

线性代数

余成龙, 郑志伟

2026 年 6 月 12 日

目录

1	线性方程组	11
1.1	网页排序算法和线性方程组	11
1.2	列向量空间与线性函数	13
1.3	高斯消元法和最简阶梯型	20
1.4	线性方程组解的结构, 自由元和主元	28
1.5	线性方程组的相容性和确定性	30
1.6	选讲: 最简行阶梯型唯一性的证明	32
1.7	挑战选读: 舒伯特胞腔的计数	33
1.8	习题	37
2	矩阵运算	42
2.1	加法, 数乘与乘法	42
2.2	行变换和矩阵乘法	45
2.3	矩阵的逆	47
2.4	矩阵的转置	49
2.5	秩在行列变换下的不变性	50
2.6	分块矩阵	51
2.7	选读: 快速傅立叶变换	57
2.8	习题	64
3	线性空间	73
3.1	\mathbb{R}^n 的子空间	73
3.2	零空间和线性生成	74
3.3	仿射空间	78
3.4	\mathbb{R} -线性空间	78

3.5	线性相关性	82
3.6	基与维数	89
3.7	向量的坐标表达	94
3.8	线性空间的构造, 和, 交	98
3.9	商空间	102
3.10	习题	105
4	线性映射	110
4.1	定义与例子	110
4.2	线性映射与矩阵	113
4.3	线性同构	117
4.4	核, 像与维数公式	118
4.5	线性映射下的子空间和商空间	121
4.6	习题	125
5	行列式	133
5.1	定义与基本性质	133
5.2	行列式的计算方法	141
5.3	伴随矩阵	145
5.4	Laplace 公式与 Cauchy-Binet 公式	147
5.5	习题	150
6	选读: 域上的线性空间	160
6.1	域	160
6.2	域上的线性空间	163
6.3	域扩张与维数的乘法公式	164
6.4	复数结构与实线性变换	165
6.5	选读: 代数数与多项式商空间 *	166
6.6	选读: 有限域上的 Grassmannian 计数 *	167
6.7	选读: 微扰法的代数化: 有理函数域方法 *	170
6.8	习题	172
7	多项式	178
7.1	多项式环	178
7.2	带余除法与整除	178
7.3	最大公因式与辗转相除法	179
7.4	裴蜀定理与互素	181

7.5	不可约多项式与唯一分解定理	182
7.6	多项式的根与形式导数	183
7.7	习题	184
8	线性变换和特征值理论	188
8.1	特征值与特征向量	189
8.2	不变子空间和上三角化	191
8.3	矩阵的相似与对角化	193
8.4	选读: PageRank、Markov 链与阻尼因子	196
8.5	代数重数与几何重数	199
8.6	Cayley-Hamilton 定理	200
8.7	极小多项式	201
8.8	友阵	205
8.9	计算示例	209
8.10	习题	210
9	双线性型与二次型	219
9.1	双线性型与格拉姆矩阵	219
9.2	对称双线性型与二次型	222
9.3	非退化性与正交补	225
9.4	Sylvester 惯性定理与正定性	227
9.5	反对称双线性型与辛矩阵	229
9.6	习题	231
10	内积空间与谱定理	240
10.1	内积空间	240
10.2	Gram-Schmidt 正交化与 QR 分解	243
10.3	正交变换与正交群	244
10.4	实对称矩阵的谱定理	245
10.5	正交矩阵的分类	249
10.6	厄米特型和酉矩阵	251
10.7	应用: 二次曲线与二次曲面	258
10.8	习题	260
11	应用选读: 奇异值分解及其应用	270
11.1	奇异值分解	271
11.2	低秩逼近与应用	276

11.3 应用: 低维拟合与主成分分析 (PCA)	284
11.4 应用场景: 最小二乘法	289
11.5 习题	293
12 应用选读: Transformer: 从内积、矩阵乘法到语言生成	298
12.1 Transformer 模型的训练过程概览	299
12.2 神经网络的基础结构	300
12.3 注意力机制: 从整句编码到选择性读取	302
12.4 从词元到矩阵: 语言如何进入向量空间	302
12.5 位置编码: 矩阵的行还需要顺序信息	304
12.6 从格拉姆矩阵到注意力: 内积一次性计算所有相似度	305
12.7 Softmax: 把分数矩阵变成行随机矩阵	306
12.8 查询、键、值向量: 为什么不是直接使用 XX^T	308
12.9 因果遮罩: 训练时如何避免使用未来信息	310
12.10多头注意力	311
12.11Transformer 块: 残差连接、层归一化和前馈网络	311
12.12输出层: 隐藏向量如何变成下一个词元概率	314
12.13训练: 从下一个词元预测到矩阵参数优化	315
12.14生成: 模型如何一个词元一个词元输出文本	321
12.15KV 缓存: 自回归生成中的矩阵分块复用	322
12.16一个小型语言模型的完整数学流程	323
12.17Transformer 模型的主要特点	324
12.18习题	325
13 挑战选读: 若尔当标准型	329
13.1 广义特征子空间分解	330
13.2 幂零变换的若尔当标准型	331
13.3 若尔当标准型定理	338
13.4 矩阵次幂的计算和应用: 递推数列的通项公式	339
13.5 习题	342
14 选读: 矩阵函数和常微分方程	350
14.1 矩阵的幂级数与矩阵指数	350
14.2 若尔当块上的矩阵函数	352
14.3 常系数线性常微分方程组	352
14.4 高阶标量 ODE 的矩阵降阶法	356
14.5 系统的稳定性	358

14.6 习题	366
15 挑战选读: 有理标准型	372
15.1 准素分解	373
15.2 $p(T)$ -拟幂零变换的结构	374
15.3 有理标准型定理	377
15.4 与若尔当标准型的统一	378
15.5 计算示例	379
15.6 习题	382

前言

线性代数是现代数学最基础也最具渗透力的分支之一。它不仅是代数学、几何学、分析学、概率论和数论等众多数学领域的共同语言，也是物理学、工程学、计算机科学、经济学乃至生物学的核心工具。从量子力学中的态空间、机器学习中的注意力机制，到数据科学中的主成分分析，线性代数的思想和方法无处不在。学习线性代数，就是在学习一种刻画“线性结构”的思维方式——这种思维方式将帮助你理解高维空间中的几何、分析非线性问题的局部近似、以及设计高效的数值算法。

历史：从算法到结构

线性代数的历史可以追溯到两千年前。中国汉代的数学典籍《九章算术》（约公元前 200 年至公元 200 年之间）中，已有一整章“方程”专门讨论多元一次方程组的解法。书中将方程组系数排成方阵，通过“遍乘直除”逐步消元，所用算法与今天的高斯消元法完全一致。值得一提的是，当时的计算者用竹筹在方形格板上摆出数字阵列，红筹代表正数，黑筹代表负数——这或许是历史上最早的“矩阵操作”。这一算法比欧洲数学家高斯的系统化工作早了整整一千八百年。

在欧洲，行列式的研究先于矩阵代数的诞生。**莱布尼茨**（Leibniz, 1693 年）在写给洛必达的一封信中，首次使用行列式的记号来判断方程组是否有解。1750 年，**克莱默**（Gabriel Cramer）发表了以其名字命名的法则，同时引出了一个著名的悖论。用后来的**贝祖定理**（Bézout's theorem）来表述，两条 n 次平面曲线最多有 n^2 个交点，因此两条三次曲线最多相交于 $3^2 = 9$ 个点。另一方面，一条三次曲线由 10 个系数决定，除去整体倍数，相当于有 9 个自由参数；因此从计数上看，9 个点似乎足以唯一确定一条三次曲线。然而，如果这 9 个点本身正是两条三次曲线的交点，那么这两条曲线的任意线性组合仍然经过这 9 个点，于是通过这些点的三次曲线并不唯一，而是形成一个一维参数族。这表明，这 9 个交点的分布并不是完全自由的。克莱默本人无法对此给出令人满意的解释。这个**克莱默悖论**（Cramer's paradox）刺激了后来者深入研究齐次线性方程组的解空间结构，最终成为线性代数发展的推动力之一。

拉普拉斯（Laplace, 1772 年）给出了行列式按行展开的一般公式；**柯西**（Cauchy, 1812 年）第一次用现代符号系统地整理了行列式理论，证明了乘积公式 $\det(AB) = \det A \cdot \det B$ 。而真正将线性代数带入公众视野的，是一个关于**高斯**（Carl Friedrich Gauss）和一颗小行星的戏剧性故事。

1801 年元旦，意大利天文学家皮亚齐（Piazzi）在西西里岛观测天空时，发现了一颗前所未见的亮点——后来命名为**谷神星**（Ceres）。他追踪了 41 天后，谷神星便消失在太阳的强光中。当时全欧洲的天文学家都急切地想预测它下次出现的位置，然而多数人用的古典方法需要更长的观测弧，41 天的数据远远不够。年仅 24 岁的高斯不慌不忙，悄悄拿出了他自

已发明但从未公开发表的一套方法——**最小二乘法** (method of least squares)：将观测数据建立超定方程组，然后寻找使各方程误差平方和最小的解。用这套方法，他在几个月内算出了谷神星的轨道。1801年12月7日，天文学家冯·察赫 (Franz Xaver von Zach) 将望远镜对准高斯所预言的方向，谷神星赫然出现。这一事件令高斯一夜成名，也让最小二乘法——乃至其背后的线性方程组理论——得到了整个欧洲科学界的高度重视。

矩阵作为独立的代数对象，直到19世纪中叶才从行列式的背景中独立出来。**西尔维斯特** (James Joseph Sylvester, 1850年) 创造了“matrix” (矩阵) 一词，取其拉丁语“子宫/母体”之意，因为行列式可以从矩阵中“生育”出来。他的挚友与合作者**凯莱** (Arthur Cayley, 1858年) 系统发展了矩阵代数，定义加法、数乘与乘法，并对 2×2 和 3×3 矩阵验证了后来以他命名的**凯莱-哈密顿定理**：每个矩阵均满足其自身的特征方程。对于一般阶数，凯莱在论文中写道：“我没有认为有必要为一般情形的定理进行正式证明” (*I have not thought it necessary to undertake the labour of a formal proof*)。这个慵懒但诚实的笔记，让后来的数学家整整忙碌了数十年。

同时代的**格拉斯曼** (Hermann Grassmann, 1844年) 走了一条更为曲折的道路。他在《线性扩张论》 (*Die lineale Ausdehnungslehre*) 中建立了高维几何的代数语言，引入外积和多重线性结构——实质上是今天外代数 (exterior algebra) 的完整框架。然而这部著作在当时几乎无人能读懂。数学界的审稿人认为它“充满哲学玄思而缺乏严格性”，将其束之高阁。备受冷落的格拉斯曼转而研究梵文，成为享有声誉的语言学家——他对梵语语音规律的发现 (“格拉斯曼定律”) 反而在语言学界广为人知。格拉斯曼在数学上的天才，直到他去世数十年后才被外微分形式理论和现代物理所重新发现。

皮亚诺 (Giuseppe Peano, 1888年) 第一次用公理化方式定义了抽象向量空间 (加法、数乘、封闭性、零元……)，标志着现代线性代数从具体计算走向抽象结构。

20世纪初，**希尔伯特** (Hilbert) 将线性代数推广到无穷维的函数空间，建立了泛函分析和谱理论。1925到1927年间，海森堡、玻恩等人创立量子力学，发现力学量必须用**不对易的算符** (矩阵) 来描述——海森堡甚至最初不知道他所发明的“乘法体系”就是矩阵乘法。**冯·诺伊曼** (von Neumann) 随即将量子力学的数学基础公理化：物理状态是希尔伯特空间中的向量，可观测量是自伴算子，测量结果是特征值。线性代数的特征值理论，就这样成为了整个现代物理的语言骨架。

进入计算机时代，线性代数重新焕发活力。矩阵分解——LU分解、QR分解、奇异值分解——成为科学计算的基础算法。2012年以来，**深度学习**的革命在很大程度上就是线性代数的胜利：神经网络的前向传播是一系列矩阵乘法，梯度下降是向量微积分，注意力机制是对查询向量与键向量内积的软化选择……可以说，现代人工智能的数学心脏，就是线性代数。

本书的思路与特色

本书以**线性方程组**作为出发点,以**高斯消元法**作为贯穿始终的核心计算工具,逐步建立起线性代数的完整理论体系.

与许多传统教材先花大量篇幅引入行列式不同,本书有意地将行列式的系统讨论推迟到较后面的位置.这一安排基于如下考量:线性代数中许多核心概念——矩阵的秩、行秩等于列秩、线性方程组解的结构——都可以也应当通过高斯消元法来自然地定义和证明,而不必依赖行列式这一“黑箱式”的工具.高斯消元法不仅计算上高效,而且概念上透明,学生可以从清楚地看到每一步的几何含义.当我们在后续章节正式引入行列式时,将从交错多重线性函数的几何意义出发,使学生体会到行列式的定义和性质是多么自然和必要.

本书的核心学习路线是

线性方程组 \rightarrow 矩阵运算 \rightarrow 线性空间与线性映射 \rightarrow 行列式与特征值 \rightarrow 内积空间与谱定理.

围绕这条主线,书中还穿插若干应用选读和挑战选读内容.这些内容用于展示线性代数通向现代数学和应用的方向,但初次阅读时不需要全部掌握.

全书内容概览

全书正文按十五章组织主线内容,并在相关位置穿插若干选读、应用选读和思考题材料,大致可分为如下几个板块:

板块一: 线性方程组与矩阵运算 (§1–§2). 第1章从实际问题(网页排序算法)出发引入线性方程组,发展高斯消元法,建立最简行阶梯型理论,并完整讨论线性方程组解的结构.第2章系统介绍矩阵的加法、数乘、乘法、逆和转置等代数运算,将初等行变换用矩阵乘法的语言重新表达,并证明秩在行列变换下的不变性.这两章为后续所有章节提供了计算基础.

板块二: 线性空间与线性映射 (§3–§4). 第3章从 \mathbb{R}^n 的子空间出发,抽象出一般线性空间的公理化定义,引入线性相关性、基、维数等核心概念,并讨论子空间的和、交与商空间.第4章定义线性映射,建立线性映射与矩阵之间的对应关系(表示矩阵),证明维数公式(秩-零度定理),并讨论相似变换、第一同构定理和相抵标准型.这两章将前面具体的矩阵计算提升到更抽象、更统一的理论框架.

板块三: 行列式 (§5). 第5章从有向面积的几何直观出发,将行列式定义为归一化的交错多重线性函数,并严格证明这一函数空间是一维的——从而保证了行列式的存在唯一性.在此基础上建立余子式展开、行化简法、分块矩阵行列式公式、伴随矩阵与Cramer法则等计算工具,以及更一般的Laplace公式和Cauchy-Binet公式.本章还补充了排列与逆序数的代数背景,以及通过子式刻画矩阵秩的等价定义.

板块四: 域、多项式与特征值理论 (§6–§8). 第6章将线性代数的理论从实数域推广到一般域,讨论域扩张、复数结构和有限域等内容.第7章系统介绍一元多项式环的基本理

论——带余除法、最大公因式、不可约分解和重根判定——为后续特征多项式和极小多项式的讨论做好准备. 第 8 章是代数理论的核心, 引入特征值与特征向量, 讨论不变子空间、上三角化、可对角化条件, 以及 Cayley-Hamilton 定理和极小多项式.

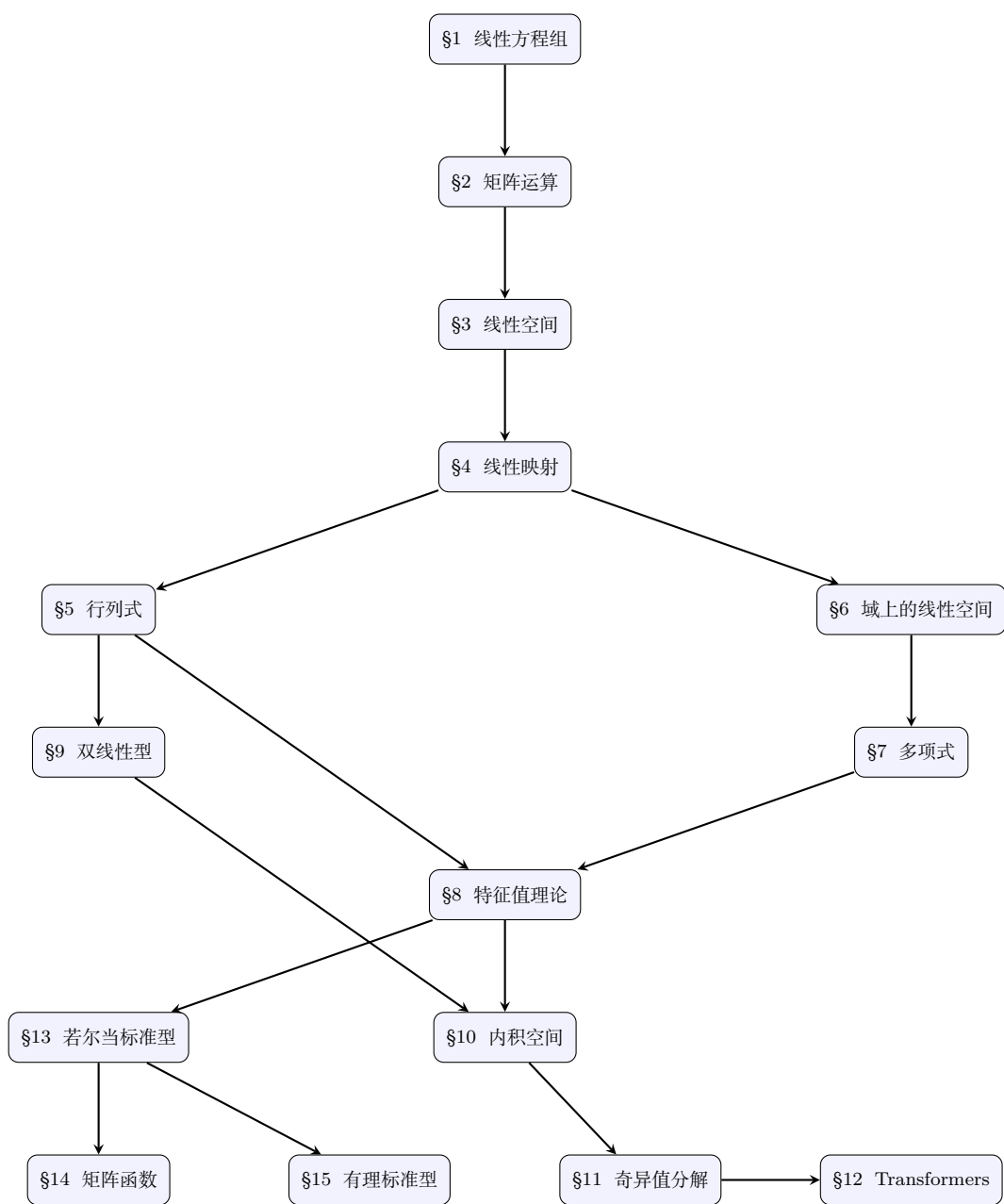
板块五: 双线性型、内积空间与谱定理 (§9–§10). 第 9 章引入双线性型和二次型, 讨论对称双线性型的对角化 (Sylvester 惯性定理) 和正定性. 第 10 章在此基础上引入内积空间, 发展正交性理论, 证明实对称矩阵的谱定理, 并讨论正交变换、酉变换的分类, 以及二次曲线和曲面的应用.

板块六: 奇异值分解及应用 (§11–§12). 第 11 章建立矩阵的奇异值分解 (SVD), 证明其存在性和唯一性, 并讨论低秩逼近 (Eckart-Young 定理)、主成分分析 (PCA) 和最小二乘法等重要应用. 第 12 章以 Transformers 和注意力机制为主题, 展示线性代数在现代深度学习中的核心作用.

板块七: 若尔当标准型及推广 (§13–§15). 第 13 章从广义特征子空间分解出发, 先处理幂零情形, 再建立一般的若尔当标准型定理, 并给出矩阵次幂和递推数列通项公式等应用. 第 14 章利用若尔当型定义矩阵的幂级数和矩阵指数, 并将其应用于常系数线性常微分方程组的求解和系统稳定性分析. 第 15 章引入有理标准型, 通过准素分解给出另一种标准型理论, 并讨论其与若尔当标准型的统一.

章节依赖关系

本书的章节之间存在如下逻辑依赖关系:



其中最核心的主线为: 线性方程组 → 矩阵运算 → 线性空间 → 线性映射 → 行列式/特征值 → 内积空间与谱定理. 标注为“选读”、“应用选读”、“挑战选读”或归入“思考题”的内容可在初次阅读时跳过, 不影响主线的学习.

