de resultados que se hace en la sección 5.2, interesa trabajar no en todo \mathbb{R}^n sino en algunos de sus subconjuntos.

Definición C.7. Un subconjunto $R \subset \mathbb{R}^n$ es *cerrado* respecto a la norma $\|\cdot\|_1$ si cualquier punto $X \in \mathbb{R}^n$ que es límite en $\|\cdot\|_1$ de una sucesión contenida en R pertenece a R .

Ejercicio C.2. Mostrar que el conjunto \mathcal{P} formado por los vectores

$$X = (x_1, \dots, x_n) \in \mathbb{R}^n$$

que satisfacen

1. $x_i \geq 0$, para $i = 1, 2, \dots, n$;
2. $x_1 + x_2 + \dots + x_n = 1$.

es un subconjunto cerrado de \mathbb{R}^n .

Teorema C.8. Sea \mathcal{X} un subconjunto cerrado de \mathbb{R}^n y $f : \mathcal{X} \rightarrow \mathcal{X}$ una contracción. Entonces

1. f tiene un único punto fijo en \mathcal{X} .
2. existe un único $X \in \mathcal{X}$ tal que para cualquier $X_0 \in \mathcal{X}$ la sucesión $f^{(k)}X_0$ converge a X cuando $k \rightarrow \infty$.

Ejercicio C.3. Demostrar el teorema C.8. Sugerencia: imitar la prueba del teorema C.5, probando ahora que el límite de $f^{(k)}(X)$ pertenece a \mathcal{X} .

C.1.1 Ejercicios adicionales

Ejercicio C.4. Mostrar que las bolas abiertas

$$B(X, r) = \{Y \in \mathbb{R}^n; \|Y - X\|_1 < r\}$$

no son cerradas, pero

$$\bar{B}(X, r) = \{Y \in \mathbb{R}^n; \|Y - X\|_1 \leq r\}.$$

sí lo son.

Ejercicio C.5. Mostrar que toda sucesión convergente respecto a una distancia d es de Cauchy respecto a d .

Ejercicio C.6. Mostrar que \mathbb{R}^n es completo respecto a la distancia inducida por el módulo. Estudiar si es completo respecto a la distancia de Hamming (ver la definición 1.8 de la distancia de Hamming, en la página 40).

Ejercicio C.7. Mostrar que los cocientes $q_n = f_n/f_{n-1}$, entre dos números de Fibonacci sucesivos, satisfacen para $n > 1$ la relación

$$q_{n+1} = 1 + \frac{1}{q_n}.$$

Aplicar los resultados de este apéndice a

$$f(x) = 1 + \frac{1}{x}$$

para mostrar que los cocientes q_n convergen a la razón áurea.