余成龙 郑志伟

1 线性方程组

1.1 网页排序算法和线性方程组

线性代数的一个中心问题是求解线性方程组。我们首先通过谷歌的网页排序模型来说明如何建立线性方程组，求解线性方程组，以及在现实生活中通常会想要了解方程组的哪些性质。这里的目标只是引出线性方程组；等具备矩阵运算、特征值和矩阵幂等工具之后，我们会再回到 PageRank 并做更系统的讨论。

我们现在每天使用的互联网在 20 世纪 90 年代迅速发展，网络上的信息呈爆炸式增长，如何有效地检索和组织这些海量信息成为了亟待解决的问题。早期的搜索引擎如 Archie (1990)、Gopher (1991) 和 WebCrawler (1994) 主要依赖关键词匹配和简单的文本分析，但这种方法面临着严重的局限性：搜索结果往往充斥着大量低质量网页，而真正有价值的信息却淹没其中。更为棘手的是，网站所有者很快发现可以通过堆砌关键词等手段操纵搜索排名，使得搜索质量进一步下降。

这一困境的核心在于：如何在缺乏中心化权威的互联网环境中，自动判断网页的重要性和可信度？传统的文本分析方法只能告诉我们一个网页“谈论了什么”，却无法回答“这个网页是否值得信赖”这一关键问题。正是在这样的背景下，1998 年，斯坦福大学的博士生拉里·佩奇 (Larry Page) 和谢尔盖·布林 (Sergey Brin) 提出了一个革命性的想法：网页之间的链接关系本身就蕴含着价值判断——当一个网页链接到另一个网页时，这可以被视为一种“投票”或“推荐”。基于这一洞察，他们开发了 PageRank 算法，将网页排名问题转化为一个优雅的线性代数问题。这一算法也奠定了谷歌作为搜索引擎的核心竞争力。

我们通过一个简化模型来说明其基本原理：假设有四个网页 1、2、3、4，它们之间的超链接关系如下图所示：

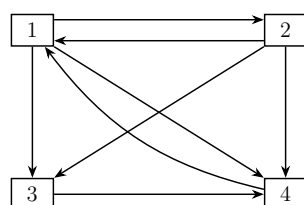


图 1: 网页链接关系示意图

其中 x_i 表示第 i 个网页的重要性分数。对于 1 号网页，其重要性分数（流量）被均分为三部分，分别流向 2、3、4 号网页：

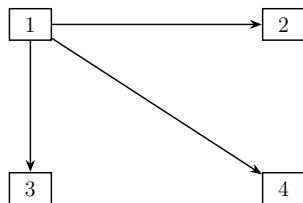


图 2: 1 号网页的流量分配

同时, 1 号网页也从 2 号和 4 号网页接收流量:

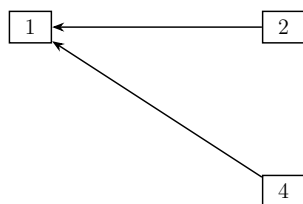


图 3: 1 号网页的流量输入

为简化模型, 我们假设流出的流量是平均分配的. 根据网页间的超链接关系, 可以建立如下线性方程组来描述各网页的重要性分数:

$$\begin{cases} x_1 = \frac{1}{3}x_2 + x_4 & (1 \text{ 号网页的流量平衡}) \\ x_2 = \frac{1}{3}x_1 & (2 \text{ 号网页的流量平衡}) \\ x_3 = \frac{1}{3}x_1 + \frac{1}{3}x_2 & (3 \text{ 号网页的流量平衡}) \\ x_4 = \frac{1}{3}x_1 + \frac{1}{3}x_2 + x_3 & (4 \text{ 号网页的流量平衡}) \end{cases}$$

我们用如下方式求解这个方程组, 将第二个方程代入第三个方程, 我们得到 $x_3 = \frac{4}{9}x_1$. 将第二个方程代入第一个方程, 我们得到 $x_4 = \frac{8}{9}x_1$. 用一个新的变量 t 来替代 x_1 , 则任意一个解一定长成如下的形式:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} t \\ \frac{1}{3}t \\ \frac{4}{9}t \\ \frac{8}{9}t \end{pmatrix}$$

其中 t 为某一个实数. 代入原方程组检验, 我们发现任意这种形式的四元组都是一个解. 这表明所有网页的重要性分数具有固定的比例关系. 另一方面, 从建立方程的过程来看, 由于我们没有设置重要性的度量单位, 这一方程组的所有解也应当只能说明网页之间的相对重

要性, 所以得到所有成比例的解也是合理的. 假设重要性是一个大于零的数, 例如代入任何大于零的 t 值, 我们得到重要性排序为 $x_1 > x_4 > x_3 > x_2$.

以上就是一个线性方程组的例子. 对于一般的 n 个网址的网络连接方式, 类似的方法都能建立起一组关于这 n 个未知数的同样个数的方程. 那么自然的问题是这样的方程组是不是都有解, 以及是不是所有解都长成类似刚才这个例子的形式, 从而决定我们所有网页的重要性的比例关系. 事实是, 我们的网络连接图需要满足一定条件这个结论才对. 例如网络如果不连通, 那么不同连通分支之间的相对重要性就得不到了. 刚才在求解过程中, 我们还观察到最后一个方程在求解过程中没有被用到, 也就是多余的. 这里多余的限制条件数目恰好对应了自由的变量 t 的个数. 这种现象也会在之后线性方程组的理论中被严格的陈述和解释. 本章只把 PageRank 看作一个建立并求解线性方程组的例子; 在掌握矩阵运算和特征值理论之后, 我们会把它解释为 Markov 链的平稳分布, 并说明阻尼因子如何改善收敛性.

1.2 列向量空间与线性函数

方程组通常写作某个集合或者空间上定义的某种类型的函数等于某个值的形式. 我们需要了解这个空间上有什么结构, 这类函数如何刻画, 以及求解的方法. 本节将从三个基本问题出发, 系统介绍列向量空间, 线性函数的概念, 然后在下一节中介绍线性方程组的求解方法:

- (1) 什么是列向量空间?
- (2) 什么是线性函数?
- (3) 如何求解线性方程组?

1.2.1 列向量空间以及加法, 数乘运算

我们记 \mathbb{R} 为全体实数的集合. 在例子中我们求数组 x_1, x_2, x_3, x_4 , 我们可以将其写作一列的形式

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix},$$

其中每个分量 x_i 都是实数, 这样的 \mathbf{x} 被称为一个长度为 4 的实数组. 如果我们考虑长度为 2 的实数组全体构成的集合

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1, x_2 \in \mathbb{R} \right\},$$

这个集合记做 \mathbb{R}^2 , 并且这个集合中的元素一一对应于平面上的点. 同时, \mathbb{R}^2 中的点 P 也可以一一对应于从原点到这个点的向量 \overrightarrow{OP} , 如下图所示:

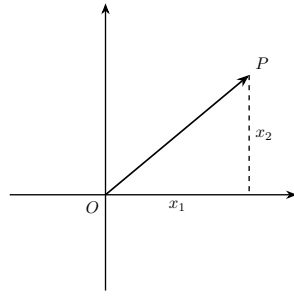


图 4: 点与向量的一一对应

类似的, 我们可以认为 \mathbb{R}^3 中的元素一一对应于三维空间中的点, 也一一对应于从原点到这个点的向量.

定义 1.1. 列向量空间 (*column vector space*) 定义为如下的集合

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \mid x_i \in \mathbb{R} \right\},$$

其中的元素称为**列向量** (*column vector*).

定义 1.2. \mathbb{R}^n 上可以定义如下两种运算:

(1) **加法** (*addition*):

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

(2) **数乘** (*scalar product*): 任取实数 $c \in \mathbb{R}$, 定义

$$c \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} cx_1 \\ cx_2 \\ cx_3 \\ \vdots \\ cx_n \end{pmatrix}.$$

注 1.1. 向量的加法和数乘有其对应的几何意义, 对于 \mathbb{R}^2 来说, 其中向量的加法和数乘的几何意义分别是平行四边形法则和伸缩变换, 如下图所示:

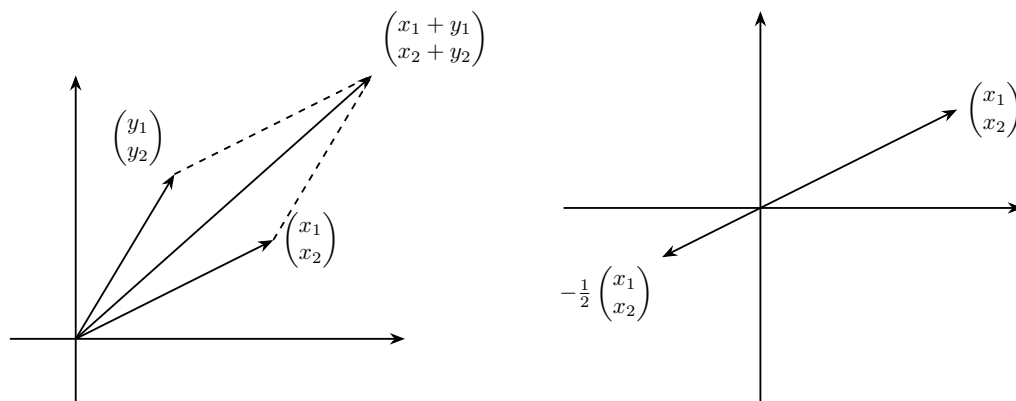


图 5: 向量加法与数乘的几何意义

由实数本身乘法和加法的性质, 我们可以得到 \mathbb{R}^n 中的加法和数乘满足如下的性质:

命题 1.1. 设 $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ 是列向量, $a, b \in \mathbb{R}$ 是实数, 那么:

(1) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (加法交换律);

(2) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ (加法结合律);

(3) 存在零向量 $\mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$, 使得对任意 $\mathbf{v} \in \mathbb{R}^n$, 有 $\mathbf{v} + \mathbf{0} = \mathbf{v}$ (加法的单位元);

(4) 对任意 $\mathbf{v} \in \mathbb{R}^n$, 存在 $-\mathbf{v} \in \mathbb{R}^n$, 使得 $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$ (加法的逆元);

(5) $a(b\mathbf{v}) = (ab)\mathbf{v}$ (数乘结合律);

(6) $1\mathbf{v} = \mathbf{v}$ (数乘的单位元);

(7) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (数乘对加法的分配律);

(8) $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ (加法对数乘的分配律).

这些运算法则抽象出来将会变成抽象线性空间的公理化定义的一部分. 当加法和乘法运算进行复合时, 我们可以得到如下的定义:

定义 1.3 (线性组合). 设 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m \in \mathbb{R}^n$ 是列向量, $c_1, c_2, \dots, c_m \in \mathbb{R}$ 是实数, 那么列向量

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \dots + c_m\mathbf{v}_m$$

称为以 c_1, \dots, c_m 为系数的 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ 的一个**线性组合** (*linear combination*).

如注记1.1中所示, 平面 \mathbb{R}^2 上不在一条直线上的两个向量 \mathbf{v}, \mathbf{w} 的所有线性组合能够通过平行四边形的方式表示平面上的任意一个向量.

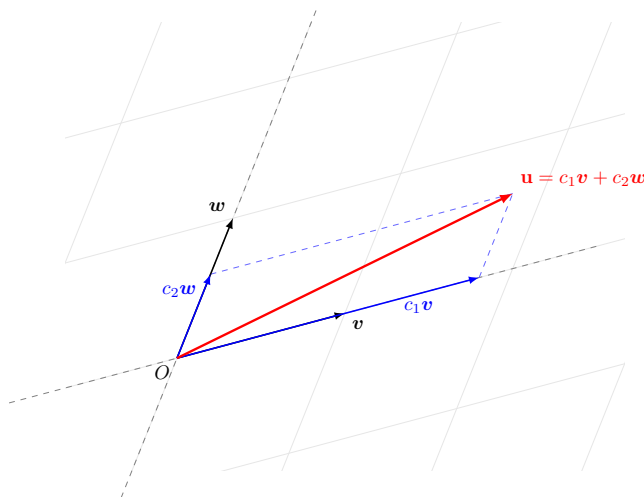


图 6: 平面 \mathbb{R}^2 上不共线向量 \mathbf{v}, \mathbf{w} 的线性组合生成整个平面

由数乘和加法的分配律, 我们可以得到线性组合有如下的封闭性性质:

命题 1.2. 设 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m \in \mathbb{R}^n$ 是列向量, $\mathbf{w}_1, \dots, \mathbf{w}_k$ 是它们的线性组合, 那么任意 $\mathbf{w}_1, \dots, \mathbf{w}_k$ 的线性组合仍然是 $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$ 的线性组合.

1.2.2 线性函数及其刻画

定义 1.4. 对于 \mathbb{R}^n 上的函数 $F: \mathbb{R}^n \rightarrow \mathbb{R}$, 如果存在 $a_1, \dots, a_n \in \mathbb{R}$ 是常数, 使得 F 有如下表达式

$$F(\mathbf{x}) = a_1x_1 + \dots + a_nx_n,$$

那么称 F 是 \mathbb{R}^n 上的**线性函数** (*linear function*).

例 1.1. 如下的 F 是 \mathbb{R}^2 上的线性函数:

$$F: \mathbb{R}^2 \rightarrow \mathbb{R}$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto (x_1 + 1)^2 - (x_1 - 1)^2 + (x_2 - 1)^2 - (x_2 + 1)^2.$$

定理 1.1. 函数 $F: \mathbb{R}^n \rightarrow \mathbb{R}$ 是线性函数当且仅当 F 满足:

(1) 对任意 $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, 有

$$F(\mathbf{x} + \mathbf{y}) = F(\mathbf{x}) + F(\mathbf{y}).$$

(2) 对任意 $c \in \mathbb{R}, \mathbf{x} \in \mathbb{R}^n$, 有

$$F(c\mathbf{x}) = cF(\mathbf{x}).$$

注 1.2. 这个定理说明 \mathbb{R}^n 上的函数 F 是线性函数当且仅当 F 与 \mathbb{R}^n 上加法与数乘, 也就是与 \mathbb{R}^n 上的线性结构相容, 这也是 F 为什么被称为线性函数.

证明. 如果 F 是线性函数, 可以直接验证 F 满足 (1), (2) 两条性质; 另一方面, 如果 F 满足 (1), (2), 我们记

$$a_1 = F\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right), \quad a_2 = F\left(\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}\right), \quad \dots$$

则

$$F\left(\begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = a_1 x_1, \quad F\left(\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}\right) = a_2 x_2, \quad \dots$$

那么任取 $v_1, \dots, v_m \in \mathbb{R}^n$, 则

$$\begin{aligned} F(v_1 + v_2 + \dots + v_m) &= F((v_1 + \dots + v_{m-1}) + v_m) \\ &= F(v_1 + \dots + v_{m-1}) + F(v_m) \\ &= F(v_1) + \dots + F(v_m). \end{aligned}$$

因此,

$$F\left(\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}\right) = F\left(\begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) + \dots + F\left(\begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix}\right) = F\left(\begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) + \dots + F\left(\begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix}\right) = a_1 x_1 + \dots + a_n x_n.$$

□

命题 1.3. 如果 F 是线性函数, 那么 $F\left(\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = 0$.

证明. 任意取 $0 \neq c \in \mathbb{R}$, 根据定义则有

$$F\left(c \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = cF\left(\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right),$$

因此 $F\left(\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = 0.$

□

例 1.2. 如下的 F_1, F_2 不是 \mathbb{R}^2 上的线性函数:

$$F_1: \mathbb{R}^2 \rightarrow \mathbb{R}$$
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto x_1 + x_2 + 4,$$

$$F_2: \mathbb{R}^2 \rightarrow \mathbb{R}$$
$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto x_1^2 + x_2^2.$$

对于函数 F_1 , 通过直接的计算得到 $F_1\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) \neq 0$, 从而利用命题 1.3 可知 F_1 不是线性函数.

对于函数 F_2 , 我们可以发现

$$F_2\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = 1, \quad F_2\left(2 \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = 4 \neq 2,$$

从而根据线性函数的定义中第二条可知 F_2 不是线性函数.

定义 1.5. \mathbb{R}^n 上 m 个线性函数 F_1, F_2, \dots, F_m 和 m 个实数 b_1, b_2, \dots, b_m 满足的方程组

$$\begin{cases} F_1(\mathbf{x}) = b_1 \\ F_2(\mathbf{x}) = b_2 \\ \vdots \\ F_m(\mathbf{x}) = b_m \end{cases}$$

称为 n 个变元的**线性方程组** (*system of linear equations*), 代入方程组使得其成立的 \mathbf{x} 称为**线性方程组的解** (*solution of system of linear equations*).

注 1.3. 我们可以给线性方程组如下的一些几何解释:

- (1) 在 \mathbb{R}^2 中, 单个线性函数 $F_1(\mathbf{x}) = a_1x_1 + a_2x_2$ 以及实数 b_1 给出的线性方程组 $a_1x_1 + a_2x_2 = b_1$ 的解是 \mathbb{R}^2 中的一条直线. 例如 $x_1 + 2x_2 = 3$ 的解是直线 $x_2 = -\frac{1}{2}x_1 + \frac{3}{2}$, 有斜率 $-\frac{1}{2}$ 和 x_2 轴的截距 $\frac{3}{2}$, 如下图所示.

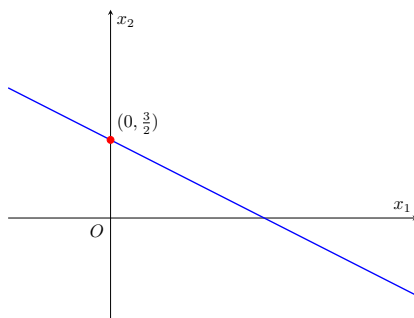


图 7: 直线 $x_1 + 2x_2 = 3$

- (2) 在 \mathbb{R}^2 中, 根据 (1) 的几何解释不难理解如下线性方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a_{21}x_1 + a_{22}x_2 = b_2 \end{cases}$$

的解是 \mathbb{R}^2 中两条直线的交点. 如果两条直线不相同, 则要么平行, 要么相交在一个点, 即对应如上线性方程要么无解, 要么有解且此时一定只有唯一解. 如果两条直线相同, 则对应有无穷多组解.

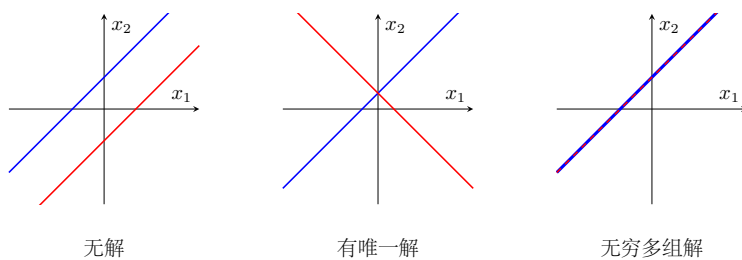


图 8: 两个未知数两个方程的解

(3) 在 \mathbb{R}^3 中, 如下线性方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \end{cases}$$

的解可以看成是 \mathbb{R}^3 中两个平面的交线. 注意: 在 \mathbb{R}^3 中两个不一样的平面不一定相交, 即如上线性方程组不一定有解, 并且如果相交, 也是交出一条线, 即此时解不唯一.

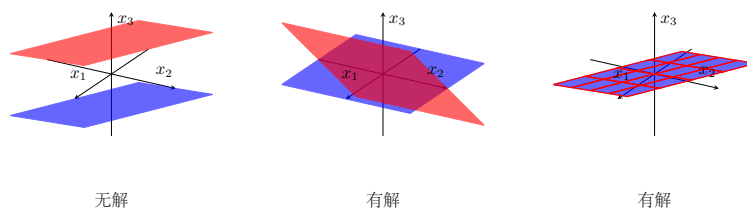


图 9: 三个未知数两个方程的解

(4) 在更高维中也有同样的解释: 由一个线性函数给出的线性方程的解可以看成是一个低一维的超平面, 而多个线性函数给出的线性方程组的解则是这些超平面的交.

1.3 高斯消元法和最简阶梯型

从《九章算术》到消元法

今天所谓的“高斯消元法”并不是某一天突然被发明出来的. 中国古代数学典籍《九章算术》的“方程”章已经把未知数的系数排成方形表格, 并通过逐列消去未知量来求解多元一次方程组. 若把当时的筹算表格翻译成现代记号, 核心步骤正是我们下面要学习的初等行变换. 换句话说, 消元法首先是一种非常朴素的计算经验: 把复杂的联立限制一步步改写成更容易读出答案的等价限制.

根据注记1.3可知一个线性方程组可能没有解, 并且即使有解也不一定只有唯一解, 那么该如何求解线性方程组呢? 在本节中我们将利用高斯消元法, 来求解一般的线性方程组. 我们先来看下面的一个简单的例子.

例 1.3 (两个未知量的消元). 先从最熟悉的二元一次方程组开始:

$$\begin{cases} x + 2y = 7, \\ 3x - y = 1. \end{cases}$$

第一式给出 $x = 7 - 2y$. 代入第二式得到

$$3(7 - 2y) - y = 1,$$

即 $21 - 7y = 1$, 所以 $y = \frac{20}{7}$, 进而

$$x = 7 - 2 \cdot \frac{20}{7} = \frac{9}{7}.$$

也可以用行变换记录同样的过程:

$$\left(\begin{array}{cc|c} 1 & 2 & 7 \\ 3 & -1 & 1 \end{array} \right) \xrightarrow{r_2 - 3r_1} \left(\begin{array}{cc|c} 1 & 2 & 7 \\ 0 & -7 & -20 \end{array} \right).$$

这一步的含义就是: 用第二个方程减去第一个方程的 3 倍, 把 x 消去.

习题 1.1. 用同样的方法解方程组

$$\begin{cases} 2x + y = 5, \\ x - y = 1. \end{cases}$$

请同时写出代入法和增广矩阵行变换两种过程.

例 1.4.

$$\begin{cases} 4x_2 - x_3 = 7 & (r_1) \\ x_1 + 2x_2 = 5 & (r_2) \\ 2x_1 + x_3 = 3 & (r_3) \end{cases}$$

显然我们交换 r_1, r_2 不改变上述方程组的解, 因此我们得到:

$$\begin{cases} x_1 + 2x_2 = 5 & (r'_1) \\ 4x_2 - x_3 = 7 & (r'_2) \\ 2x_1 + x_3 = 3 & (r'_3) \end{cases}$$

我们考虑如下操作: 保持 r'_1, r'_2 不变, 用 r'_3 减去 $2r'_1$, 得到如下的方程组:

$$\begin{cases} x_1 + 2x_2 = 5 & (r''_1) \\ 4x_2 - x_3 = 7 & (r''_2) \\ -4x_2 + x_3 = -7 & (r''_3) \end{cases}$$

上述操作并不改变方程组的解, 因为可由 r''_1, r''_2, r''_3 恢复出 r'_1, r'_2, r'_3 . 类似的最后再保持 r''_1, r''_2 不变, 用 r''_3 加上 r''_2 , 得到

$$\begin{cases} x_1 + 2x_2 = 5 \\ 4x_2 - x_3 = 7 \\ 0 = 0 \end{cases}$$

对于上述方程组我们可以用 x_3 来如下的表示 x_1, x_2 , 其中 x_3 可以取任意的实数

$$\begin{aligned} x_1 &= -\frac{1}{2}x_3 + \frac{3}{2} \\ x_2 &= \frac{1}{4}x_3 + \frac{7}{4} \end{aligned}$$

因此我们可以将方程组的解写作

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_3 \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{4} \\ 1 \end{pmatrix} + \begin{pmatrix} \frac{3}{2} \\ \frac{7}{4} \\ 0 \end{pmatrix}. \quad (1)$$

注 1.4. 根据上述结果可以发现该线性方程组有无穷组解, 这对应于几何解释中 \mathbb{R}^3 中三个平面相交出一条线. 如下图所示

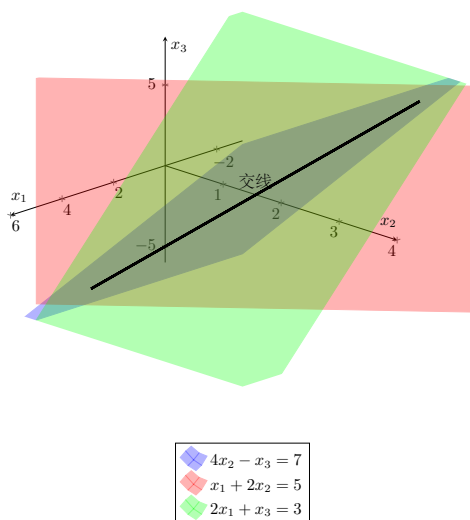


图 10: 三个平面相交出一条线

注 1.5. 在上述求解过程中, 我们只关心每一行方程中 x_i 前面的系数, 以及右侧常数项的变化情况. 通常我们可以把系数拿出来, 只对系数做如下变换:

$$\begin{pmatrix} 0 & 4 & -1 & 7 \\ 1 & 2 & 0 & 5 \\ 2 & 0 & 1 & 3 \end{pmatrix} \xrightarrow{r_1 \leftrightarrow r_2} \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \\ 2 & 0 & 1 & 3 \end{pmatrix} \xrightarrow{r_3 - 2r_1} \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \\ 0 & -4 & 1 & -7 \end{pmatrix} \xrightarrow{r_3 + r_2} \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

回顾例1.4, 在解方程中我们主要用到了如下三种操作:

(E1) 交换方程组的某两行.

(E2) 将某一行乘以非零常数 c .

(E3) 将某一行的非零常数 c 倍加到另一行上.

我们称如上的三种操作为**基础行变换** (elementary row operations). 不难发现基础行变换均可逆, 并且其逆也是基础行变换.

定义 1.6. 有限个基础行变换的复合称为**行变换** (row operations).

命题 1.4. 行变换均可逆, 并且其逆也为行变换.

证明. 因为基础行变换可逆, 且其逆也为基础行变换. 我们将一个基础行变换 O 的逆记作 O^{-1} . 则操作 $O_1 O_2 \cdots O_k$ 的逆为 $O_k^{-1} O_{k-1}^{-1} \cdots O_1^{-1}$. \square

初等行变换中得到的新的行是由旧的行通过加法和数乘得到的, 也就是旧的行的线性组合, 而且我们知道线性组合的复合仍然是原来的对象的线性组合 (性质 1.2), 因此我们可以得到如下的结论:

命题 1.5. 行变换后的每一行是最初的行的线性组合.

思考 1.1. 三种基础行变换相互之间会产生关系, 导致有些行变换可以通过其他行变换来实现. 请思考是否可以用两种基础行变换的组合来实现第三种基础行变换.

推论 1.1. 行变换不改变线性方程组的解.

由于作行变换只关注方程的系数以及右侧常数项, 因此对于如下的线性方程组

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

我们将其系数及常数项提出来记作

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

并将这个线性方程组记做 $A\mathbf{x} = \mathbf{b}$, 这也引出了矩阵的概念.

定义 1.7. 由 $m \times n$ 个数 a_{ij} 排成的 m 行 n 列的 (实) 数表称为 m 行 n 列**矩阵** (matrix), 记做 $(a_{ij})_{m \times n} \in M_{m \times n}(\mathbb{R})$. 当 $m = n$ 时, $A \in M_n(\mathbb{R})$ 被称为 n 阶**方阵** (square matrix), 此时 $M_{n \times n}(\mathbb{R})$ 通常简记为 $M_n(\mathbb{R})$, 此处 n 称为方阵的**阶数** (order of matrix).

例 1.5. 矩阵 $I_n \in M_n(\mathbb{R})$ 表示只有 (i, i) 元为 1, 其余分量为零的 n 阶方阵, 称为**单位矩阵**(identity matrix).

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

对于线性方程组 $A\mathbf{x} = \mathbf{b}$, A 称为**系数矩阵** (coefficient matrix), (A, \mathbf{b}) 称为**增广矩阵** (augmented matrix), 并将上述方程记作 $A\mathbf{x} = \mathbf{b}$. 现在我们即可以通过行变换来操作我们的增广矩阵, 使其最终的形式便于我们求解, 那么究竟该操作到什么样子为止呢?

根据例1.4, 我们发现如果我们的增广矩阵有如下的形式, 线性方程组可以直接求解:

- (1) 所有非零行在零行的上面.
- (2) 对某一非零行, 称最左边的非零元为**主元** (pivot), 第 i 行的主元严格比第 $i + 1$ 行的主元靠左.

满足上述条件的矩阵称为**行阶梯型** (row echelon form), 并且如果主元所在列的其他元素均为零, 主元本身为 1, 则称此时为**最简行阶梯型** (reduced row echelon form).

注 1.6. 由于阶梯型和最简阶梯型的定义涉及到从左到右和从上到下的顺序, 所以 A 是阶梯型 (或者最简阶梯型) 时, 其任意左上部分也是阶梯型 (或者最简阶梯型). 这一观察在很多归纳法中经常用到.

例 1.6. 在例子 1.4 中, 对应的增广矩阵为

$$(A, \mathbf{b}) = \begin{pmatrix} 0 & 4 & -1 & 7 \\ 1 & 2 & 0 & 5 \\ 2 & 0 & 1 & 3 \end{pmatrix}$$

如注记 1.5 中所示, 通过行变换之后我们可以得到

$$\begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

这是一个阶梯型。如果我们继续做矩阵的行变换, 将第二行乘以 $\frac{1}{4}$ 得到主元为 1 的行, 再用第二行的 -2 倍加到第一行, 得到最简行阶梯型

$$\begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\frac{1}{4}r_2} \begin{pmatrix} 1 & 2 & 0 & 5 \\ 0 & 1 & -\frac{1}{4} & \frac{7}{4} \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{r_1 - 2r_2} \begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{3}{2} \\ 0 & 1 & -\frac{1}{4} & \frac{7}{4} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

如果我们对最初的增广矩阵的行变换进行不同的选择，例如选择第一步将最后一行和第一行做交换

$$\begin{pmatrix} 0 & 4 & -1 & 7 \\ 1 & 2 & 0 & 5 \\ 2 & 0 & 1 & 3 \end{pmatrix} \xrightarrow{r_1 \leftrightarrow r_3} \begin{pmatrix} 2 & 0 & 1 & 3 \\ 1 & 2 & 0 & 5 \\ 0 & 4 & -1 & 7 \end{pmatrix} \xrightarrow{r_2 - \frac{1}{2}r_1} \begin{pmatrix} 2 & 0 & 1 & 3 \\ 0 & 2 & -\frac{1}{2} & \frac{7}{2} \\ 0 & 4 & -1 & 7 \end{pmatrix} \xrightarrow{r_3 - 2r_2} \begin{pmatrix} 2 & 0 & 1 & 3 \\ 0 & 2 & -\frac{1}{2} & \frac{7}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

此时得到的阶梯型和前一种阶梯型不一样。但进一步经过行变换得到的最简阶梯型是一样的。也就是从例子中我们可以看到，有不同的行变换方法可以把原矩阵变换成不同的阶梯型，但进一步经过行变换得到的最简阶梯型是一样的。

通过例子，我们可以总结出一般通过行变换将矩阵变换成最简行阶梯型的过程是：

1. 首先通过第一种初等行变换交换行，将最左边的主元所在的行移到第一行。注意到此时最左边的主元不一定唯一，所做行变换也不一定唯一。
2. 通过第二种初等行变换将第一行的主元变为 1。
3. 通过第三种初等行变换将第一行主元下方的所有元素变为零。此时最左边的主元已经唯一了。
4. 接下来对第二行到最后一行重复上述过程，使得这一部分最靠左的主元落在第二行，取值是 1，并且其下方的所有元素都变为零。在这个过程中，我们对第一行没有做任何操作，第二行到最后一行做行变换时这些行中最靠左的主元左边的元素都还是保持是零。所以此时最左边的主元还是第一行的主元。
5. 对第三行到最后一行重复上述过程……。这样我们得到一个矩阵的主元按严格从左到右的顺序依次排列在第一行，第二行，第三行……。零行由于没有主元，都在矩阵的最下方。即此时的矩阵是阶梯型。
6. 接下来，我们通过行变换将阶梯型变成最简阶梯型。我们从最后一个非零行出发，用第三种初等变换将后面行的某个倍数加到前面的行，使得主元上方的元素也变成零。这样我们就得到了一个最简阶梯型。

这些操作方式总结起来就是如下的存在性定理。

定理 1.2. 矩阵 A 可通过行变换变成最简行阶梯型。

前面的操作步骤可以写作是一个对行做归纳的形式的证明，同时我们也可以通过对列做归纳给出一个证明。

证明. 对 $m \times n$ 矩阵的列数作归纳: 假设 $n = 1$ 时, 对于 $m \times 1$ 矩阵

$$A = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}.$$

如果 $a_{11} = \cdots = a_{m1} = 0$, 则此时已经是最简行阶梯型. 若 $a_{11} = a_{21} = \cdots = a_{(k-1)1} = 0, a_{k1} \neq 0$, 那么通过 (E1) 将 a_{k1} 换到第一行, 用 (E2) 将第一行乘以 $(a_{k1})^{-1}$ 使得主元变为 1, 再用 (E3) 将第一行以下变为零, 因此此时最简行阶梯型为

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

假设对列数为 n 的时候成立, 对于 $m \times (n+1)$ 的矩阵 A , 将其写作 $A = (B, y)$, 其中 B 是 $m \times n$ 矩阵. 根据归纳假设 B 可由行变换得到最简行阶梯型, 记作 B' , 将同样的变换作用在 A 上得到 $A' = (B', y')$. 如果 B' 没有非零行, 则只需对最后一列 y' 应用 $n = 1$ 时的结论: 若 $y' = 0$, 则 A' 已经是零矩阵; 若 $y' \neq 0$, 则可通过行变换把 A' 化为第一到第 n 列全零、最后一列为 $(1, 0, \dots, 0)^T$ 的最简行阶梯型. 以下假设 B' 有非零行, 并且 B' 从第 $k+1$ 行开始是零行, 且

$$y' = \begin{pmatrix} y'_1 \\ y'_2 \\ \vdots \\ y'_k \\ y'_{k+1} \\ \vdots \end{pmatrix}$$

则对

$$\begin{pmatrix} y'_{k+1} \\ \vdots \\ y'_m \end{pmatrix}$$

应用 $n = 1$ 时的结论, 可做行变换得到最简行阶梯型, 同时也对 B' 的 $k+1$ 到 m 行作. 但由于行变换不改变零矩阵, 因此不改变 B' , 得到的矩阵记作 A'' . 考虑如下两种情况:

(1) 如果

$$\begin{pmatrix} y'_{k+1} \\ \vdots \\ y'_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

则此时 A'' 已经是最简行阶梯型.

(2) 如果

$$\begin{pmatrix} y'_{k+1} \\ \vdots \\ y'_m \end{pmatrix} \neq 0$$

则经过上述一系列化简后, A'' 的最后一列从第 $k+1$ 行到第 m 行形如

$$\begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix},$$

其中 1 位于第 $k+1$ 行. 再用第 $k+1$ 行的适当倍数加到第 $1, 2, \dots, k$ 行, 将最后一列前 k 个元素变为零, 此时得到的矩阵也是最简行阶梯型.

□

同时我们也有如下的唯一性定理和定义。

定理 1.3. 矩阵 A 通过行变换得到的最简行阶梯型不依赖于行变换的选取, 记作 $\text{rref } A$.

这个唯一性定理的证明我们放在第 1.6 节, 将依赖于我们对线性方程组解的描述. 在承认唯一性的基础上, 我们可以给出矩阵的秩的定义。

定义 1.8. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 其对应的最简阶梯型中主元的个数被定义为 A 的秩 (*rank*), 记做 $\text{rank } A$.

秩是对矩阵或者是对应的线性方程组的核心概念, 我们之后会讨论更多等价定义的方式和应用. 由于每一行每一列至多有一个主元, 因此我们有如下的命题。

命题 1.6. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 有 $\text{rank } A \leq \min\{m, n\}$.

对于这个不等式还有常用的满秩的概念。

定义 1.9. 如果矩阵 $A \in M_{m \times n}(\mathbb{R})$ 的秩 $\text{rank } A = m$, 则称 A 为行满秩矩阵 (*full row rank matrix*). 如果矩阵 $A \in M_{m \times n}(\mathbb{R})$ 的秩 $\text{rank } A = n$, 则称 A 为列满秩矩阵 (*full column rank matrix*). 如果 A 是方阵, 且 $\text{rank } A = n$, 则称 A 为满秩矩阵 (*full rank matrix*).

注 1.7. 由化简为最简阶梯型的操作步骤, 我们可以看出对于阶梯型矩阵 A , 其主元位置和 $\text{rref } A$ 中的主元位置是一致的. 所以阶梯型矩阵 A 的秩等于其主元的个数, 或者等价的其非零行的个数。

1.4 线性方程组解的结构, 自由元和主元

定义 1.10. 对于线性方程组的系数矩阵 A , $\text{rref } A$ 中主元所在的列对应的未知元称为主元 (*principal unknowns*), 其余未知元称为自由元 (*free unknowns*).

注意这里的主元 (*principal unknowns*) 和矩阵 $\text{rref } A$ 的主元 (*pivot*) 有一一对应关系。从最简阶梯型出发, 我们可以写下线性方程组的解。例如以下的线性方程组:

例 1.7. 例如线性方程组 $A\mathbf{x} = \mathbf{b}$, 其中

$$A = \begin{pmatrix} 1 & 0 & 3 & 5 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix},$$

则 x_1, x_2, x_5 是主元, x_3, x_4, x_6 是自由元。并且根据上述最简行阶梯型, 我们可以直接分析出方程组的解的情况:

1. 如果 b_4 或者 b_5 不是零, 则方程组 $A\mathbf{x} = \mathbf{b}$ 无解。
2. 如果 $b_4 = b_5 = 0$, 则 x_3, x_4, x_6 取定任意实数后, 主元由方程组唯一确定。或者说, 我们可以将原方程组等价的写作如下形式:

$$\begin{aligned} x_1 &= b_1 - 3x_3 - 5x_4 - x_6 \\ x_2 &= b_2 - 2x_3 - x_4 - 2x_6 \\ x_5 &= b_3. \end{aligned}$$

此时任意一组自由元的取值 $\begin{pmatrix} x_3 \\ x_4 \\ x_6 \end{pmatrix}$ 都唯一的对应到一组解

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} b_1 - 3x_3 - 5x_4 - x_6 \\ b_2 - 2x_3 - x_4 - 2x_6 \\ x_3 \\ x_4 \\ b_3 \\ x_6 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ 0 \\ 0 \\ b_3 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_6 \begin{pmatrix} -1 \\ -2 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

定理 1.4 (线性方程组解的结构定理). 对于方程 $A\mathbf{x} = \mathbf{b}$, 用行变换将 (A, \mathbf{b}) 化作最简行阶梯型 $(\bar{A}, \bar{\mathbf{b}})$, 则

- (1) 方程有解等价于 \bar{A} 的零行对应的 \bar{b}_i 也是零.
- (2) 方程有解时自由元可以任意取值, 且自由元的每一组取值都唯一决定了一组解. 特别地, 方程有唯一解当且仅当没有自由元.

假设 x_{i_1}, \dots, x_{i_r} 是主元, x_{j_1}, \dots, x_{j_s} 是自由元. 我们用映射的观点来看这个自由元取值和解的关系, 定义到自由元的分量的投影映射

$$\pi: \mathbb{R}^n \rightarrow \mathbb{R}^s,$$

$$\pi(\mathbf{x}) \mapsto \begin{pmatrix} x_{j_1} \\ x_{j_2} \\ \vdots \\ x_{j_s} \end{pmatrix}.$$

推论 1.2. 假设线性方程组 $A\mathbf{x} = \mathbf{b}$ 有解, 且 S 是其解集, 则投影映射 π 限制在 S 上是 $S \rightarrow \mathbb{R}^s$ 的双射.

利用最简阶梯型和方程组的解的关系, 我们现在可以证明最简阶梯型的唯一性. 具体细节在小节1.6中. 这个证明过程比较长, 初次学习时可以跳过. 这里的证明过程参考了首位女菲尔兹奖得主 Maryam Mirzakhani 本科生阶段写的短文 “A Simple Proof of a Theorem of Schur”, <https://doi.org/10.1080/00029890.1998.12004879>.

由于秩定义成最简阶梯型中主元的个数, 我们有如下对有解和无解的判定法则。

推论 1.3. 线性方程组 $A\mathbf{x} = \mathbf{b}$

- (1) 有解当且仅当 $\text{rank } A = \text{rank}(A, \mathbf{b})$.
- (2) 有唯一解当且仅当 $\text{rank } A = \text{rank}(A, \mathbf{b})$ 并且 $\text{rank } A$ 与 A 的列数相同.

证明. 对增广矩阵 (A, \mathbf{b}) 的最简阶梯型 $(\bar{A}, \bar{\mathbf{b}})$. 我们有 \bar{A} 也是 A 的最简阶梯型. □

注意到对零矩阵做行变换, 我们总是得到零矩阵. 特别的, 对于 \mathbf{b} 等于零的情形, 做行变换时得到的 $\bar{\mathbf{b}}$ 也是零, 对应的线性方程组总是有解的.

定义 1.11. 方程 $A\mathbf{x} = \mathbf{0}$ 称为 **齐次线性方程组** (*system of homogeneous linear equations*).

定理 1.5. 齐次线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解包含了零向量, 且在加法和数乘下封闭.

证明. 注意到

$$A(\mathbf{x} + \mathbf{y}) = A\mathbf{x} + A\mathbf{y},$$

$$A(c\mathbf{x}) = cA\mathbf{x}.$$

□

在齐次线性方程组时，限制条件的个数小于未知数的个数会导致有无穷多解的直观也是对的。

命题 1.7. 假设 A 是 $m \times n$ 的的矩阵，且 $m < n$. 则对应的齐次线性方程组 $Ax = \mathbf{0}$ 含有非零解.

证明. 由于最简阶梯型中每一列至多只有一个主元，因此当方程个数小于未知数个数时，主元的个数少于未定元的个数。所以总存在某一个自由元可以取非零值，从而齐次线性方程组一定有非零解。□

定理 1.6. 对于线性方程组 $Ax = \mathbf{b}$, 如果 \tilde{x} 是其某一解 (特解), 则 $Ax = \mathbf{b}$ 的所有解均可唯一的表达为 $x = y + \tilde{x}$, 其中 y 是 $Ax = \mathbf{0}$ 的解.

证明. 只需验证如下两点:

(1) 验证 $y + \tilde{x}$ 是解.

(2) 验证当 x 是解时, $x = (x - \tilde{x}) + \tilde{x}$, 其中 $x - \tilde{x}$ 满足 $Ax = \mathbf{0}$.

□

注 1.8. 从几何上来看，齐次线性方程组 $Ax = \mathbf{0}$ 的解构成了 \mathbb{R}^n 中的一个对加法数乘封闭的子集，之后我们会用更抽象的观点去描述这种子集，并称其为一个子空间。而 $Ax = \mathbf{b}$ 的解相当于是将这个子空间做了平移。

直观上来看，对于 n 个变元的齐次线性方程组 $Ax = \mathbf{0}$ ，自由元的个数说明了解有多大自由度，我们定义这个量是矩阵 A 的零度 (Nullity)，记作 $\text{Null}(A)$ 。而主元个数，或者等价的秩，说明了方程组的限制条件的个数。我们有如下的定量描述。

定理 1.7 (Rank-Nullity 定理). 一个 $m \times n$ 矩阵 A 的零度等于 $\text{Null}(A) = n - \text{rank } A$.