Bibliografía



- [1] Chuaqui, M., Riera, G. *Transformaciones en Geometría Euclidiana y No-Euclidiana*. J.C. Sáez Editor, Santiago, 2011.
- [2] COMAP (the Consortium for Mathematics and Its Applications). *For All Practical Purposes*. Freeman, 2009.
Hay traducción al español de la edición de 1994:
COMAP. *Las matemáticas en la vida cotidiana*. Addison-Wesley, Universidad Autónoma de Madrid, 1994.
Ver también el sitio <http://bcs.whfreeman.com/fapp7e/>.
- [3] Fernández, P. *El secreto de Google y el Álgebra lineal*. Boletín de la Sociedad Española de Matemática Aplicada, 2004, 30, pp. 115-141
Está disponible en el sitio http://www.uam.es/personal_pdi/ciencias/gallardo/upm_google.pdf
- [4] Flores-Bazán, F. *Optimización Lineal: una mirada introductoria*. J.C. Sáez Editor, Santiago, 2011.
- [5] Gajardo, P. *Modelando Fenómenos de Evolución*. J.C. Sáez Editor, Santiago, 2011.
- [6] Gil, O. *Curso aceleradísimo de Álgebra Lineal*. En línea, 2009.
Está disponible en el sitio web del autor.
- [7] Gil, O. *Nociones de análisis de Fourier discreto, con aplicaciones*. En línea, 2009.
Está disponible en el sitio web del autor.
- [8] Labra, A., Suazo, A. *Elementos de la Teoría de Cuerpos*. J.C. Sáez Editor, Santiago, 2011.
- [9] Lay, D. *Linear Algebra and its Applications*. Addison-Wesley, 2003.
Hay traducción al español:
Lay, D. *Álgebra Lineal y Aplicaciones*. Pearson, 2007.
Ver también el sitio web www.laylinalgelbra.com/
- [10] Lacourly, N. *Estadística Multivariada*. J.C. Sáez Editor, Santiago, 2011.
- [11] Lewin, R. *Introducción al Álgebra*. J.C. Sáez Editor, Santiago, 2011.
- [12] Hildebrandt, S., Tromba, A. *Matemática y Formas Óptimas*. Prensa Científica, 1990.
- [13] Moreno, A., Ramírez, H. *Grafos: Fundamentos y Algoritmos*. J.C. Sáez Editor, Santiago, 2011.
- [14] Olver, P., Shakiban, C. *Applied Linear Algebra*. Prentice Hall, 2005.
- [15] Osses, A. *Análisis Numérico*. J.C. Sáez Editor, Santiago, 2011.
- [16] Strang, G. *Linear Algebra and Its Applications*. Academic Press, 1976.
Hay traducción al español:
Strang, G. *Álgebra Lineal y sus aplicaciones*. Addison-Wesley, 1986.
- [17] Trefethen, L., Bau, D. *Numerical linear algebra*. SIAM, 1997.

Índice de figuras



1.1. Parejas de números de Fibonacci consecutivos	25
2.1. Dos redes sencillas	46
2.2. Discos de Gerschgorin y valores propios de la matriz que genera los números de Fibonacci	54
2.3. Matriz de consumo para una economía	72
3.1. Proyección de $(0, 1)$ sobre $(\sqrt{3}/2, 1/2)$	79
3.2. Base ortonormal (e_r, e_φ)	83
3.3. Base ortonormal $(e_r, e_\varphi, e_\theta)$	84
3.4. Proyección de $(0, 0, 1)$ sobre \mathbb{S}	89
3.5. La base \mathcal{A}	95
3.6. La base $\mathcal{A}^{(1)}$	96
3.7. Las bases \mathcal{Q} y \mathcal{O} .	98
4.1. La elipse definida por (4.10)	111
4.2. La elipse definida por (4.10) vista en los ejes (y_1, y_2)	113
4.3. La parábola definida por (4.10), y los ejes correspondientes a los distintos sistemas de coordenadas usados para su reconocimiento.	114
4.4. S^1 y su imagen por M	121
4.5. La imagen de S^1 variando con ϵ .	130
4.6. Un “HOLA” algo ruidoso	133
4.7. Los valores singulares del “HOLA” algo ruidoso	134
4.8. Reconstrucción de rango 4 del “HOLA” ruidoso	135
5.1. Transiciones en una población.	141
5.2. Transiciones entre consonantes y vocales en <i>Evgueni Onegin</i>	144