1.5 线性方程组的相容性和确定性

我们对于线性方程组的解的存在性和唯一性等定性性质有如下定义。

定义 1.12. 对于线性方程组 $Ax = \mathbf{b}$, 我们有如下定义:

(1) 如果方程有解，我们称这个线性方程组是**相容的** (*consistent*).

(2) 如果方程无解，我们称这个线性方程组是**不相容的** (*inconsistent*).

(3) 如果方程有唯一解，我们称这个线性方程组是**确定的** (*definite*).

推论 1.4.

(1) 线性方程组 $Ax = b$ 是相容的等价于 $\text{rank } A = \text{rank}(A, b)$.

(2) 线性方程组 $Ax = b$ 是确定的等价于 $Ax = b$ 是相容的, 且 $\text{rank } A$ 等于 A 的列数.

定理 1.8. 对于 n 阶方阵 A , 线性方程组 $Ax = b$ 是否有唯一解只取决于 A , 与 b 无关.

证明. 根据推论 1.4 可知, $Ax = b$ 有唯一解等价于 $\text{rank } A = n$. □

例 1.8 (插值多项式的存在性和唯一性). 对于互不相同的实数 c_1, \dots, c_r , 以及任意实数 k_1, \dots, k_r , 存在唯一的次数小于等于 $r-1$ 的多项式 $f(x) = a_0 + a_1x + \dots + a_{r-1}x^{r-1}$ 使得对于任意 $i = 1, \dots, r$ 使得

$$f(c_i) = k_i \quad (2)$$

证明. 注意到 (2) 是关于 a_0, \dots, a_{r-1} 这 r 个未知元的线性方程组, 不妨记做

$$A \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{pmatrix} = \begin{pmatrix} k_0 \\ k_1 \\ \vdots \\ k_{r-1} \end{pmatrix}.$$

根据线性方程组的解的结构定理, 上述方程组有唯一解当且仅当下面的线性方程组有唯一解

$$A \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

这等价于 c_1, \dots, c_r 是 $f(x)$ 的根, 而以 c_1, \dots, c_r 为根的次数不超过 $r-1$ 的多项式是唯一的 (只能为 0), 从而说明了 (2) 解的唯一性. □

注 1.9. 类似例 1.8 的结论也可以推广多项式在某些点的取值和导数值同时被指定的情形. 例如, 给定互不相同的实数 c_1, \dots, c_r , 以及任意实数 $k_{i,j}$, $i = 1, \dots, r$, $j = 0, \dots, m_i - 1$, 存在唯一的次数小于等于 $m_1 + \dots + m_r - 1$ 的多项式 $f(x)$ 使得对于任意 $i = 1, \dots, r$ 和 $j = 0, \dots, m_i - 1$ 使得

$$f^{(j)}(c_i) = k_{i,j}.$$

这个结论可以通过构造一个合适的线性方程组来证明. 此时对应的线性方程组中方程个数和未知数个数均为 $m_1 + \dots + m_r$. 所以只需要验证对应的齐次线性方程组只有零解即可.

类似例子也经常出现在物理学中, 很多规律都可以归结为求解线性方程组, 并且其中未知数个数和方程个数相同. 此时为了验证某个物理系统的解的存在性和唯一性, 我们只需要验证对应的齐次线性方程组只有零解即可. 习题中有图上的热方程对应的例子.

1.6 选讲: 最简行阶梯型唯一性的证明

令 A 是一个 $m \times n$ 阶的矩阵, 在本节中我们介绍如何证明最简行阶梯型 $\text{rref } A$ 的唯一性.

定理 1.9 (= 定理1.3). 对于任意矩阵 A , 经过行变换得到的最简行阶梯型不依赖于行变换的选取, 只依赖于初始的矩阵 A .

证明. 我们对 n 做归纳法来证明: 当 $n = 1$ 时, $\text{rref } A$ 只有如下两种情况:

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

注意到行变换将零矩阵变成零矩阵, 并且由于行变换可逆, 从而行变换将非零矩阵变成非零矩阵. 因此在 $n = 1$ 的情况, 最简行阶梯型 $\text{rref } A$ 是否为零完全由 A 是不是零来决定.

现在假设命题对列数是 n 的情况成立, 对于 $n + 1$ 列的矩阵 A , 将其写成 $A = (B, y)$ 的形式, 其中 B 是 n 列的矩阵, y 是一个列向量. 假设此时 $\text{rref } A$ 有 $A' = (B', y')$ 和 $A'' = (B'', y'')$ 两种形式. 删除最后一列后, B' 和 B'' 都是由 B 经过行变换得到的最简行阶梯型, 从而根据归纳假设 $B' = B''$.

现在考虑线性方程组

$$B \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = y. \quad (3)$$

由于行变换不改变线性方程组解的情况, 从而方程组 (3) 等价于如下两种方程组

$$B' \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = y', \quad B'' \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = y''.$$

对于方程组 (3), 我们有如下两种情况:

(i) (3) 无解, 假设 B 有 r 个主元, 那么

$$y' = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = y'',$$

其中 1 位于第 $r+1$ 行.

(ii) (3) 有解. 假设 B 的主元分别在 i_1, \dots, i_r 列. 令自由元均取 0, 则得到关于 x_{i_1}, \dots, x_{i_r} 这 r 个未知元的线性方程组, 并且有解:

$$x_{i_1} = y'_1, \dots, x_{i_r} = y'_r,$$

或者

$$x_{i_1} = y''_1, \dots, x_{i_r} = y''_r.$$

但由于此时解是唯一的, 从而 $y' = y''$, 从而得到最简行阶梯型 $\text{rref } A$ 是唯一的.

□

注 1.10. 上述证明中我们用到了如下性质: 行变换将矩阵 A 的零行变换为零行, 并且不改变其他行的零性.

1.7 挑战选读: 舒伯特胞腔的计数

挑战选读说明

Schubert cell 是表示论、代数几何和代数组合中非常重要的对象. 本小节只是借助最简行阶梯型展示它最初级的组合影子, 不属于第一章主线内容. 初学时可以完全跳过, 不影响后续关于线性方程组、矩阵和线性空间的学习.

最简行阶梯型的存在唯一性给出来了 $m \times n$ 矩阵在行变换所定义的等价关系下的标准形式的唯一性. 这种表达方式在几何和代数中有广泛的应用. 在本节中, 我们介绍舒伯特胞腔的概念, 并通过最简行阶梯型来描述舒伯特胞腔的结构. 设 k, n 为正整数, 且 $k \leq n$. 在之后的章节中, 我们定义 \mathbb{R}^n 中所有通过原点的 k 维子空间的集合为格拉斯曼流形 (Grassmannian) $G(k, n)$. 对这种几何对象组成的族进行参数化会引入舒伯特胞腔 (Schubert cell) 的概念. 最简阶梯型的组合结构将给出一些有意思的计数结果. 我们首先在以下两个例子中讨论三维空间中的直线和平面的情况.

例 1.9. 考虑 2×3 阶矩阵 A , 满足 $\text{rank } A = 2$, 则 $A\mathbf{x} = \mathbf{0}$ 这个线性方程组的解反映在 \mathbb{R}^3 中的几何意义则是 \mathbb{R}^3 中穿过原点的直线. 由于 $\text{rank } A = 2$, 则最简行阶梯型 $\text{rref } A$ 拥有的可能性如下:

$$\begin{pmatrix} 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{pmatrix}, \quad \begin{pmatrix} 1 & b & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

所以 \mathbb{R}^3 中通过原点的直线的集合 $G(1, 3)$ 一一对应于

$$\mathbb{R}^2 \amalg \mathbb{R} \amalg \mathbb{R}^0,$$

其中 \mathbb{R}^0 表示单点集.

例 1.10. 考虑 2×3 阶矩阵 A , 满足 $\text{rank } A = 1$, 则 $A\mathbf{x} = \mathbf{0}$ 这个线性方程组的解反映在 \mathbb{R}^3 中的几何意义则是 \mathbb{R}^3 中穿过原点的二维平面. 由于 $\text{rank } A = 1$, 则最简行阶梯型 $\text{rref } A$ 拥有的可能性如下:

$$\begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & b \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

所以 \mathbb{R}^3 中通过原点的平面的集合 $G(2, 3)$ 一一对应于

$$\mathbb{R}^2 \amalg \mathbb{R} \amalg \mathbb{R}^0.$$

更一般的, 我们可以考虑 \mathbb{R}^4 中的平面.

例 1.11. 考虑 2×4 阶矩阵 A , 满足 $\text{rank } A = 2$, 则 $A\mathbf{x} = \mathbf{0}$ 这个线性方程组的解反映在 \mathbb{R}^4 中的几何意义则是 \mathbb{R}^4 中穿过原点的二维平面. 由于 $\text{rank } A = 2$, 则最简行阶梯型 $\text{rref } A$ 拥有的可能性如下:

$$\begin{pmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & a_3 & a_4 \end{pmatrix}, \quad \begin{pmatrix} 1 & b_1 & 0 & b_2 \\ 0 & 0 & 1 & b_3 \end{pmatrix}, \quad \begin{pmatrix} 1 & c_1 & c_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & d_1 \\ 0 & 0 & 1 & d_2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & e & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

所以 \mathbb{R}^4 中通过原点的平面的集合 $G(2, 4)$ 一一对应于

$$\mathbb{R}^4 \amalg \mathbb{R}^3 \amalg \mathbb{R}^2 \amalg \mathbb{R}^2 \amalg \mathbb{R} \amalg \mathbb{R}^0.$$

对于一般 \mathbb{R}^n 的 k 维子空间, 我们类似的将其表示成 $n - k$ 线性方程的形式, 或者是有 $m = n - k$ 个主元的 $m \times n$ 最简阶梯型矩阵. 在这种对应下, 我们定义 $G(k, n)$ 的舒伯特胞腔以及对应的胞腔维数为如下:

定义 1.13. 考虑秩为 m 的 $m \times n$ 阶最简行阶梯型矩阵组成的集合 $G(n-m, n)$. 其中主元分别固定在 $i_1 < i_2 < \dots < i_m$ 列的所有最简行阶梯型矩阵称为 $G(n-m, n)$ 中的**舒伯特胞腔** (Schubert cell). 每个舒伯特胞腔中的参数定义了一个从 \mathbb{R}^d 到该胞腔的双射, 其中 d 称为该胞腔的维数.

在上述用 $m = n - k$ 个方程描述 $G(k, n)$ 的约定下, 若主元列为 $i_1 < \dots < i_m$, 则第 j 个主元行的自由参数个数为 $k + j - i_j$. 因此对应胞腔的维数为

$$d = \sum_{j=1}^m (k + j - i_j).$$

对应的舒伯特胞腔的计数的生成函数称为格拉斯曼流形的庞加莱多项式

定义 1.14. 格拉斯曼流形 $G(k, n)$ 的**庞加莱多项式** (Poincaré polynomial)定义为

$$P_{k,n}(t) = \sum_{d \geq 0} c_d t^d,$$

其中 c_d 是 $G(k, n)$ 中维数为 d 的舒伯特胞腔的个数.

以上的例子1.9, 1.10和1.11中我们已经计算出了 $G(1, 3)$, $G(2, 3)$ 和 $G(2, 4)$ 的庞加莱多项式分别为

$$P_{1,3}(t) = t^2 + t + 1,$$

$$P_{2,3}(t) = t^2 + t + 1,$$

$$P_{2,4}(t) = t^4 + t^3 + 2t^2 + t + 1.$$

由于所有的舒伯特胞腔均可以通过选择主元所在的列 $i_1 < i_2 < \dots < i_m$ 来唯一确定, 因此舒伯特胞腔的个数等于 n 列取 m 列的个数.

命题 1.8. 对于格拉斯曼流形 $G(k, n)$, 其舒伯特胞腔的总数为

$$P_{k,n}(1) = \binom{n}{k}.$$

其中维数最大的舒伯特胞腔对应于主元最靠近左边的情形, 即主元在第 $1, 2, \dots, m$ 列. 此时胞腔的维数为 $m(n-m)$.

更一般的, 我们可以得到庞加莱多项式的通项公式. 我们首先推广一下二项式系数的概念.

定义 1.15. 对于非负整数 n, k 满足 $k \leq n$, 定义 **q -整数**为

$$[n]_q = 1 + q + q^2 + \dots + q^{n-1} = \frac{1 - q^n}{1 - q},$$

则定义 q -阶乘为

$$[n]_q! = [n]_q[n-1]_q \cdots [1]_q,$$

类似的定义 q -二项式系数(也称为高斯系数)为

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}.$$

定理 1.10. 格拉斯曼流形 $G(k, n)$ 的庞加莱多项式为

$$P_{k,n}(t) = \binom{n}{k}_t.$$

证明. 令 $m = n - k$. 由上面的维数公式,

$$P_{k,n}(t) = \sum_{1 \leq i_1 < \cdots < i_m \leq n} t^{\sum_{j=1}^m (k+j-i_j)}.$$

我们按最后一列是否为主元来分类. 如果第 n 列是主元, 则 $i_m = n$, 最后一行不贡献自由参数, 其余主元列给出 $G(k, n-1)$ 中的胞腔, 贡献为 $P_{k,n-1}(t)$. 如果第 n 列不是主元, 则所有主元列都落在前 $n-1$ 列; 与 $G(k-1, n-1)$ 中同一组主元列相比, 每一行多出最后这一列的一个自由参数, 总共多出 $m = n - k$ 个自由参数, 贡献为 $t^{n-k} P_{k-1,n-1}(t)$. 因此

$$P_{k,n}(t) = P_{k,n-1}(t) + t^{n-k} P_{k-1,n-1}(t),$$

并且边界条件为 $P_{0,n}(t) = P_{n,n}(t) = 1$. 另一方面, t -二项式系数满足同样的递推关系和边界条件:

$$\binom{n}{k}_t = \binom{n-1}{k}_t + t^{n-k} \binom{n-1}{k-1}_t.$$

故 $P_{k,n}(t) = \binom{n}{k}_t$. □

也可以通过归纳的方式证明庞加莱多项式和 q -二项式系数都满足类似的递推关系, 从而得到定理 1.10. 这一对 q -二项式系数的组合解释也证明 q -二项式系数是多项式, 并且系数均为非负整数. 通过组合公式, 我们还可以得到庞加莱多项式是对称的, 即 $P_{k,n}(t) = P_{n-k,n}(t)$. 其系数还有回文对称性 (palindromic).

命题 1.9. 格拉斯曼流形 $G(k, n)$ 的庞加莱多项式满足

$$P_{k,n}(t) = t^{k(n-k)} P_{k,n}(t^{-1}).$$

其中还有一个重要的单峰性质 (unimodality) 我们暂时无法用初等办法验证.

命题 1.10 (单峰性质). 格拉斯曼流形 $G(k, n)$ 的庞加莱多项式 $P_{k,n}(t) = \sum_{d \geq 0} c_d t^d$ 的系数列 $\{c_d\}$ 满足单峰性质, 即存在某个 d_0 使得 $c_0 \leq c_1 \leq \dots \leq c_{d_0} \geq c_{d_0+1} \geq \dots$.

在引入有限域上的线性空间之后, 我们还可以对定理1.10给出另一种组合解释, 这里就不再赘述.

比起“算出一个解”, 我们经常更关心“解集的结构”

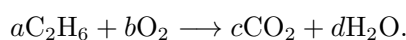
在很多实际问题中, 我们真正关心的不是某一个答案, 而是所有可能答案的形状. 例如化学方程式配平给出的是一个齐次线性方程组, 因此配平系数通常只确定到一个共同倍数; 电路中的 Kirchhoff 电流定律会给出若干线性约束, 自由元对应可以自由选择支路电流; 图上的稳定温度问题中, 边界温度确定后内部温度是否唯一. 主元和自由元的语言把这些现象统一了起来.

1.8 习题

1.8.1 练习题

习题里所有矩阵不加说明都是实矩阵.

习题 1.2 (建模: 化学方程式配平). 用线性方程组配平乙烷燃烧反应



1. 分别根据 C、H、O 三种元素守恒写出关于 a, b, c, d 的齐次线性方程组.
2. 求出所有解, 并取最小正整数解.
3. 解释为什么配平方程的解通常只确定到一个共同倍数.

习题 1.3 (三元一次方程组的几何图像). 下列每个方程组都表示三个平面的交集. 分别判断其解集是空集、一个点、一条直线、一个平面, 还是整个空间, 并用消元法验证.

$$\begin{cases} x + y + z = 1, \\ 2x + y - z = 0, \\ x - y + 2z = 3, \end{cases} \quad \begin{cases} x + y + z = 1, \\ 2x + 2y + 2z = 2, \\ x - y = 0, \end{cases} \quad \begin{cases} x + y + z = 1, \\ 2x + 2y + 2z = 3, \\ x - y = 0. \end{cases}$$

习题 1.4. 用消元法解线性方程组

1. 关于两个变元 x_1, x_2 的线性方程组

$$\begin{cases} x_1 - 2x_2 = 1 \\ 2x_1 - x_2 = 2 \end{cases}$$

2. 关于四个变元 x_1, x_2, x_3, x_4 的线性方程组

$$\begin{cases} x_1 - 2x_2 + 3x_3 - 4x_4 = 4 \\ x_2 - x_3 + x_4 = -3 \\ x_1 + 3x_2 + x_4 = 1 \\ -7x_2 + 3x_3 + x_4 = -3 \end{cases}$$

3. 关于三个变元 x, y, z 的线性方程组

$$\begin{cases} 2x + y - z = 8 \\ -3x - y + 2z = -11 \\ -2x + y + 2z = -3 \end{cases}$$

习题 1.5. 讨论 λ 取何值时, 线性方程组

$$\begin{cases} \lambda x_1 + x_2 + x_3 = 1 \\ x_1 + \lambda x_2 + x_3 = \lambda \\ x_1 + x_2 + \lambda x_3 = \lambda^2 \end{cases}$$

有唯一解, 无穷多解, 无解, 并在有解时求其解。

习题 1.6. 考虑包含 m 个主元的最简阶梯型的 $m \times n$ 的实矩阵, 主元出现的位置相同的这样的矩阵视作一类, 求不同的种类数有多少?

习题 1.7. 考虑一个连通无向无圈无多重边的有限图 G . 令 V 是顶点的集合, 将其视为网页, 构造如下网络. 如果两个顶点之间有边连接, 则假设两个网页之间有彼此两个方向之间的超链接连接. 我们利用 Google 的 PageRank 算法得到关于每个网页重要性 $(x_i)_{i \in V}$ 的线性方程组. 证明此时 x_i 等于经过顶点 i 的边数是这个方程组的一组解.

习题 1.8. 构造一个 3 阶方阵, 其 9 个元素各不相同, 且行简化阶梯型有且只有一个主元.

习题 1.9. 设

$$A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

证明

1. $Ax = b$ 有解当且仅当 $b_1 + b_2 + b_3 = 0$.

2. $Ax = 0$ 的解集是 $\{kx_1 : k \in \mathbb{R}\}$, 其中 $x_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$.

3. 当 $Ax = b$ 有解时, 若 x_0 是一个解, 则解集是 $\{x_0 + kx_1 : k \in \mathbb{R}\}$.

习题 1.10. 把下列矩阵化为最简行阶梯型: (默认空格处为 0)

1.
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{pmatrix}$$

2.
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 0 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{pmatrix}$$

3.
$$\begin{pmatrix} 1 & 1 & & & \\ 1 & 2 & 1 & & \\ & 1 & 2 & 1 & \\ & & & 1 & 2 \end{pmatrix}$$

4.
$$\begin{pmatrix} 2 & 1 & & & \\ 1 & 2 & 1 & & \\ & 1 & 2 & 1 & \\ & & & 1 & 2 \end{pmatrix}$$

5.
$$\begin{pmatrix} 1 & 1 & -1 \\ 2 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}$$

习题 1.11. 考虑一个连通无向无圈无多重边的有限图 G . 假设 V 是顶点的集合, 其中只有一条边相连的顶点称为边界点, 有多条边相连的顶点称为内部点. 假设内部点和边界点的集合都非空. 对每一个顶点 i 取一个温度 $T_i \in \mathbb{R}$, 称 $T = (T_i)_{i \in V}$ 是一个图上的温度分布. 如果每一个内部点的温度等于与之相连的点的温度的平均值, 则称这一分布称为稳定的. 证明: 对于每一组边界点的温度值, 存在唯一的内部点的温度取值, 使得这一温度分布是稳定的.

习题 1.12. 将下列问题转化为求解线性方程组的问题, 并求解:

1. 设 2×2 矩阵 A 满足 $A \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$ 且 A 的第一列元素之和为 2, 求所有可能的 A .

2. 空间中有一个平面经过点 $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, 求所有与该平面垂直的向量.

3. 写出通过 5 点 $M_1(0, 1), M_2(2, 0), M_3(-2, 0), M_4(1, -1), M_5(-1, -1)$ 的二次曲线的方程. 这里二次曲线是 xy -平面上形如 $ax^2 + bxy + cy^2 + dx + ey + f = 0$ 的方程决定的曲线.

习题 1.13. 若 A, C 均为 $m \times n$ 矩阵, 如果对任何 b , 线性方程组 $Ax = b$ 与 $Cx = b$ 都有相同的解集, 是否一定有 $A = C$?

习题 1.14. 证明: 交换矩阵的两行或者两列不改变秩.