Índice de Notaciones



- A, B , matrices. En general con columnas linealmente independientes que forman una base \mathcal{A} o \mathcal{B} de algún subespacio, 29, 33
 A^{-1} , inversa de la matriz A , 29
 A_i , i -ésima columna de la matriz A , 31
 D , matriz diagonal, 30
 I_n , matriz identidad $n \times n$, 175
 J , matriz en alguna forma canónica, 59–61, 120
 M, N , matrices, 24
 $M = M = \tilde{V}\tilde{\Sigma}\tilde{U}^\top$, forma reducida de la SVD, 133
 $M = QDQ^\top$, diagonalización de una matriz simétrica, 109
 $M > N$, relación de orden en que todas las entradas de M son mayores que las de N , 73
 M^+ , pseudoinversa, 104, 141
 M^\top , matriz traspuesta de una matriz M , 77
 M^k , potencia k -ésima de una matriz M , 65
 M_k , sucesiones de matrices, 35
 $M_k \rightarrow M$, sucesión de matrices M_k convergiendo a una matriz límite M , 35
 O, Q , matrices ortogonales, 82
 O , matriz ortogonal, 82
 $O^\top X$, coordenadas de X en la base ortonormal formada por las columnas de O , 82
 $P_{\mathbb{S}}(X)$, proyección ortogonal de X sobre \mathbb{S} , 88
 QR , descomposición QR de una matriz, 99
 S^1 , circunferencia unidad, 123
 S^1 , conjunto de vectores de módulo 1 en \mathbb{R}^2 , circunferencia unidad, 37
 S^2 , conjunto de vectores de módulo 1 en \mathbb{R}^3 , esfera unidad, 37
 S^{n-1} , conjunto de vectores de módulo 1 en \mathbb{R}^n , 37
 S^{n-1} , esfera unidad en \mathbb{R}^n , 127
 $V\Sigma U^\top$, SVD de M , 126
 X , vector, 28
 $X = (x_1, x_2, \dots, x_n)$, vector de \mathbb{R}^n , 174
 $X \cdot Y$, producto escalar, 37, 176
 $X \mapsto MX$, transformación que al vector X le asocia el producto MX de la matriz M por X , 28, 43, 174
 $X_{\mathcal{A}}$, coordenadas de X en la base \mathcal{A} , 28
 X_k , sucesión de vectores, 36
 Z , vector complejo, 63
 $[n, k, d]$, parámetros de un código lineal, 166
 $[x_1 \ x_2 \ \dots \ x_n]^\top$, columna $n \times 1$ (naturalmente identificada con un vector de \mathbb{R}^n), 174
 $\Im(Z)$, vector parte imaginaria de un vector complejo, 63
 $\Re(Z)$, vector parte real de un vector complejo, 63
 Σ , matriz diagonal con los valores singulares de una matriz M , 126
 $\det(M)$, determinante de una matriz cuadrada M , 50
 $\ker(M)$, núcleo de una matriz M , 50
 $\lim_{k \rightarrow \infty} M_k = M$, la matriz M es el límite de la sucesión M_k , 35
 \mathbb{C} , conjunto de los números complejos, 173

$\mathbb{GF}(q)$, cuerpo de Galois con q elementos, 178
 \mathbb{K} , cuerpo cualquiera, 170, 173
 \mathbb{R} , conjunto de los números reales, 173
 \mathbb{R}^2 , conjunto de las parejas ordenadas de números reales, 25
 \mathbb{R}^n , conjunto de las n -uplas de números reales, 28, 173
 \mathbb{S} , subespacio, 175
 \mathbb{S} , subespacio vectorial, 28
 \mathbb{Z}_2 , cuerpo finito con los símbolos 0 y 1, 155
 \mathcal{A}, \mathcal{B} , conjuntos de vectores. En general, una base de algún subespacio, 28
 \mathcal{C} , base canónica, 28, 175
 \mathcal{O} , base ortonormal, 82
 \mathcal{O} , familia ortonormal, 80
 \mathcal{Q} , familia ortogonal, 80
 \mathcal{S}^\perp , conjunto ortogonal a \mathcal{S} , 91
 \mathcal{X} , conjunto genérico, 39
 \mathcal{X}^n , listas de n elementos de \mathcal{X} , 40
 \overline{Z} , vector conjugado de un vector complejo, 63
 \overline{z} , conjugado del complejo z , 38
 σ_1 , mayor valor singular, 133
 σ_i , valores singulares, 125
 $\varphi(X) = X^\top MX$, forma cuadrática, 111
 $d(x, y)$, distancia entre x e y , 39
 e^{Mt} , exponencial de una matriz, 75
 e_i , i -ésimo vector en \mathcal{C} , 175
 f_n , números de Fibonacci, 23
 $p(\lambda)$, polinomio característico de una matriz, 51
 $r(M)$, radio espectral de una matriz M , 66
 $s(y)$, síndrome de Y , 169
 $w(X)$, peso de la palabra X , 168
 $x_{k,i}$, i -ésimo coeficiente del vector X_k en una sucesión de vectores, 37
 z , número complejo, 38
 (e_r, e_φ) , base ortonormal asociada a las coordenadas polares, 82
 $(e_r, e_\varphi, e_\theta)$, base ortonormal asociada a las coordenadas esféricas, 83
 (e_r, e_φ, e_z) , base ortonormal asociada a las coordenadas cilíndricas, 83
SVD, descomposición en valores singulares, 122