习题 1.15. 设 A 为 $m \times n$ 矩阵, B 为 $m \times k$ 矩阵, 证明 $\text{rank}(AB) \leq \text{rank}(A) + \text{rank}(B)$.

习题 1.16. 判断下列方程是否为线性方程. 若不是, 请说明原因.

$$2x - 3y + z = 1, \quad xy + z = 2, \quad x^2 - y = 0, \quad \frac{1}{2}x + 4y = 7.$$

习题 1.17. 解下列线性方程组.

$$\begin{cases} x + y + z = 6, \\ 2x - y + z = 3, \\ x + 2y - z = 2. \end{cases}$$

习题 1.18. 用消元法判断下列方程组有无解. 若有解, 写出全部解.

$$\begin{cases} x + 2y - z = 1, \\ 2x + 4y - 2z = 3. \end{cases}$$

习题 1.19. 求下列方程组的增广矩阵, 并把它化为阶梯形矩阵.

$$\begin{cases} x - y + 2z = 4, \\ 2x + y - z = 1, \\ 3x + 0y + z = 5. \end{cases}$$

习题 1.20. 设参数 $a \in \mathbb{R}$. 讨论下列方程组在不同 a 下解的情况.

$$\begin{cases} x + y = 1, \\ 2x + 2y = a. \end{cases}$$

习题 1.21. 求齐次方程组的全部解, 并用一个或几个向量表示解集.

$$\begin{cases} x + y + z = 0, \\ 2x - y + z = 0. \end{cases}$$

习题 1.22. 给出一个三元一次方程组, 使它的解集是一条直线. 再给出一个三元一次方程组, 使它没有解.

1.8.2 思考题

习题 1.23. 若 A, A' 均为 $m \times n$ 矩阵, b, b' 为 m 维向量, 方程 $Ax = b$ 与 $A'x = b'$ 的解集相同且非空, 请思考 (A', b') 是否一定可由 (A, b) 经过行变换得到, 你能对 $m = n = 2$ 写出证明吗?

习题 1.24 (二次曲线束与线性方程组). 平面上的二次曲线是指形如

$$F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

的曲线, 其中 $a, b, c, d, e, f \in \mathbb{R}$ 且不全为零. 已知平面上两条不同的二次曲线

$$F_i(x, y) = a_i x^2 + b_i xy + c_i y^2 + d_i x + e_i y + f_i = 0 \quad (i = 1, 2)$$

恰好交于四个不同的点 (x_i, y_i) , $i = 1, 2, 3, 4$. 求证: 过这四个点的任意二次曲线

$$F(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

均可写为 $\lambda_1 F_1 + \lambda_2 F_2 = 0$ 的形式, 其中 λ_1, λ_2 不全为零.

2 矩阵运算

本章我们介绍矩阵的基本概念及其运算. 矩阵是线性代数中最基本的对象之一, 其在数学和应用数学中有广泛的应用. 线性方程组的系数矩阵就是矩阵的一个重要应用, 此外矩阵还可以用来表示线性映射, 并且在计算机图形学中有重要的应用. 本章我们主要介绍矩阵的加法和乘法等基本运算, 并且介绍矩阵的转置和逆矩阵等概念.

2.1 加法, 数乘与乘法

在 $M_{m \times n}(\mathbb{R})$ 上定义如下的运算:

1. 加法: $A = (a_{ij})_{m \times n}, B = (b_{ij})_{m \times n}$, 则 $A + B := (a_{ij} + b_{ij})_{m \times n}$.
2. 数乘: $A = (a_{ij})_{m \times n}, c \in \mathbb{R}$, 则 $cA := (ca_{ij})_{m \times n}$.

以上两种结构和列向量空间的 \mathbb{R}^n 上的加法和数乘一样. 此外矩阵空间还有额外的乘法结构, 在研究线性方程组的时候我们已经见到了矩阵和列向量相乘的例子: 给定

$$\mathbf{c} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \mathbb{R}^n \text{ 和 } A \in M_{m \times n}(\mathbb{R}),$$

如果按照列向量排列的形式将 A 记做 $A = (\mathbf{v}_1, \dots, \mathbf{v}_n)$, 那么

$$A\mathbf{c} := c_1\mathbf{v}_1 + \dots + c_n\mathbf{v}_n,$$

也即是以 c_1, \dots, c_n 为系数的 A 中的列向量 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 的线性组合.

对于两个矩阵 A, B , 如果 A 的列数与 B 的行数相同, 我们则可以用上面的办法将矩阵乘法定义为:

定义 2.1. 对于 $A \in M_{m \times n}(\mathbb{R})$ 以及 $B = (\mathbf{w}_1, \dots, \mathbf{w}_\ell) \in M_{n \times \ell}(\mathbb{R})$, 则**矩阵乘法** (*matrix multiplication*) 定义为

$$AB := (A\mathbf{w}_1, \dots, A\mathbf{w}_\ell).$$

同时, 矩阵乘法还可以用如下等价的方式定义:

定义 2.2. 对于 $A = (a_{ij}) \in M_{m \times n}(\mathbb{R}), B = (b_{ij}) \in M_{n \times l}(\mathbb{R})$, 则**矩阵乘法** (*matrix multiplication*) 定义为 $AB := (c_{ij})_{m \times l}$, 其中

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}.$$

由于定义 2.2 中的对称性, 我们还可以从行向量的角度理解矩阵乘法: 左边矩阵的每一行给出右边矩阵各行的线性组合.

定义 2.3. 对于 $A \in M_{m \times n}(\mathbb{R})$ 以及 $B \in M_{n \times \ell}(\mathbb{R})$, 将 A 写作

$$A = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{pmatrix}$$

其中 \mathbf{a}_i 是行向量, 那么 AB 定义为具有如下行向量的矩阵:

$$AB = \begin{pmatrix} \mathbf{a}_1 B \\ \mathbf{a}_2 B \\ \vdots \\ \mathbf{a}_m B \end{pmatrix}.$$

每一行 $\mathbf{a}_i B$ 是 B 的行向量的线性组合, 其系数由 \mathbf{a}_i 给出.

注 2.1. 对于矩阵 A, B , 只有 A 的列数与 B 的行数相同时, 矩阵乘法 AB 才有意义.

矩阵乘法与计算机图形

二维或三维图形中的一个点可以写成列向量. 旋转、缩放、错切、投影等操作都可以用矩阵表示, 而连续做两个图形变换就对应矩阵乘法. 例如先旋转再拉伸, 和先拉伸再旋转, 通常得到不同结果, 这正是矩阵乘法一般不交换的几何原因. 计算机动画、游戏引擎、机器人姿态控制中反复出现的“坐标变换链”, 本质上就是矩阵乘法的链式复合.

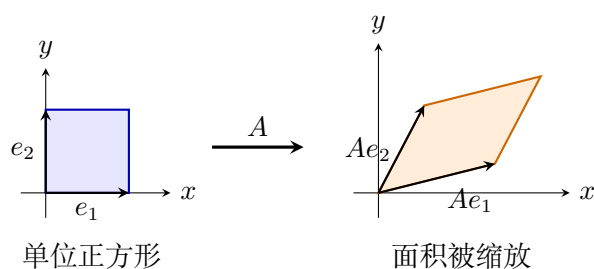


图 11: 矩阵由两个列向量 Ae_1, Ae_2 决定, 并把单位正方形变成平行四边形.

例 2.1 (二阶矩阵乘法). 设

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}.$$

则

$$AB = \begin{pmatrix} 1 \cdot 0 + 2 \cdot (-1) & 1 \cdot 1 + 2 \cdot 2 \\ 3 \cdot 0 + 4 \cdot (-1) & 3 \cdot 1 + 4 \cdot 2 \end{pmatrix} = \begin{pmatrix} -2 & 5 \\ -4 & 11 \end{pmatrix}.$$

注意每个位置都是“左边矩阵的一行”与“右边矩阵的一列”对应相乘再相加。

习题 2.1. 计算

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

再交换两个矩阵的顺序计算一次, 比较两个结果是否相同。

命题 2.1. 矩阵乘法具有结合律. 即对于任意 $A \in M_{m \times n}(\mathbb{R}), B \in M_{n \times p}(\mathbb{R}), C \in M_{p \times q}(\mathbb{R})$, 有

$$(AB)C = A(BC).$$

证明. 记 $A = (a_{ir}), B = (b_{r\ell}), C = (c_{\ell j})$. 对任意第 i 行第 j 列的位置, 有

$$\begin{aligned} ((AB)C)_{ij} &= \sum_{\ell=1}^p (AB)_{i\ell} c_{\ell j} = \sum_{\ell=1}^p \left(\sum_{r=1}^n a_{ir} b_{r\ell} \right) c_{\ell j} \\ &= \sum_{r=1}^n a_{ir} \left(\sum_{\ell=1}^p b_{r\ell} c_{\ell j} \right) = \sum_{r=1}^n a_{ir} (BC)_{rj} = (A(BC))_{ij}. \end{aligned}$$

两个矩阵在每一个位置上的元素都相同, 因此 $(AB)C = A(BC)$. □

注意到一组向量本身也是其线性组合, 组合系数组成的矩阵就会是乘法的单位元。

定义 2.4. 对于 $n \in \mathbb{N}$, 定义 $n \times n$ 阶的**单位矩阵** (*identity matrix*) 为

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

命题 2.2. 对于任意 $A \in M_{m \times n}(\mathbb{R})$, 有

$$I_m A = A I_n = A.$$

一类和单位矩阵类似的矩阵是纯量矩阵和对角矩阵:

定义 2.5. 一个 $n \times n$ 阶矩阵 $D = (d_{ij})$ 如果满足 $d_{ij} = 0$ 当 $i \neq j$ 时, 则称 D 为一个**对角矩阵** (*diagonal matrix*). 此时也记作 $D = \text{diag}(d_{11}, d_{22}, \dots, d_{nn})$. 特别地, 如果 $d_{11} = d_{22} = \cdots = d_{nn} = c$, 则称 D 为**纯量矩阵** (*scalar matrix*), 记作 cI_n .

注意, 在有些情况下, 对一般的 $m \times n$ 阶矩阵也可以定义对角矩阵, 即 $d_{ij} = 0$ 当 $i \neq j$ 时. 这里我们暂时只考虑方阵的对角矩阵. 可由定义得到对角阵的乘法是对角线元素的逐点乘积:

命题 2.3. 对于任意对角矩阵 $A = \text{diag}(a_1, a_2, \dots, a_n)$ 和 $B = \text{diag}(b_1, b_2, \dots, b_n)$, 有

$$AB = BA = \text{diag}(a_1 b_1, a_2 b_2, \dots, a_n b_n).$$

由加法和乘法的分配律, 我们还得到加法, 数乘与乘法之间的关系:

命题 2.4. 对于任意 $A, B \in M_{m \times n}(\mathbb{R}), C \in M_{n \times \ell}(\mathbb{R}), D \in M_{p \times m}(\mathbb{R})$ 以及 $\lambda \in \mathbb{R}$, 有

- (1) $D(A + B) = DA + DB$;
- (2) $(A + B)C = AC + BC$;
- (3) $\lambda(AC) = (\lambda A)C = A(\lambda C)$.

一般情况下, 矩阵的乘法不满足交换律, 即 $AB \neq BA$, 甚至有可能一个乘积有定义而另一个没有定义. 例如对于 $A \in M_{m \times n}(\mathbb{R}), B \in M_{n \times \ell}(\mathbb{R})$, 则 AB 有定义, 但是 $\ell \neq m$ 时, BA 没有定义. 即使 $m = \ell$ 时, BA 有定义, 在 $m \neq n$ 时, AB 和 BA 的阶数也不同. 即使 $m = n = \ell$ 时, AB 和 BA 的阶数相同, 但是一般情况下仍然有 $AB \neq BA$. 例如我们取 A 是 n 阶对角阵, 其对角线元素依次为 c_1, c_2, \dots, c_n , 且 c_i 两两不同, 则和 A 交换的 n 阶方阵 B 也必须是对角阵.

2.2 行变换和矩阵乘法

由于对矩阵 A 左乘某个矩阵可以视为做 A 行向量的线性组合 (定义2.3), 而行变换也正好是对行做一些线性组合 (命题1.5), 我们可以重新将之前对系数矩阵做的初等行变换用矩阵的语言再解释一遍.

定义 2.6. 如下的三类矩阵被称为**初等矩阵** (*elementary matrix*):

(E1)

$$E[ij] = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 0 & \cdots & 1 & & & & \\ & & \vdots & \ddots & \vdots & & & & \\ & & 1 & \cdots & 0 & & & & \\ & & & & & \ddots & & & \\ & & & & & & & & 1 \end{pmatrix}$$

即交换 I_n 的第 i 行与第 j 行得到的矩阵.

(E2)

$$E[i, c] = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & c & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

即将 I_n 的第 i 行乘以 c 得到的矩阵, 其中 $c \neq 0$.

(E3)

$$E[ij, c] = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \vdots & \ddots & \\ & & c & \cdots & 1 \\ & & & & \ddots \\ & & & & & 1 \end{pmatrix}$$

即将 I_n 的第 i 行乘以 c 加到第 j 行得到的矩阵, 其中 $c \neq 0$.

这三类矩阵分别对应于在恒等矩阵上做初等行变换 (E1),(E2),(E3) 得到的矩阵, 这里得到的每一行是恒等矩阵对应行的线性组合, 所以组合系数就是得到的初等矩阵的每一行. 如果同样的操作对矩阵 A 来做, 那么对应就是以这些系数来做 A 的行向量的线性组合, 也就是等于这个初等矩阵与 A 的乘积.

命题 2.5. 对 $A \in M_{m \times n}(\mathbb{R})$ 做初等行变换 O 等价于对左乘相应的初等矩阵 E .

例 2.2. 假设矩阵

$$A = \begin{pmatrix} \mathbf{r}_1 \\ \mathbf{r}_2 \\ \mathbf{r}_3 \end{pmatrix},$$

那么如果我们对其作用 (E3) 将第三行的 2 倍加到第一行上去, 得到的新的系数矩阵记做 A' , 那么

$$A' = \begin{pmatrix} \mathbf{r}_1 + 2\mathbf{r}_3 \\ \mathbf{r}_2 \\ \mathbf{r}_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A.$$

因此我们可以看出初等行变换 (E3) 可以看作是初等矩阵 (E3) 左乘.

推论 2.1. 对 A 做行变换 $O_1 \dots O_k$ 等价于左乘对应的初等矩阵的乘积 $E_k \dots E_2 E_1$, 其中 E_i 是对应于行变换 O_i 的初等矩阵.

在很多时候我们想记录下来对矩阵做了一系列初等行变换之后左乘的矩阵 $E_k \dots E_2 E_1$ 是什么, 此时我们有如下常用的方法.

命题 2.6. 设 $A \in M_{m \times n}(\mathbb{R})$. 将 A 与 m 阶单位矩阵 I_m 按列拼接起来, 记做 $(A|I_m)$. 如果对 $(A|I_m)$ 做初等行变换 O_1, \dots, O_k 得到 $(E_k \dots E_2 E_1 A|B)$, 其中 E_i 是对应于行变换 O_i 的 m 阶初等矩阵, 那么 $B = E_k \dots E_2 E_1$.

证明. 由于行变换只对行进行线性组合, 因此对 $(A|I_m)$ 做行变换 O_1, \dots, O_k 等价于分别对 A 和 I_m 做同样的行变换. 由上面的讨论可知, 对 A 做这些行变换等价于左乘 $E_k \dots E_2 E_1$, 而对 I_m 做这些行变换等价于左乘 $E_k \dots E_2 E_1$. 因此拼接起来的结果就是 $(E_k \dots E_2 E_1 A|E_k \dots E_2 E_1)$. \square

2.3 矩阵的逆

注意到我们的初等行变换是可逆的, 用矩阵的语言来说, 对于初等矩阵 $B \in M_n(\mathbb{R})$, 总存在另一个初等矩阵 B' 使得 $B'BA = A$ 对任意的 $A \in M_{n \times m}(\mathbb{R})$ 成立. 或者等价的 $B'B = I_n$. 我们定义如下的概念:

定义 2.7. 对于矩阵 $A \in M_n(\mathbb{R})$

- (1) 若有 B 使得 $BA = I_n$, 则称 B 为 A 的**左逆** (*left inverse*).
- (2) 若有 C 使得 $AC = I_n$, 则称 C 为 A 的**右逆** (*right inverse*).
- (3) 如果左逆右逆均存在, 则称 A **可逆** (*invertible*).

由前面初等行变换可逆的结论, 我们知道初等矩阵均存在左逆. 更一般的, 我们有如下对于可逆性的等价性定理:

定理 2.1. 对于矩阵 $A \in M_n(\mathbb{R})$, 如下叙述等价:

1. A 可逆.
2. A 存在左逆.
3. A 存在右逆.
4. $\text{rref}(A) = I_n$.
5. 对任意 $b \in \mathbb{R}^n$, 方程 $Ax = b$ 有唯一解.
6. 存在某个 $b \in \mathbb{R}^n$, 方程 $Ax = b$ 有唯一解.
7. $Ax = 0$ 只有零解.

8. $\text{rank } A = n$.

9. 矩阵 A 可以表示为初等矩阵的乘积.

证明. 根据线性方程组解的结构定理, 即定理1.4, 我们已经知道 (4),(5),(7),(8) 等价. 显然 (5) \Rightarrow (6). 反过来, 如果存在某个 b 使 $Ax = b$ 有唯一解, 设其解为 x_0 . 若 $Ax = 0$ 有非零解 u , 则 $x_0 + u$ 也是 $Ax = b$ 的解, 与唯一性矛盾, 因此 $Ax = 0$ 只有零解. 所以 (6) \Rightarrow (7). 这说明 (4),(5),(6),(7),(8) 等价.

(2) \Rightarrow (7): 如果 A 存在左逆 B , 那么 $Ax = 0$ 推出 $x = BAx = B0 = 0$, 即 $Ax = 0$ 只有零解.

(5) \Rightarrow (3): 如果对任意 $b \in \mathbb{R}^n$, 方程 $Ax = b$ 都存在唯一解, 那么取标准基向量

$$b_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots$$

那么不妨记 $Ax = b_1, Ax = b_2, \dots, Ax = b_n$ 唯一的解分别是 w_1, \dots, w_n . 令 $C = (w_1, \dots, w_n)$ 则 $AC = I_n$, 即 C 是 A 的右逆.

注 2.2. 至此已经证明了如果矩阵 A 存在左逆, 那么其一定存在右逆, 即 (2) \Rightarrow (3).

(3) \Rightarrow (2): 假设 A 有右逆, 存在 C 使得 $AC = I_n$, 从而 $CAC = C$. 另一方面, 由于 C 存在左逆 A , 从而 C 存在右逆, 不妨记为 D , 因此

$$CA = CACD = CD = I_n$$

即 C 也是 A 的左逆.

(9) \Rightarrow (2): 如果 A 可以表示为初等矩阵的乘积, 那么由于初等矩阵均有左逆, 因此 A 也有左逆.

(4) \Rightarrow (9): 如果 $\text{rref}(A) = I_n$, 那么根据推论2.1, 存在初等矩阵 E_1, \dots, E_k 使得 $E_k E_{k-1} \cdots E_1 A = I_n$, 因此 $A = E_1^{-1} E_2^{-1} \cdots E_k^{-1}$, 也即 A 可以表示为初等矩阵的乘积. \square

命题 2.7. 若 A 可逆, 则左逆与右逆均唯一存在且相同, 记做 A^{-1} .

证明. 我们只需要证明如果 A 可逆, 那么其左逆右逆都唯一: 假设 C 是 A 的一个左逆, D 是 A 的一个右逆, 那么

$$C = CI_n = CAD = I_n D = D$$

即 A 的任何左逆与右逆都相同. 那么假设 C_1, C_2 是 A 的两个左逆, 由于 C_1 也是 A 的右逆, 从而 $C_1 = C_2$, 即 A 的左逆唯一, 类似的, 我们也可以说明 A 的右逆唯一. \square

注 2.3 (求逆方法). 上述结论表明, 如果 A 可逆, 那么 $\text{rref}(A) = I_n$, 而根据推论 2.1 可知行变换等价于左乘初等矩阵, 因此将其化为最简行阶梯型的初等矩阵的乘积就是 A^{-1} . 那么我们应该如何将这此初等矩阵的乘积记录下来呢? 考虑矩阵 (A, I_n) , 对其进行操作使得 A 化为最简行阶梯型, 那么对应的左乘的矩阵 B , 则有 $B(A, I_n) = (I, B)$, 所以此时 $B = A^{-1}$. 这样左乘的矩阵记录在了右边, 从而给出了 A 的逆.

例 2.3. 考虑

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix},$$

则

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

因此

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

注 2.4. 更一般的, 那么我们有如下的求 2 阶可逆方阵逆的办法:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

2.4 矩阵的转置

矩阵中一个很常见的操作就是将矩阵的行与列进行交换, 这就是矩阵的转置操作.

定义 2.8. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 其转置矩阵 (*transpose matrix*) 是一个 $n \times m$ 阶矩阵 $A^T = (b_{ij})_{n \times m}$, 其中 $b_{ij} = a_{ji}$.

定义 2.9. 如果矩阵 $A \in M_n(\mathbb{R})$ 满足 $A^T = A$, 则被称为对称矩阵 (*symmetric matrix*). 类似的, 如果 $A^T = -A$, 则称为反对称矩阵 (*skew-symmetric matrix*).

例 2.4. 对于列向量来说, 其转置为行向量; 对于行向量来说, 其转置为列向量.