Índice de autores



- Arrow, Kenneth (1921), 48
 Beltrami, Eugenio (1835-1900), 122
 Berlekamp, Elwyn (1940-), 170
 Bessel, Friedrich (1784-1846), 93
 Brin, Serguei (1973), 45
 Brown, Robert (1773-1858), 146
 Buniakovsky, Viktor (1804-1889), 78

 Cauchy, Agustín (1789-1857), 121, 179
 Cauchy, Agustín (1789-1857), 37, 77
 Cayley, Arthur (1821-1895), 121

 de Fermat, Pierre (1601-1665), 121
 Descartes, René, 121

 Einstein, Albert (1879-1955), 147
 Euclides (~325 AC, ~265 AC), 78

 Fibonacci (Leonardo de Pisa) (1170-1250), 23
 Frobenius, Georg (1849-1917), 75

 Galois, Evaristo (1811-1832), 178
 Gelfand, Israel (1913-2009), 122
 Gerschgorin, Semyon (1901-1933), 52
 Gibbs, Josiah Williard (1839-1903), 78
 Golay, Marcel (1902-1989), 167, 168
 Golub, Gene (1932-2007), 122
 Gramm, Jorgens (1850-1916), 95

 Hamilton, William Rowan (1805-1865), 77
 Hamming, Richard (1915-1998), 40, 158
 Heaviside, Oliver (1850-1925), 77
 Heisenberg, Werner (1901-1976), 122
 Hilbert, David (1862-1943), 78, 122

 Jacobi, Carl (1804-1851), 68
 Jordan, Camille (1838-1922), 61, 122

 Kronecker, Leopold (1823-1891), 175
 Lagrange, Joseph Louis (1736-1813), 77
 Leontief, Wassily (1905-1999), 49, 72

 Markov, Andrei (1856-1922), 146

 Page, Larry (1973), 45
 Parseval, Marc Antoine (1755-1836), 93
 Perron, Oskar (1880-1975), 74
 Pitágoras (~569AC-~475AC), 77, 86

 Reed, Irving (1923-, 170

 Schmidt, Erhard (1876-1959), 95, 122
 Schrödinger, Erwin (1887-1961), 122
 Schwarz, Hermann (1843-1921), 37, 78
 Shannon, Claude (1916-2001), 158
 Singleton, Richard (1928-2007), 165, 170
 Solomon, Gustave (1930-1996), 170

 von Neumann, John (1903-1957), 122
 Wiener, Norbert (1894-1965), 146

Índice de Términos



- byte*, 156
- algoritmo
 - de Gramm-Schmidt, 95
- alternativa de Fredholm, 94
- análisis de componentes principales, 138
- base canónica, 175
- bases, 174
- bit, 156
- borradura, 157
- código, 162
 - de Golay, 167
 - de repetición, 157
 - dual, 172
 - simplex, 172
- códigos
 - de Hamming $[2^m - 1, 2^m - m - 1, 3]$, 169
 - lineales, 166
 - lineales $[n, k, d]$, 166
- cónicas, 112
- cadena de Markov, 145
 - estacionaria, 146
- cadena de Markov, 143
- circunferencia unidad, 123
- codificación, 162
- completitud, 179
 - de \mathbb{R} , 179
 - de \mathbb{R}^n , 179
- conjugado
 - de un número complejo, 38
 - de un vector, 63
- conjunto ortogonal
 - a un conjunto dado, 91
- contracciones, 180
- control de paridad, 156
- convergencia, 35
 - respecto a una distancia, 40
 - respecto a una norma, 36
- coordenadas, 175
 - cilíndricas, 83
 - polares, 82
 - esféricas, 83
- corregir *e* errores, 158
- cota de Singleton, 165
- cuerpo, 177
 - finito, 155, 177
- dígitos de control, 156
- decodificación
 - por síndromes, 169
 - por vecino más próximo, 163
- delta de Kronecker, 175
- descomposición QR , 99
- Descomposición en valores singulares (ver SVD), 122
- desigualdad de Cauchy-Schwarz, 37
- discos de Gerschgorin, 52
- distancia, 39
 - del taxista, 39
 - inducida por una norma, 39
- distancia de Hamming, 40
- distancia en \mathbb{R}^n , 85
- distancia mínima
 - en un código, 164
- ecuaciones diferenciales, 60, 75
- ecuaciones normales, 104
- eliminación gaussiana, 100, 102
- equilibrio dinámico, 145
- error, 157