命题 2.8. 对于矩阵转置来说, 我们有如下性质:

1. $(A^T)^T = A$.
2. $(AB)^T = B^T A^T$.

证明. (1): 直接根据定义即可. (2): 由矩阵的乘法视为列向量的线性组合或者行向量的线性组合可得到. \square

推论 2.2. 对矩阵 A 做列变换等价于右乘可逆矩阵.

证明. 利用转置矩阵的观点, 对矩阵 A 进行列变换, 等价于对 A^T 进行行变换再转置. 对 A^T 做行变换等价于左乘某个可逆矩阵 E , 得到 EA^T . 再转置得到 $(EA^T)^T = AE^T$. 由于 E^T 仍然可逆, 所以列变换等价于右乘可逆矩阵. \square

2.5 秩在行列变换下的不变性

回忆定义1.8, 我们定义矩阵 A 的秩为其最简行阶梯型的主元个数. 一个自然的问题就是 A^T 的秩与 A 的秩有什么关系呢?¹ 我们可以证明 $\text{rank } A = \text{rank } A^T$, 这主要依赖于下面的定理.

定理 2.2. 列变换不改变矩阵 A 的秩.

这里证明中将用到的线性方程组解的结构定理, 即定理1.4的两个推论

1. 如果方程个数小于未知数个数, 那么齐次线性方程组 $Ax = 0$ 中一定有自由元, 从而有非零解.
2. 齐次线性方程组 $Ax = 0$ 的某个解等于零当且仅当对应的自由元等于零.

证明. 根据推论2.2, 对矩阵 A 作列变换等价于右乘可逆矩阵. 因此我们只需要证明对于可逆矩阵 B , 有 $\text{rank } A = \text{rank}(AB)$. 记 $C = AB$, 令 $r = \text{rank } A, s = \text{rank } C$. 假设 $s > r$. 考虑齐次线性方程组 $Ax = 0$, 则有主元 x_{i_1}, \dots, x_{i_r} , 以及自由元 $x_{j_1}, \dots, x_{j_{n-r}}$. 由定理1.4, 该方程组的解集可以表达为

$$Ax = 0 \iff x_{i_k} = f_k(x_{j_1}, \dots, x_{j_{n-r}}), \forall k = 1, 2, \dots, r \quad (4)$$

其中每个 f_k 都是自由元 $x_{j_1}, \dots, x_{j_{n-r}}$ 的线性函数.

另一方面, 考虑齐次线性方程组 $Cy = 0$, 则其解和 $Ax = 0$ 的解有一一对应关系, 即 $x = By, y = B^{-1}x$.

假设方程组 $Cy = 0$ 有主元 y_{p_1}, \dots, y_{p_s} , 以及自由元 $y_{q_1}, \dots, y_{q_{n-s}}$. 将求解公式(4)代入表达式 $y = B^{-1}x$ 中自由元 $y_{q_1}, \dots, y_{q_{n-s}}$ 所在的行, 我们得到一系列线性函数

$$y_{q_t} = g_t(x_{j_1}, \dots, x_{j_{n-r}}), \forall t = 1, 2, \dots, n-s \quad (5)$$

其中每个 g_t 都是自由元 $x_{j_1}, \dots, x_{j_{n-r}}$ 的线性函数. 由于 $s > r$, 因此 $n-s < n-r$, 也即式子(5)中的变量个数多于线性函数的个数. 所以存在 $x_{j_1}, \dots, x_{j_{n-r}}$ 不全为零, 使得式子(5)中每一个 $y_{q_t} = 0$. 此时考虑这组 $x_{j_1}, \dots, x_{j_{n-r}}$ 非零值对应的 $Ax = 0$ 的解, 也是得到一个非零解 x . 另一方面这个解对应的 $y = B^{-1}x$ 是 $Cy = 0$ 的解. 此时这个解中对应的自由元

¹在一些教材中我们这里定义的矩阵的秩又被称为行秩, A^T 的秩被称为 A 的列秩, 即我们要证明矩阵的行秩与列秩相同.

$y_{q_1}, \dots, y_{q_{n-s}}$ 全为零, 所以 $\mathbf{y} = \mathbf{0}$. 这就导致了 $\mathbf{x} = B\mathbf{y} = \mathbf{0}$, 与 \mathbf{x} 非零解矛盾. 因此假设不成立, 即 $s \leq r$.

对于 $A = CB^{-1}$, 由于 B^{-1} 也是可逆矩阵, 同理可得 $\text{rank } A \leq \text{rank } C$, 即 $r \leq s$. 综上所述, $r = s$, 即 $\text{rank } A = \text{rank}(AB)$. \square

推论 2.3. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$ 来说, $\text{rank } A = \text{rank } A^T$.

证明. 设 $k = \text{rank } A$. 先对 A 做行变换得到 $\text{rref}(A)$, 再对其做列变换, 可以将主元列移到前 k 列并消去其余列中的主元行分量, 从而得到秩标准形

$$S = \begin{pmatrix} \mathbf{I}_k & \mathbf{O}_{k \times n-k} \\ \mathbf{O}_{m-k \times k} & \mathbf{O}_{m-k \times n-k} \end{pmatrix}$$

其中 \mathbf{O} 代表分量全为零的矩阵. 也就是说, 存在可逆矩阵 $P \in M_m(\mathbb{R})$ 和 $Q \in M_n(\mathbb{R})$ 使得 $PAQ = S$. 转置后有

$$Q^T A^T P^T = S^T.$$

由于左乘、右乘可逆矩阵不改变秩, 且 $\text{rank } S^T = k$, 得到 $\text{rank } A^T = k = \text{rank } A$. \square

从上述证明过程中, 根据可逆矩阵与行列变换的关系, 我们还能看出:

推论 2.4. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 存在可逆矩阵 $P \in M_m(\mathbb{R}), Q \in M_n(\mathbb{R})$ 使得

$$PAQ = \begin{pmatrix} \mathbf{I}_k & \mathbf{O}_{k \times n-k} \\ \mathbf{O}_{m-k \times k} & \mathbf{O}_{m-k \times n-k} \end{pmatrix}$$

其中 $k = \text{rank } A$, 这被称为 A 的**秩标准形** (也称相抵标准形, *rank normal form*).

定义 2.10. 矩阵 $A, B \in M_{m \times n}(\mathbb{R})$ 之间被称为**相抵** (*equivalent*), 如果存在可逆矩阵 $P \in M_m(\mathbb{R}), Q \in M_n(\mathbb{R})$ 使得 $PAQ = B$.

定理 2.3. $m \times n$ 阶矩阵 A, B 之间相抵当且仅当 $\text{rank } A = \text{rank } B$, 即相抵关系完全由矩阵的秩分类.

证明. 由于行列变换不改变矩阵的秩, 从而相抵矩阵有相同的秩; 另一方面, 如果 A, B 有相同的秩, 它们的相抵标准型相同, 从而相抵. \square

2.6 分块矩阵

分块矩阵是提供一种将矩阵划分为若干子矩阵的表示方法, 在矩阵的乘法, 求逆, 行列变换中有重要应用. 从已有的矩阵或者向量出发恰当的构造分块矩阵也可以提供原来矩阵或者向量的一些性质, 是研究矩阵恒等式和不变量的重要技巧. 在这一小节中, 我们将介绍分块矩阵的基本概念, 在分块矩阵下矩阵的加法, 数乘, 乘法以及求逆等运算. 然后应用一些经典的分块方法来求一些矩阵的逆, 以及得到一些矩阵秩的不等式.

分块矩阵：把大系统拆成小模块

分块矩阵的意义不仅是排版方便,更是“模块化思维”.在工程系统中,一个大型状态向量可能由位置、速度、温度、控制输入等不同部分组成;在数据科学中,一个数据矩阵可能按样本组、特征组或训练/测试部分拆分;在数值计算中,大型线性方程组常常按子区域分块求解.分块矩阵让我们在不展开所有元素的情况下讨论整体结构,是从“逐元素计算”走向“结构计算”的第一步.

给定矩阵 A , 我们可以做适当的划分, 将其看作矩阵元素是矩阵的矩阵. 例如

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

如果做以下的划分, 或者等价的, 在矩阵的表达中添加一些横线和竖线的分隔,

$$A = \left(\begin{array}{cc|c} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right),$$

我们可以将其看成 2×2 的矩阵分块 $(A_{ij})_{2 \times 2}$, 其中

$$A_{11} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad A_{12} = \begin{pmatrix} a_{13} \\ a_{23} \end{pmatrix} \quad A_{21} = \begin{pmatrix} a_{31} & a_{32} \end{pmatrix} \quad A_{22} = \begin{pmatrix} a_{33} \end{pmatrix}$$

将其写作

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}.$$

处于同一横排的子矩阵行数相同, 处于同一竖排的子矩阵列数相同. 例如上面的 A_{11}, A_{12} 均有两行, A_{21}, A_{22} 均有一行; A_{11}, A_{21} 均有两列, A_{12}, A_{22} 均有一列.

2.6.1 分块矩阵的运算

对分块矩阵做数乘等价于对每一个分块做相同的数乘. 在前面例子中, 我们有

$$cA = \begin{pmatrix} cA_{11} & cA_{12} \\ cA_{21} & cA_{22} \end{pmatrix}.$$

如果两个矩阵 $A, B \in M_{m \times n}(\mathbb{R})$ 有相同的分块方式, 即 $A = (A_{ij})_{p \times q}, B = (B_{ij})_{p \times q}$, 那么它们的加法也等于每个分块对应相加, 即 $A + B = (A_{ij} + B_{ij})_{p \times q}$.

分块矩阵的乘法与普通矩阵的乘法类似, 只不过将矩阵元素替换成了子矩阵. 通过直接计算我们可以得到:

命题 2.9. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, $B \in M_{n \times l}(\mathbb{R})$, 如果两者写成分块矩阵 $A = (A_{ij})_{p \times q}$, $B = (B_{ij})_{q \times r}$, 且 A 的列划分与 B 的行划分相同, 则其乘积 $C = AB$ 也是一个分块矩阵 $C = (C_{ij})_{p \times r}$, 其中 $C_{ij} = \sum_{k=1}^q A_{ik}B_{kj}$.

这里的行列划分相同保证了矩阵 A_{ik} 与 B_{kj} 可做矩阵乘法.

例 2.5. 对于分块矩阵

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad N = \begin{pmatrix} E & F \\ G & H \end{pmatrix}.$$

其中 A, B, C, D, E, F, G, H 都是矩阵, 且 A, C 的列数等于 E, F 的行数, B, D 的列数等于 G, H 的行数, 那么

$$MN = \begin{pmatrix} AE + BG & AF + BH \\ CE + DG & CF + DH \end{pmatrix}.$$

和对角矩阵类似, 我们也有分块对角阵的概念.

定义 2.11. 如果方阵 $A \in M_n(\mathbb{R})$ 可以写成如下形式

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$

其中 A_i 都是方阵, 则称 A 为**分块对角矩阵** (*block diagonal matrix*).

与对角矩阵类似, 如果有两个相同分块方式的分块对角矩阵 $A = (A_{ij})_{k \times k}$, $B = (B_{ij})_{k \times k}$, 那么它们的乘积也是一个分块对角矩阵, 且

$$AB = \begin{pmatrix} A_1B_1 & 0 & \cdots & 0 \\ 0 & A_2B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_kB_k \end{pmatrix}.$$

因此我们有如下关于分块对角矩阵逆的结论.

命题 2.10. 如果方阵 A 可以写成分块对角的形式

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix}$$

那么有 A 可逆当且仅当每一个 A_i 均可逆, 此时

$$A^{-1} = \begin{pmatrix} A_1^{-1} & 0 & \cdots & 0 \\ 0 & A_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k^{-1} \end{pmatrix}.$$

证明. 将 A_i 做行变换化作最简阶梯型, 同时将相同的行变换作用在 A 对应的行上, 得到的仍然是阶梯型, 所以 $\text{rank}(A) = \text{rank}(A_1) + \cdots + \text{rank}(A_k)$. 因此 A 可逆当且仅当每一个 A_i 均可逆. 另一方面, 如果每一个 A_i 均可逆, 那么

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{pmatrix} \begin{pmatrix} A_1^{-1} & 0 & \cdots & 0 \\ 0 & A_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k^{-1} \end{pmatrix} = \begin{pmatrix} I_{n_1} & 0 & \cdots & 0 \\ 0 & I_{n_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I_{n_k} \end{pmatrix} = I_n.$$

□

类似刚刚的证明过程, 我们还可以证明如下关于分块矩阵的秩的不等式:

命题 2.11. 如果矩阵 M 可以写成分块的形式

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

那么

1. 有秩不等式: $\text{rank}(M) \geq \text{rank}(A) + \text{rank}(C)$.
2. 当 $B = 0$ 时, 则有等式 $\text{rank}(M) = \text{rank}(A) + \text{rank}(C)$.
3. 当 A, C 均为方阵时, 则 M 可逆当且仅当 A, C 均可逆.

证明. 分别对 A, C 所在的行列做初等行列变换将其化为其相抵标准型, 则有

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \rightarrow \begin{pmatrix} I_{r_1} & 0 & * & * \\ 0 & 0 & * & * \\ 0 & 0 & I_{r_2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

其中 $r_1 = \text{rank}(A), r_2 = \text{rank}(C)$. 同时利用行变换消去 I_{r_2} 上方的所有非零元素, 并将其平移到第 $r_1 + 1$ 至 $r_1 + r_2$ 行. 这样的矩阵前面 $r_1 + r_2$ 行已经是阶梯型, 且主元下方都是零.

$$\begin{pmatrix} I_{r_1} & 0 & 0 & * \\ 0 & 0 & I_{r_2} & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{6}$$

后面的行可能还有一些非零行，经过行变换后可能提供更多主元，所以 $\text{rank}(M) \geq r_1 + r_2$. 当 A, C 是方阵，且均可逆时，由不等式得到 M 是满秩的，从而可逆. 当 M 可逆时，最简阶梯型中不能有零行或者零列，由上方的形式(6)可知 A, C 均可逆. \square

2.6.2 分块矩阵的行列变换

我们可以对分块矩阵进行分块行列变换，得到相对较好的形式.

例 2.6. 例如对于分块矩阵

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

其中 A, D 都是方阵. 如果 A 可逆，我们希望用列变换的形式将其下三角化. 为了记录下列变换所右乘的矩阵，我们将恒等矩阵放在下方做同样的列变换，即考虑

$$\begin{pmatrix} A & B \\ C & D \\ I & O \\ O & I \end{pmatrix}.$$

我们对上方的矩阵做列变换，将前面分块的列右乘 $-A^{-1}B$ 加到后面分块的列上，这里特别需要注意的是由于是做列变换或者列的线性组合，我们只能对某一些列组成的分块右乘矩阵.

$$\begin{pmatrix} A & B \\ C & D \\ I & O \\ O & I \end{pmatrix} \rightarrow \begin{pmatrix} A & 0 \\ C & D - CA^{-1}B \\ I & -A^{-1}B \\ O & I \end{pmatrix}.$$

因此对应的列变换矩阵为

$$\begin{pmatrix} I & -A^{-1}B \\ 0 & I \end{pmatrix}.$$

也即

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & -A^{-1}B \\ 0 & I \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & D - CA^{-1}B \end{pmatrix}$$

即通过行列变换将其下三角化.

对于 B, C, D 可逆的时候我们也可以做类似的事情. 特别地是，如果我们采取不同的变换得到相同的等式，这有时候可以给我们带来一些非平凡的结果.

例 2.7. 对于列向量 α, β ，考虑矩阵 A 的求逆：

$$A = \begin{pmatrix} I & \alpha \\ \beta^T & 1 \end{pmatrix}.$$

一方面我们做如下的行变换先消去 β^T :

$$\begin{aligned} \begin{pmatrix} \mathbf{I} & \alpha & \mathbf{I} & \mathbf{O} \\ \beta^T & 1 & \mathbf{O} & 1 \end{pmatrix} &\rightarrow \begin{pmatrix} \mathbf{I} & \alpha & \mathbf{I} & \mathbf{O} \\ 0 & 1 - \beta^T \alpha & -\beta^T & 1 \end{pmatrix} \rightarrow \begin{pmatrix} \mathbf{I} & \alpha & \mathbf{I} & \mathbf{O} \\ 0 & 1 & -\beta^T(1 - \beta^T \alpha)^{-1} & (1 - \beta^T \alpha)^{-1} \end{pmatrix} \\ &\rightarrow \begin{pmatrix} \mathbf{I} & 0 & \mathbf{I} + \alpha(1 - \beta^T \alpha)^{-1} \beta^T & -(1 - \beta^T \alpha)^{-1} \alpha \\ 0 & 1 & -(1 - \beta^T \alpha)^{-1} \beta^T & (1 - \beta^T \alpha)^{-1} \end{pmatrix} \end{aligned}$$

其中第一步之后我们由命题2.11得到, 矩阵 A 可逆当且仅当 $1 - \beta^T \alpha \neq 0$. 并且我们得到了

$$A^{-1} = \begin{pmatrix} \mathbf{I} + \alpha(1 - \beta^T \alpha)^{-1} \beta^T & -(1 - \beta^T \alpha)^{-1} \alpha \\ -(1 - \beta^T \alpha)^{-1} \beta^T & (1 - \beta^T \alpha)^{-1} \end{pmatrix}.$$

另一方面我们可以先消去 α :

$$\begin{aligned} \begin{pmatrix} \mathbf{I} & \alpha & \mathbf{I} & \mathbf{O} \\ \beta^T & 1 & \mathbf{O} & 1 \end{pmatrix} &\rightarrow \begin{pmatrix} \mathbf{I} - \alpha \beta^T & 0 & \mathbf{I} & -\alpha \\ \beta^T & 1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} \mathbf{I} & 0 & (\mathbf{I} - \alpha \beta^T)^{-1} & -(\mathbf{I} - \alpha \beta^T)^{-1} \alpha \\ \beta^T & 1 & 0 & 1 \end{pmatrix} \\ &\rightarrow \begin{pmatrix} \mathbf{I} & 0 & (\mathbf{I} - \alpha \beta^T)^{-1} & -(\mathbf{I} - \alpha \beta^T)^{-1} \alpha \\ 0 & 1 & -\beta^T (\mathbf{I} - \alpha \beta^T)^{-1} & 1 + \beta^T (\mathbf{I} - \alpha \beta^T)^{-1} \alpha \end{pmatrix} \end{aligned}$$

同样的, 也是第一步之后我们由命题2.11得到, 矩阵 A 可逆当且仅当 $\mathbf{I} - \alpha \beta^T$ 可逆. 并且有

$$A^{-1} = \begin{pmatrix} (\mathbf{I} - \alpha \beta^T)^{-1} & -(\mathbf{I} - \alpha \beta^T)^{-1} \alpha \\ -\beta^T (\mathbf{I} - \alpha \beta^T)^{-1} & 1 + \beta^T (\mathbf{I} - \alpha \beta^T)^{-1} \alpha \end{pmatrix}.$$

由于两种方法得到的结果相同, 且矩阵 A 可逆的条件等价, 因此我们有 $\mathbf{I} - \alpha \beta^T$ 可逆当且仅当 $1 - \beta^T \alpha \neq 0$, 且此时有非平凡等式

$$\begin{aligned} (\mathbf{I} - \alpha \beta^T)^{-1} &= \mathbf{I} + \alpha(1 - \beta^T \alpha)^{-1} \beta^T \\ (1 - \beta^T \alpha)^{-1} &= 1 + \beta^T (\mathbf{I} - \alpha \beta^T)^{-1} \alpha \end{aligned}$$

利用命题2.11和分块矩阵的行列变换, 我们还能得到著名的 Frobenius 秩不等式.

命题 2.12 (Frobenius 秩不等式). 对于矩阵 $A \in M_{m \times n}(\mathbb{R}), B \in M_{n \times k}(\mathbb{R}), C \in M_{k \times \ell}$, 有

$$\text{rank}(AB) + \text{rank}(BC) \leq \text{rank}(ABC) + \text{rank}(B).$$

证明. 下面每一步都是可逆的分块行变换或分块列变换, 等价于左乘或右乘可逆分块矩阵, 因此不改变矩阵的秩:

$$\begin{pmatrix} AB & 0 \\ B & BC \end{pmatrix} \rightarrow \begin{pmatrix} 0 & -ABC \\ B & BC \end{pmatrix} \rightarrow \begin{pmatrix} 0 & ABC \\ B & 0 \end{pmatrix} \rightarrow \begin{pmatrix} ABC & 0 \\ 0 & B \end{pmatrix}.$$

根据命题2.11, 我们有

$$\text{rank}(AB) + \text{rank}(BC) \leq \text{rank}(ABC) + \text{rank}(B).$$

□

例 2.8. 对于矩阵 $A \in M_n(\mathbb{R})$, 有 $A^2 = I$ 当且仅当 $\text{rank}(A + I_n) + \text{rank}(A - I_n) = n$.

证明. 注意到

$$\begin{pmatrix} I_n + A & 0 \\ 0 & I_n - A \end{pmatrix} \rightarrow \begin{pmatrix} I_n + A & I_n + A \\ 0 & I_n - A \end{pmatrix} \rightarrow \begin{pmatrix} I_n + A & 2I_n \\ 0 & I_n - A \end{pmatrix} \rightarrow \begin{pmatrix} I_n + A & 2I_n \\ \frac{1}{2}(A^2 - I_n) & 0 \end{pmatrix}$$

从而 $A^2 = I$ 当且仅当 $\text{rank}(A + I_n) + \text{rank}(A - I_n) = n$. □

注 2.5. 类似的技巧可以证明, 如果 $f(x)$ 和 $g(x)$ 是互素多项式, 则对于 $A \in M_n(\mathbb{R})$, 有 $f(A)g(A) = 0$ 当且仅当 $\text{rank}(f(A)) + \text{rank}(g(A)) = n$.