- esfera unidad, 37, 127
- espacio afín, 78
- espacio euclídeo, 78
- espacio vectorial \mathbb{R}^n , 173
- espacios de Hilbert, 78
- estado de una población, 143
- estado estacionario, 145
- estado inicial, 144
- factorización, 31, 56, 78, 100, 109, 126, 132
- familia
 - ortogonal, 80
 - ortonormal, 80
- forma canónica de Jordan, 60
- forma canónica real, 64
- formas cuadráticas, 111
- geometría
 - del taxista, 39
- independencia lineal, 174
- isometrías, 41
 - en \mathbb{R}^n , 85
- método
 - de Jacobi, 68
 - de las potencias, 68
 - de mínimos cuadrados, 102
- método iterativo, 70
- módulo de un vector, 37
- matrices
 - con diagonal dominante, 56, 70
 - diagonalizables, 56
 - nilpotentes, 55
 - normales, 117
 - semejantes, 30
- matriz
 - $m \times n$, 173
 - de codificación, 167
 - de conectividad, 45
 - de consumo de una economía, 72
 - de control, 167
 - de orden n , 173
 - de transición, 145
 - diagonal, 30
 - exponencial, 60, 75
 - ortogonal, 82
 - regular de transición, 152
- modelo, 143
- movimiento browniano, 146
- multiplicidad
 - algebraica de un valor propio, 51
 - geométrica de un valor propio, 44
- mínimos cuadrados, 78
- número de condición, 105, 131
- números de Fibonacci, 24
- norma, 36
- normalizar un vector, 80
- orden de nilpotencia, 55
- ortonormalidad, 80
- palabras, 157
 - código, 162
- parte imaginaria
 - de un vector, 63
- parte real
 - de un vector, 63
- peso de una palabra, 168
- polinomio característico, 51
- producto
 - vectorial, 78
- producto escalar
 - en \mathbb{C}^n , 38
 - en \mathbb{R}^n , 37
- proyección ortogonal, 88
- punto fijo, 180
 - de una función, 50
- radio espectral, 66, 70
- razón áurea, 26
- reducción de dimensionalidad, 138
- residuo, 106
- síndrome, 169
- serie geométrica, 71
- seudoinversa, 104, 141
- signo de una forma cuadrática, 112
- sistema incompatible, 102

- solución
 - por mínimos cuadrados, 103
- subespacio
 - invariante, 32, 45, 149
- sucesiones
 - de matrices, 35
- sucesiones de Cauchy, 179
- SVD, 122
 - forma reducida, 133
 - forma vectorial, 125
 - versión vectorial, 124
- teorema
 - de Frobenius, 75
 - de Perron, 75
 - de punto fijo, 179
 - espectral, 109
- transiciones, 143
- valor propio, 43
- valores propios, 25
- valores singulares, 39, 125
 - multiplicidad, 125
 - y rango, 125
- vecino más próximo, 163
- vector
 - de probabilidad, 145
- vector propio, 43
- vectores
 - de probabilidad, 148
 - ortogonales, 77
- vectores propios, 25