2.7 选读: 快速傅立叶变换

选学背景

快速傅立叶变换展示矩阵乘法和复数根在算法中的威力. 本小节需要复数、递归和一点算法复杂度背景, 不影响矩阵运算主线; 对计算机科学或竞赛算法感兴趣的读者可以先读直观部分, 暂时跳过严格复杂度推导.

1965 年, James W. Cooley 与 John W. Tukey 在《Mathematics of Computation》上发表了一篇仅五页的论文², 提出了一种将离散傅立叶变换的计算复杂度从 $O(n^2)$ 降至 $O(n \log n)$ 的分治算法, 即**快速傅立叶变换** (Fast Fourier Transform, FFT). 这一算法被广泛认为是 20 世纪最重要的数值算法之一.

事实上, FFT 的核心思想可以追溯到更早的年代. 1805 年, 高斯 (C. F. Gauss) 在研究小行星轨道的插值问题时, 就在未发表的手稿中记录了本质相同的算法——比 Cooley–Tukey 的论文早了整整 160 年! 但在没有电子计算机的时代, 这一发现并未引起重视. 直到 Cooley 和 Tukey 的工作出现在数字计算机蓬勃发展的背景下, FFT 才迅速改变了科学计算的面貌.

FFT 的影响是深远的. 在它诞生之前, 对一个包含 $n = 10^6$ 个采样点的信号做频谱分析需要约 10^{12} 次运算, 以当时计算机的速度需要数天乃至数周; 而 FFT 将运算量降至约 2×10^7 次, 几乎可以瞬间完成. 正是这种“从不可能到轻而易举”的飞跃, 使得 FFT 成为现代数字信号处理、图像分析、无线通信、量子计算等众多领域不可或缺的基石.

从线性代数的角度看, FFT 的本质是一种**结构化矩阵的快速乘法**: 它利用单位根的精妙代数性质, 将一个 $n \times n$ 范德蒙德矩阵与向量的乘法从 $O(n^2)$ 加速到 $O(n \log n)$. 这是“利用矩阵结构降低计算复杂度”这一核心思想的经典范例, 也是本节将其纳入线性代数教材的原因.

我们从多项式乘法这一最直观的动机出发, 来介绍 FFT 的原理.

²J. W. Cooley and J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series*, Math. Comp. **19** (1965), 297–301.

给定两个 d 次多项式

$$\begin{aligned} h_1(x) &= a_0 + a_1x + \cdots + a_dx^d \\ h_2(x) &= b_0 + b_1x + \cdots + b_dx^d \end{aligned}$$

多项式乘积为

$$h(x) = h_1(x)h_2(x) := c_0 + c_1x + \cdots + c_{2d}x^{2d},$$

其中 $c_k = \sum_{i+j=k} a_ib_j$. 如果直接计算所有 a_ib_j 并把它们累加到对应的 c_{i+j} 中, 需要 $(d+1)^2$ 次系数乘法, 即复杂度为 $O(d^2)$. 能否做得更快? 答案是肯定的——借助快速傅立叶变换 (fast Fourier transformation) 与快速傅立叶逆变换 (inverse fast Fourier transformation), 我们可以将复杂度降到 $O(d \log d)$. 其关键思想是: 与其直接操作系数, 不如先将多项式转化为“点值表示”, 在点值层面完成乘法, 再转换回系数表示.

具体来说, 注意到 $h(x)$ 是一个 $2d$ 次多项式, 其可以由在 $2d+1$ 个不同的 x 处取值决定, 即我们有如下的矩阵表达式

$$\begin{pmatrix} h(x_0) \\ h(x_1) \\ \vdots \\ h(x_{2d}) \end{pmatrix} = M \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2d} \end{pmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{2d} \\ 1 & x_1 & x_1^2 & \cdots & x_1^{2d} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{2d} & x_{2d}^2 & \cdots & x_{2d}^{2d} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2d} \end{pmatrix}$$

其中 M 被称为**范德蒙德矩阵** (Vandermonde matrix).

如果知道了 $h_1(x_i)$ 与 $h_2(x_i)$ 的这些节点值, 节点值 $h(x_i)$ 可以通过 $h(x_i) = h_1(x_i)h_2(x_i)$ 计算, 这只需要进行 $2d+1$ 次乘法运算, 其时间复杂度为 $O(d)$. 因此关键在于如何以 $O(d \log d)$ 的时间复杂度通过 $h_1(x)$ 与 $h_2(x)$ 的系数来得到节点值 $h_1(x_i), h_2(x_i)$, 以及如何以 $O(d \log d)$ 的时间复杂度通过节点值 $h(x_i)$ 来得到 $h(x)$ 的系数, 这就是快速傅立叶变换与快速傅立叶逆变换要完成的事情.

现在我们对一个一般的 $n-1$ 次多项式 $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ 来介绍快速傅立叶变换与快速傅立叶逆变换. 不失一般性的, 我们可以假设 $n = 2^s$, 因为我们总可以把一个多项式等价的看成是次数更高的多项式, 但是那些高次项的系数是零.

注意到任意给 n 个节点 x_1, \dots, x_n , 通过暴力计算得到所有的 $f(x_i)$ 需要 n^2 次乘法, 因此时间复杂度为 $O(n^2)$. 快速傅立叶变换并不选取任意 n 个节点, 而是选取 n 个**单位根**作为节点.

定义 2.12 (n 次单位根). 设 n 为正整数. 称 $\omega \in \mathbb{C}$ 为 n **次单位根**, 若 $\omega^n = 1$. 全体 n 次单位根为

$$\omega_n^k = e^{2\pi i k/n}, \quad k = 0, 1, \dots, n-1.$$

其中 $\omega_n := e^{2\pi i/n}$ 称为 n **次本原单位根**.

单位根有以下重要性质, 这些性质是快速傅立叶变换算法得以成立的代数基础:

- (1) 周期性: $\omega_n^{k+n} = \omega_n^k$;
- (2) 折半引理: $\omega_n^{2k} = \omega_{n/2}^k$ (当 n 为偶数时);
- (3) 消去引理: $\omega_n^{n/2} = e^{i\pi} = -1$, 因此 $\omega_n^{k+n/2} = -\omega_n^k$;
- (4) 求和引理: $\sum_{k=0}^{n-1} \omega_n^{jk} = \begin{cases} n, & j \equiv 0 \pmod{n}, \\ 0, & j \not\equiv 0 \pmod{n}. \end{cases}$

快速傅立叶变换的核心思想是: 利用上述性质, 按照奇偶性将 $f(x)$ 分成两部分

$$f(x) = (a_0 + a_2x^2 + \cdots + a_{n-2}x^{n-2}) + (a_1x + a_3x^3 + \cdots + a_{n-1}x^{n-1}),$$

令 $f_{\text{even}}(y) = a_0 + a_2y + a_4y^2 + \cdots + a_{n-2}y^{n/2-1}$, $f_{\text{odd}}(y) = a_1 + a_3y + a_5y^2 + \cdots + a_{n-1}y^{n/2-1}$, 则

$$f(x) = f_{\text{even}}(x^2) + x f_{\text{odd}}(x^2).$$

例 2.9. 例如 $h(x) = x^4 + 3x^3 + 2x^2 + x + 1$, 我们将其写作

$$\begin{aligned} h(x) &= (x^4 + 2x^2 + 1) + x(3x^2 + 1) \\ &= h_{\text{even}}(x^2) + x h_{\text{odd}}(x^2). \end{aligned}$$

对于任意 $0 \leq k < \frac{n}{2}$, 我们有

$$f(\omega_n^k) = f_{\text{even}}(\omega_n^{2k}) + \omega_n^k f_{\text{odd}}(\omega_n^{2k}) = f_{\text{even}}(\omega_{n/2}^k) + \omega_n^k f_{\text{odd}}(\omega_{n/2}^k)$$

以及

$$f(\omega_n^{k+n/2}) = f_{\text{even}}(\omega_n^{2k+n}) + \omega_n^{k+n/2} f_{\text{odd}}(\omega_n^{2k+n}) = f_{\text{even}}(\omega_{n/2}^k) - \omega_n^k f_{\text{odd}}(\omega_{n/2}^k).$$

上式最后一步用到了 $\omega_n^{k+n/2} = -\omega_n^k$ (因为 $\omega_n^{n/2} = e^{i\pi} = -1$) 以及 $\omega_n^{2k+n} = \omega_n^{2k}$. 因此如果我们已经知道了 $f_{\text{even}}(\omega_{n/2}^k)$ 与 $f_{\text{odd}}(\omega_{n/2}^k)$ 这些节点值, 则可以通过 $O(n)$ 的复杂度得到 $f(\omega_n^k)$ 这些节点值. 而对于 $f_{\text{even}}(x)$ 和 $f_{\text{odd}}(x)$ 来说这是规模缩小了一半的子问题, 所以我们不断向下递归分治, 当 $n = 1$ 时结束, 从而可以以 $O(n \log n)$ 的复杂度通过多项式系数得到节点值.

算法复杂度的严格推导

设对 n 个点进行快速傅立叶变换所需的运算次数为 $T(n)$. 每一步递归中, 我们将问题分成两个规模为 $n/2$ 的子问题 (分别计算 f_{even} 和 f_{odd} 在 $n/2$ 个单位根处的值), 合并时需要 $O(n)$ 次运算 (即对 $k = 0, 1, \dots, n/2 - 1$, 分别计算一次乘法 $\omega_n^k \cdot f_{\text{odd}}(\omega_{n/2}^k)$, 一次加法和一次减法). 因此有递推关系

$$T(n) = 2T(n/2) + O(n), \quad T(1) = O(1).$$

设 $n = 2^s$, 展开递推:

$$T(2^s) = 2T(2^{s-1}) + c \cdot 2^s = 2(2T(2^{s-2}) + c \cdot 2^{s-1}) + c \cdot 2^s = 4T(2^{s-2}) + 2c \cdot 2^s = \dots = 2^s T(1) + sc \cdot 2^s.$$

由此得 $T(n) = O(n) + O(n \log_2 n) = O(n \log n)$. 这便是快速傅立叶变换的时间复杂度为 $O(n \log n)$ 的严格推导.

注 2.6. 此即经典的主定理 (*Master Theorem*) 的特殊情形: 对 $T(n) = aT(n/b) + O(n^d)$, 当 $a = b^d$ 时 $T(n) = O(n^d \log n)$. 这里 $a = 2, b = 2, d = 1$, 恰好落入 $a = b^d$ 的情形.

如果我们用矩阵的语言来解释快速傅立叶变换, 这相当于以 $O(n \log n)$ 的复杂度计算了如下矩阵乘法

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \omega_n^3 & \dots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \omega_n^6 & \dots & \omega_n^{2(n-1)} \\ 1 & \omega_n^3 & \omega_n^6 & \omega_n^9 & \dots & \omega_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \omega_n^{3(n-1)} & \dots & \omega_n^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} f(1) \\ f(\omega_n) \\ f(\omega_n^2) \\ f(\omega_n^3) \\ \vdots \\ f(\omega_n^{n-1}) \end{pmatrix}$$

Python 递归实现

下面给出快速傅立叶变换的递归实现. 该实现严格按照上述数学推导, 将多项式系数按奇偶下标拆分, 递归求解后按蝶形运算合并.

```
import cmath

def fft(a):
    """
    快速傅立叶变换 (递归实现)
    输入: a = [a_0, a_1, ..., a_{n-1}], 长度 n 为 2 的幂
    输出: [f(omega^0), f(omega^1), ..., f(omega^{n-1})]
    """
    n = len(a)
    if n == 1:
        return a
    # 按奇偶下标拆分
    a_even = fft(a[0::2]) # 偶数下标系数
    a_odd = fft(a[1::2]) # 奇数下标系数
    omega_n = cmath.exp(2j * cmath.pi / n) # n 次本原单位根
```

```

omega = 1
result = [0] * n
for k in range(n // 2):
    result[k]          = a_even[k] + omega * a_odd[k]
    result[k + n // 2] = a_even[k] - omega * a_odd[k]
    omega *= omega_n
return result

def ifft(y):
    """
    快速傅立叶逆变换（递归实现）
    输入：y = [f(omega^0), ..., f(omega^{n-1})]
    输出：多项式系数 [a_0, a_1, ..., a_{n-1}]
    """
    n = len(y)
    # 取共轭后做 FFT，再除以 n
    y_conj = [v.conjugate() for v in y]
    a = fft(y_conj)
    return [v.conjugate() / n for v in a]

def poly_multiply(h1, h2):
    """
    利用 FFT 计算两个多项式的乘积
    输入：h1, h2 为多项式系数列表
    输出：乘积多项式的系数列表
    """
    # 将长度补齐为 2 的幂
    n = 1
    while n < len(h1) + len(h2) - 1:
        n *= 2
    h1 += [0] * (n - len(h1))
    h2 += [0] * (n - len(h2))
    # FFT -> 逐点相乘 -> IFFT
    y1 = fft(h1)
    y2 = fft(h2)
    y = [a * b for a, b in zip(y1, y2)]

```

return [round(v.real) for v in ifft(y)]

注 2.7. 上述递归实现的时间复杂度为 $O(n \log n)$, 空间复杂度为 $O(n \log n)$ (因递归栈深度为 $\log n$, 每层分配长度为 n 的数组). 在实际工程中, 通常采用迭代版本 (Cooley-Tukey 蝶形算法) 以避免递归开销, 并可原址计算将空间复杂度降至 $O(n)$.

如果想要通过节点值得到多项式系数, 实际上就是要计算如上矩阵的逆矩阵, 但是不难发现

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & \omega_n^2 & \omega_n^3 & \cdots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \omega_n^6 & \cdots & \omega_n^{2(n-1)} \\ 1 & \omega_n^3 & \omega_n^6 & \omega_n^9 & \cdots & \omega_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2(n-1)} & \omega_n^{3(n-1)} & \cdots & \omega_n^{(n-1)(n-1)} \end{pmatrix}$$

的逆矩阵为

$$W^{-1} = \frac{1}{n} \overline{W}.$$

证明. 只需验证 $W\overline{W} = nI_n$. 设 W 的第 (j, k) 个元素为 $W_{jk} = \omega_n^{jk}$, \overline{W} 的第 (k, l) 个元素为 $\overline{W}_{kl} = \omega_n^{-kl}$. 则

$$(W\overline{W})_{jl} = \sum_{k=0}^{n-1} \omega_n^{jk} \cdot \omega_n^{-kl} = \sum_{k=0}^{n-1} \omega_n^{(j-l)k}.$$

由上文中单位根的求和引理, 当 $j = l$ 时上式 $= n$, 当 $j \neq l$ 时上式 $= 0$. 因此 $W\overline{W} = nI_n$, 即 $W^{-1} = \frac{1}{n} \overline{W}$. \square

这意味着, 如果想要通过 $f(x)$ 的节点值得到 $f(x)$ 的系数, 只需要将这些节点值作为多项式 $g(x)$ 的系数, 然后取 $\omega_n^0, \omega_n^{-1}, \dots, \omega_n^{-(n-1)}$ 作为节点进行快速傅立叶变换, 得到的节点值 $g(\omega_n^{-i})$ 除以 n 就是 $f(x)$ 的系数.

完整的多项式乘法流程

综上, 利用快速傅立叶变换计算两个 d 次多项式 $h_1(x)$ 与 $h_2(x)$ 的乘积, 完整流程如下:

- (1) **补零:** 设 n 为大于 $2d + 1$ 的最小的 2 的幂. 将 h_1 和 h_2 的系数向量补零至长度 n .
- (2) **FFT (求值):** 分别对 h_1 和 h_2 的系数向量做快速傅立叶变换, 得到它们在 n 个单位根处的取值. 复杂度: $O(n \log n)$.
- (3) **逐点相乘:** 计算 $h(x_i) = h_1(x_i) \cdot h_2(x_i)$, $i = 0, 1, \dots, n - 1$. 复杂度: $O(n)$.
- (4) **IFFT (插值):** 对乘积的节点值做快速傅立叶逆变换, 得到 $h(x)$ 的系数. 复杂度: $O(n \log n)$.

总时间复杂度为 $O(n \log n) = O(d \log d)$, 相比于暴力计算的 $O(d^2)$ 有本质改进.

快速傅立叶变换的应用

快速傅立叶变换的意义远远超出了多项式乘法本身. 以下列举几个重要的应用方向.

1. 大整数乘法

两个 n 位整数的乘法可以归结为多项式乘法: 将整数视为以某个进制为基底的多项式, 例如整数 1234 对应多项式 $4 + 3x + 2x^2 + x^3$ (以 $x = 10$ 代入即可还原). 因此利用 FFT 可以在 $O(n \log n)$ 时间内完成大整数乘法, 远优于小学竖式算法的 $O(n^2)$ 复杂度. 这是现代高精度计算库 (如 GMP) 的核心技术之一. 进一步地, Schönhage–Strassen 算法利用数论变换 (Number Theoretic Transform, NTT)——即在有限域 $\mathbb{Z}/p\mathbb{Z}$ 上的 FFT——实现了 $O(n \log n \log \log n)$ 的大整数乘法.

2. 信号处理与频谱分析

在信号处理领域, FFT 是将时域信号转化为频域表示的标准工具. 给定时域采样信号 $(x_0, x_1, \dots, x_{n-1})$, 其离散傅立叶变换

$$X_k = \sum_{j=0}^{n-1} x_j e^{-2\pi i j k / n}, \quad k = 0, 1, \dots, n-1$$

给出了信号在各个频率分量上的振幅和相位. 如果用直接法计算, 需要 $O(n^2)$ 次运算, 而 FFT 将其降至 $O(n \log n)$. 这使得实时频谱分析成为可能, 广泛应用于音频处理、无线通信、雷达系统等.

3. 图像处理与数据压缩

二维 FFT 是图像处理的基础工具. JPEG 图像压缩标准使用的离散余弦变换 (DCT) 本质上是实数 FFT 的变体. 通过将图像从空间域变换到频率域, 可以识别并丢弃人眼不敏感的高频分量, 从而实现高效压缩. 此外, FFT 也广泛用于图像滤波 (如去除周期性噪声)、图像配准等任务.

4. 卷积计算

两个离散序列 (a_0, \dots, a_{n-1}) 与 (b_0, \dots, b_{m-1}) 的卷积定义为 $c_k = \sum_{i+j=k} a_i b_j$, 这与多项式乘法的系数计算完全一致. 因此 FFT 可以将任意卷积运算从 $O(nm)$ 加速到 $O(N \log N)$ (N 为补零后的长度). 卷积在概率论 (概率密度函数的卷积)、统计学 (滑动平均)、深度学习 (卷积神经网络) 中都有核心应用.

5. 求解偏微分方程

谱方法 (spectral method) 是求解偏微分方程的重要数值方法之一. 其核心思想是将未知函数展开为傅立叶级数, 利用 FFT 快速地在物理空间和频率空间之间转换. 例如, 对于周期性边界条件下的热方程 $u_t = u_{xx}$, 在频率空间中微分算子变为简单的乘法, 从而将偏微分方程转化为常微分方程组. FFT 使得每个时间步的计算复杂度仅为 $O(n \log n)$.

6. 数论与组合

在算法竞赛和组合数学中, FFT (特别是数论变换 NTT) 被广泛用于:

- 计算生成函数的乘积, 从而高效求解计数问题;
- 在模素数意义下进行多项式运算, 避免浮点误差;
- 快速计算 Möbius 反演等数论函数的卷积.

2.8 习题

2.8.1 练习题

习题中的矩阵均为实矩阵.

习题 2.2 (初等矩阵记录行变换). 设

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

1. 写出左乘后实现行变换 $r_2 \leftarrow r_2 - 4r_1$ 的初等矩阵 E_1 .
2. 写出左乘后交换第 1 行和第 3 行的初等矩阵 E_2 .
3. 计算 $E_2 E_1 A$, 并说明两个行变换的先后顺序.

习题 2.3 (矩阵乘法不交换的几何原因). 令

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

1. 分别描述 R 和 S 对平面图形的作用.
2. 计算 RS 与 SR .
3. 取点 $(1, 1)^T$, 分别计算 $RS(1, 1)^T$ 和 $SR(1, 1)^T$, 并解释为什么“先旋转再拉伸”和“先拉伸再旋转”不同.

习题 2.4. 计算矩阵乘法:

$$1. \begin{bmatrix} 1 & 4 & 7 & 9 \\ -3 & 3 & 8 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 5 & 6 & 7 \\ 9 & -2 & 0 \\ 11 & -1 & -3 \\ 1 & 0 & 0 \end{bmatrix};$$

$$2. \begin{bmatrix} X & 1 & 0 \\ X^2 + X & 2 & 0 \\ 0 & X & X - 1 \end{bmatrix} \begin{bmatrix} -1 & X & -X \\ 8 & -X - 2 & -2 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$3. \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix} \quad (\theta, \varphi \in \mathbb{R}).$$

$$4. \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}^6. \quad (\text{为什么?})$$

习题 2.5. 设矩阵 A, B 的行数相等. 证明: 存在矩阵 X 使得 $AX = B$ 当且仅当 $\text{rank}(A) = \text{rank}((A, B))$. (其中 (A, B) 表示将两个矩阵拼接得到的矩阵.)

习题 2.6. 设有 n 个矩阵 $A^{(1)}, \dots, A^{(n)}$ (注意, 此处上标不是乘方), 其大小未知, 但满足乘积 $P = A^{(1)}A^{(2)} \dots A^{(n)}$ 有意义. 记 $A^{(k)}$ 的第 i 行第 j 个元素为 $a_{ij}^{(k)}$, P 的第 i 行第 j 个元素为 p_{ij} . 请用 $a_{ij}^{(k)}$ 表示 p_{ij} .

提示: 答案并不复杂. $n = 2$ 时的答案为

$$p_{ij} = \sum_k a_{ik}^{(1)} a_{kj}^{(2)}.$$

习题 2.7. 设 $G = (V, E)$ 是一个图, 顶点集 $V = \{1, 2, \dots, n\}$. n 阶矩阵 A 是 G 的邻接矩阵, 即 A 的元素 a_{ij} 等于顶点 i, j 之间边的数量.

证明 A^k 的第 i 行第 j 个元素等于 i, j 之间长度为 k 的道路的数量. (所谓 i, j 之间长度为 k 的道路, 是指 V 的一列元素 $i = v_0, v_1, \dots, v_k = j$ 和 E 的一列元素 e_1, \dots, e_k , 满足 e_h 的顶点为 v_{h-1}, v_h .)

提示: 使用问题 2.6 的结果.

习题 2.8. 证明: 与所有 n 阶方阵均可交换的 n 阶方阵必为纯量方阵, 即形如 $\lambda I_n, \lambda \in \mathbb{R}$.

习题 2.9. 设 $A \in M_n(\mathbb{R})$ 是对角线元素互不相同的对角矩阵, 证明所有与 A 乘法交换的矩阵均为对角矩阵.

习题 2.10. 称 n 阶方阵 $A = (a_{ij})$ 为上三角阵 (*upper triangular matrix*), 如果对于任意 $i > j$, 有 $a_{ij} = 0$. 如果此时 A 的对角线元素均为 0, 称 A 为严格上三角阵 (*strictly upper*

triangular matrix). 类似地, 如果 A 满足对于任意 $i < j$, 有 $a_{ij} = 0$, 则称 A 为下三角阵 (lower triangular matrix); 如果此时 A 的对角线元素均为 0, 称 A 为严格下三角阵 (strictly lower triangular matrix).

验证这四类矩阵均在矩阵加法、数乘和乘法下封闭. 更进一步, 证明一个上三角阵和一个严格上三角阵的乘积是一个严格上三角阵; 一个下三角阵和一个严格下三角阵的乘积是一个严格下三角阵.

习题 2.11. 假设 A 是对角线元素两两不同的 n 阶上三角阵. 证明: 与 A 可交换的 n 阶方阵一定也是上三角的.

习题 2.12. 对任意正整数 n , 设 n 阶上三角阵 $J_n = (a_{i,j})$ 满足 $a_{i,i+1} = 1$ ($1 \leq i \leq n-1$), 其余矩阵元都等于 0. 求所有 $m \times n$ 矩阵 B , 满足 $J_m B = B J_n$.

习题 2.13. 对 $n \times n$ 矩阵 $X = (x_{ij})_{1 \leq i,j \leq n}$, 定义其“迹”为

$$\text{tr}(X) = x_{11} + x_{22} + \cdots + x_{nn}.$$

1. 设 A 是 $m \times n$ 矩阵, B 是 $n \times m$ 矩阵, 证明 $\text{tr}(AB) = \text{tr}(BA)$.
2. 证明不存在 $n \times n$ 的矩阵 A, B 使得 $AB - BA = I_n$.

习题 2.14. 考虑如下 2 阶方阵的集合 $M = \left\{ A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$.

1. 请证明 M 在矩阵的加法, 数乘和乘法下封闭.
2. 请证明 M 上的乘法满足交换律, 而且 M 中的任何非零矩阵均可逆, 且逆矩阵也在 M 中.
3. 比较 M 中的加法和乘法结构与复数 $\mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$ 的加法和乘法结构, 有何异同?

习题 2.15. 计算如下矩阵的逆矩阵:

1. $\begin{bmatrix} 1 & a & z \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix};$

2. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad - bc \neq 0;$

3. $\begin{bmatrix} 17 & 8 & 3 \\ 2 & 3 & 1 \\ 0 & 8 & 2 \end{bmatrix}$. 利用你计算的结果解方程 $\begin{bmatrix} 17 & 8 & 3 \\ 2 & 3 & 1 \\ 0 & 8 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 18 \\ 36 \\ 0 \end{bmatrix}$.

习题 2.16. 回顾第一次课里介绍的 Google 的 PageRank 算法. 对任意一个有向图 G , 其对应的线性方程组是否一定有非零解?

提示: 这个方程可以表示为 $Ax = 0$, A 是某个方阵. 考虑 A^T 以及方程 $A^T y = 0$.

习题 2.17. 证明线性方程组 $Ax = b$ 有解当且仅当 $\begin{bmatrix} A^T \\ b^T \end{bmatrix} y = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ 无解.

习题 2.18. 令 $A = (a_{ij})_{1 \leq i, j \leq n}$ 为 n 阶实矩阵. 证明若 $\forall 1 \leq i \leq n, |a_{ii}| > \sum_{j \neq i} |a_{ij}|$, 则 A 可逆.

提示: 利用 $Ax = 0$ 是否有非零解的判定法则.

习题 2.19. 证明 $n \times m$ 的实矩阵 A 的秩小于或等于 1 等价于存在 n 维列向量 α 和 m 维列向量 β 使得 $A = \alpha\beta^T$.

习题 2.20. 设 A 是一个 n 阶方阵, 证明 $A^4 = I_n$ 当且仅当 $\text{rank}(A^2 + I_n) + \text{rank}(A + I_n) + \text{rank}(A - I_n) = 2n$.

习题 2.21. 假设 A 是可逆矩阵, u, v 是列向量. 证明:

1. $A + uv^T$ 可逆当且仅当 $1 + v^T A^{-1} u \neq 0$.

2. $A + uv^T$ 可逆时有 $(A + uv^T)^{-1} = A^{-1} - \frac{A^{-1} uv^T A^{-1}}{1 + v^T A^{-1} u}$

习题 2.22. 求下述 n 阶矩阵的逆:

$$\begin{pmatrix} 1 + a_1 & 1 & \cdots & 1 \\ 1 & 1 + a_2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 + a_n \end{pmatrix}$$

(其中 $a_i \neq 0$.)

习题 2.23. 假设 $A \in M_{n \times m}(\mathbb{R}), B \in M_{m \times n}(\mathbb{R})$. 证明 $I_n + AB$ 可逆当且仅当 $I_m + BA$ 可逆. 进一步思考: 对哪些实数 λ , 总有 $\lambda I_n + AB$ 可逆等价于 $\lambda I_m + BA$ 可逆?

习题 2.24. 设

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}.$$

计算 $A + B, A - B, 2A, AB$ 和 BA .

习题 2.25. 设 A 是 2×3 矩阵, B 是 3×4 矩阵, C 是 4×2 矩阵. 判断 AB, BA, BC, ABC, CAB 是否有定义, 并写出有定义时的矩阵大小.

习题 2.26. 计算

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

习题 2.27. 求矩阵

$$A = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$$

的逆矩阵, 并用乘法验证结果。

习题 2.28. 判断下列矩阵是否可逆。若可逆, 求其逆矩阵。

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

习题 2.29. 把下列线性方程组写成矩阵方程 $Ax = b$ 的形式。

$$\begin{cases} 2x - y + z = 0, \\ x + 3y = 5. \end{cases}$$

习题 2.30. 设

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}.$$

用初等行变换求 A 的秩。

习题 2.31. 说明为什么矩阵乘法一般不满足交换律。请用一个具体的 2×2 例子验证。

2.8.2 思考题

习题 2.32 (Strassen 算法). 设 A, B 为 $2^n \times 2^n$ 矩阵, 我们想要计算乘积 $C = AB$ 。Strassen 算法的一种表述如下: 将 A, B 和 C 分割成大小相等的块矩阵

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}, \quad C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix},$$

其中 $A_{ij}, B_{ij}, C_{ij} \in M_{2^{n-1} \times 2^{n-1}}(\mathbb{R})$ 。朴素算法如下:

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} A_{11} \times B_{11} + A_{12} \times B_{21} & A_{11} \times B_{12} + A_{12} \times B_{22} \\ A_{21} \times B_{11} + A_{22} \times B_{21} & A_{21} \times B_{12} + A_{22} \times B_{22} \end{bmatrix}$$

这种构造并没有减少乘法的数量：仍然需要 8 次矩阵块的乘法来计算 C_{ij} 矩阵，这与使用标准矩阵乘法所需的乘法数量相同。Strassen 算法定义了新的值：

$$\begin{aligned} M_1 &= (A_{11} + A_{22}) \times (B_{11} + B_{22}); \\ M_2 &= (A_{21} + A_{22}) \times B_{11}; \\ M_3 &= A_{11} \times (B_{12} - B_{22}); \\ M_4 &= A_{22} \times (B_{21} - B_{11}); \\ M_5 &= (A_{11} + A_{12}) \times B_{22}; \\ M_6 &= (A_{21} - A_{11}) \times (B_{11} + B_{12}); \\ M_7 &= (A_{12} - A_{22}) \times (B_{21} + B_{22}), \end{aligned}$$

使用 7 次乘法（每个 M_k 一次）而不是 8 次。现在我们可以用 M_k 来表达 C_{ij} ：

$$\begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} M_1 + M_4 - M_5 + M_7 & M_3 + M_5 \\ M_2 + M_4 & M_1 - M_2 + M_3 + M_6 \end{bmatrix}$$

递归地这样做，比较朴素算法和 Strassen 算法需要的两个数乘法的次数。让自己相信 Strassen 算法更高效。（还有一个更快的算法，由 Coppersmith-Winograd 提出）。

习题 2.33. 设 $A = (a_{ij})_{1 \leq i, j \leq n}$ 是一个可逆方阵。 A 的一个 LDU 分解指 $A = LDU$ ，其中 L 是一个主对角线均为 1 的下三角矩阵， U 是一个主对角线均为 1 的上三角矩阵， D 是一个可逆的对角矩阵。记 $A_m = (a_{ij})_{1 \leq i, j \leq m}$ 。证明， A 存在 LDU 分解当且仅当对每个 $1 \leq m \leq n$ ， A_m 都可逆，并且当 A 存在 LDU 分解时，其 LDU 分解是唯一的。（注：这 A_m 称做 A 的顺序主子阵。请用这个结论说服自己，“大部分”实矩阵都具有 LDU 分解，思考如何来定义“大部分”。）

习题 2.34 (Bruhat 分解雏形)。令 $GL(n, \mathbb{R})$ 是域 \mathbb{R} 上的 n -阶可逆矩阵全体， B 是上三角矩阵全体。记 S_n 是每行每列有且仅有一个 1 的 n -矩阵全体。对任意 $w \in S_n$ ，定义 $GL(n, \mathbb{R})$ 的子集为

$$BwB = \{A_1 \cdot w \cdot A_2 \mid A_1 \in B, A_2 \in B\}.$$

证明 $GL(n, \mathbb{R})$ 是所有 BwB 的无交并。这是表示论和代数几何中 Bruhat 分解的矩阵版本雏形，初学时可作为思考题跳过。

习题 2.35. 称 n 阶实方阵 A 是幂零矩阵，如果 $A^k = 0$ 对某个正整数 k 成立。证明

1. 若 A 是 n 阶幂零矩阵，则 $I + A$ 可逆。
2. 假设 $I - X$ 是 n 阶幂零方阵， B 是 n 阶实方阵，且 $X^m B = B X^m$ 对某一个正整数 m 成立。请问是否一定有 $XB = BX$ 成立？如果是请证明，如果不是请给出反例。

习题 2.36. 设 A, B 是 \mathbb{R} 上的 $m \times n$ 矩阵, $\text{rank}(A) = r, \text{rank}(B) = s$, 并且 $\text{rank}(A+B) = r+s$ 证明: 存在 m 阶可逆矩阵 P 与 n 阶可逆矩阵 Q 使得

$$PAQ = \begin{pmatrix} I_r & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad PBQ = \begin{pmatrix} 0 & 0 & 0 \\ 0 & I_s & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

习题 2.37. 如下归纳地定义方阵

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, A_n = \begin{bmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{bmatrix}$$

. 求 A_n 的平方 $(A_n)^2$.

习题 2.38. 对 n 阶方阵 A , 证明以下秩等式

$$\text{rank}(A+I) + \text{rank}(A-I) = \text{rank}(A^2 - I) + n.$$

习题 2.39 (常对角同值矩阵的行列式与逆矩阵). 已知 n 阶实矩阵

$$A = \begin{pmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{pmatrix}$$

其中 a, b 均为实数, 且 $a \neq b, a + (n-1)b \neq 0$.

1. 计算 $\det(A)$.
2. 求 A^{-1} .

习题 2.40 (Sylvester 秩不等式). 设 $A \in M_{m \times n}(\mathbb{R}), B \in M_{n \times p}(\mathbb{R})$. 证明:

$$\text{rank}(A) + \text{rank}(B) - n \leq \text{rank}(AB).$$

习题 2.41 (像与核的直和分解). 设 $A \in M_n(\mathbb{R})$. 证明下列条件等价:

1. $\text{rank}(A^2) = \text{rank}(A)$;
2. $\text{im}(A) \cap \ker(A) = \{0\}$.

并且证明, 如果 A 满足上述条件, 则有

$$\mathbb{R}^n = \text{im}(A) \oplus \ker(A).$$

习题 2.42 (矩阵和的秩取到加法上界). 设 $A, B \in M_n(\mathbb{R})$. 证明

$$\text{rank}(A + B) = \text{rank}(A) + \text{rank}(B)$$

的充要条件是

$$\text{im}(A) \cap \text{im}(B) = \{0\}, \quad \text{im}(A^T) \cap \text{im}(B^T) = \{0\}.$$

习题 2.43 (秩与秩一分解). 设 $A \in M_{m \times n}(\mathbb{R})$, 且 $\text{rank}(A) = r$. 证明: r 恰好等于把 A 表示成若干个秩一矩阵之和所需项数的最小值.

习题 2.44 (Frobenius 秩不等式与取等条件). 设

$$A \in M_{m \times n}(\mathbb{F}), \quad B \in M_{n \times p}(\mathbb{F}), \quad C \in M_{p \times q}(\mathbb{F}).$$

证明:

1.

$$\text{rank}(ABC) \geq \text{rank}(AB) + \text{rank}(BC) - \text{rank}(B).$$

2. 上式取等当且仅当

$$\text{im}(BC) \cap \ker(A) = \text{im}(B) \cap \ker(A).$$

习题 2.45 (乘积秩取等条件). 设 $A \in M_{m \times n}(\mathbb{F})$, $B \in M_{n \times p}(\mathbb{F})$. 证明:

1.

$$\text{rank}(AB) = \text{rank}(B) \iff \ker(A) \cap \text{im}(B) = \{0\}.$$

2.

$$\text{rank}(AB) = \text{rank}(A) \iff \text{im}(B) + \ker(A) = \mathbb{F}^n.$$

3. 判定 Sylvester 不等式

$$\text{rank}(AB) \geq \text{rank}(A) + \text{rank}(B) - n$$

取等的充要条件。

习题 2.46 (交换矩阵的秩不等式). 假设 A, B 均为 n 阶实矩阵, 且 $AB = BA$. 证明:

$$\text{rank}(A + B) \leq \text{rank}(A) + \text{rank}(B) - \text{rank}(AB).$$

习题 2.47 (分块上三角矩阵的逆). 令 A, B, C, D, E, F 是三阶实方阵, 且

$$\begin{pmatrix} I_3 & A & C \\ 0 & I_3 & B \\ 0 & 0 & I_3 \end{pmatrix}^{-1} = \begin{pmatrix} I_3 & D & F \\ 0 & I_3 & E \\ 0 & 0 & I_3 \end{pmatrix}.$$

已知

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 0 \\ 5 & 0 & 1 \end{pmatrix},$$

且 $C = A + B - I$ 。求 $\det C$ 。

3 线性空间

在前面章节中, 我们讨论了线性方程组的解法和结构, 以及矩阵作为线性方程组系数的推广和运算规则. 线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解集所具有的加法和数乘封闭性, 以及矩阵乘法所体现的线性组合的思想, 暗示了其背后存在着更一般的数学结构. 本章我们将从具体的 \mathbb{R}^n 空间出发, 抽象出线性空间的一般定义, 并研究保持这种线性结构的映射——线性映射. 通过引入基与坐标的概念, 我们将建立起抽象线性空间与 \mathbb{R}^n , 线性映射与矩阵之间的对应关系, 从而利用矩阵工具来解决更广泛的线性问题.

值得强调的是, 向量并不一定非要理解成几何中的箭头. 一个长度为 n 的声音采样序列、一张灰度图像、一个随时间变化的温度函数都可以看成向量. 关键不在于对象外形, 而在于它们都允许做加法和数乘, 因而都存在线性组合. 线性空间的抽象正是为了把这些表面不同的问题放到同一种语言下讨论.

3.1 \mathbb{R}^n 的子空间

回忆对于齐次线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解构成的集合非空 (包含 $\mathbf{0}$), 且满足:

1. 加法封闭, 即任意 $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{R}^n$, 如果 $A\mathbf{x}_1 = \mathbf{0}$ 且 $A\mathbf{x}_2 = \mathbf{0}$, 则

$$A(\mathbf{x}_1 + \mathbf{x}_2) = A\mathbf{x}_1 + A\mathbf{x}_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

2. 数乘封闭, 即任意实数 c 与 $\mathbf{x} \in \mathbb{R}^n$, 如果 $A\mathbf{x} = \mathbf{0}$, 则

$$A(c\mathbf{x}) = cA\mathbf{x} = c\mathbf{0} = \mathbf{0}.$$

定义 3.1. 将满足这两条性质的 \mathbb{R}^n 的非空子集 W 称为 \mathbb{R}^n 的**子空间** (*subspace*).

1. 加法封闭: 对任意 $u, v \in W$, 有 $u + v \in W$.
2. 数乘封闭: 对任意 $v \in W$ 与 $c \in \mathbb{R}$, 有 $cv \in W$.

由于加法和数乘做复合我们得到的是线性组合, 所以我们可以将子空间定义为 \mathbb{R}^n 中在线性组合下封闭的非空子集.

注 3.1 (为什么子空间一定经过原点?). 初学者常常会觉得“经过原点”这一点像是人为附加的限制, 其实它恰好刻画了线性问题和非线性问题的分界. 例如满足

$$x_1 + x_2 + x_3 = 0$$

的所有向量构成 \mathbb{R}^3 的一个子空间, 因为它是齐次线性方程组的解集, 对加法和数乘都封闭. 但满足

$$x_1 + x_2 + x_3 = 100$$

的所有向量虽然在几何上也是一个平面，却不是子空间，因为它不包含零向量，也不对数乘封闭。前者对应齐次约束，后者对应平移后的几何对象。这正是线性结构与仿射结构的基本区别。

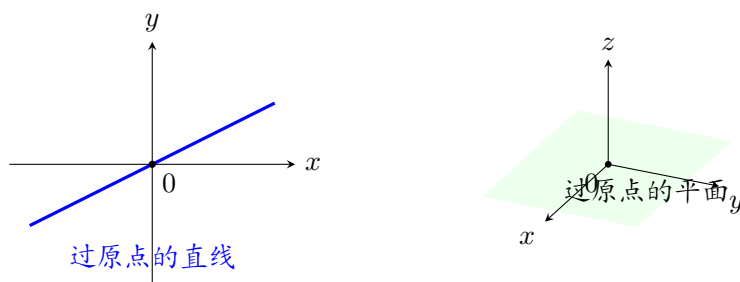
例 3.1. $\{0\}$ 是子空间³，称为零空间 (zero space)。

命题 3.1. \mathbb{R}^n 的任何一个子空间 W 均包含零空间。

证明. 任取 $w \in W$, 由于 W 对于数乘封闭, 那么 $0 = 0 \cdot w \in W$. □

注 3.2. 零空间是在包含关系下最小的子空间。

例 3.2. 我们考虑分类 \mathbb{R}^2 中的子空间。由加法和数乘的几何含义 (注记 1.1) 可知, 通过原点的直线都是 \mathbb{R}^2 的子空间。反之, 如果 W 中包含一个非零的向量, 则 W 也一定包含这条向量所在的过原点的直线。如果 W 中包含两个不共线的向量, 由图 6 可知, 这两个向量的线性组合可以表达 \mathbb{R}^2 中所有的向量。因此 \mathbb{R}^2 的子空间分为三类: 零空间, 通过原点的直线, 整个 \mathbb{R}^2 。类似的, 也可以看到 \mathbb{R}^3 中的子空间有四类: 零空间, 通过原点的直线, 通过原点的平面, 整个 \mathbb{R}^3 。



从例子中我们可以看到, 子空间是对过原点的点线面这些平直几何对象在高维空间中的推广。

3.2 零空间和线性生成

下面我们给出 \mathbb{R}^n 子空间的两种常见来源和构造方法: 矩阵的零空间和线性生成。

定义 3.2. 给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, 齐次线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解是 \mathbb{R}^n 的子空间, 被称为解空间, 也被称为 A 的核 (kernel), 记为 $\ker A$ 。有时也称为 A 的零空间 (null space)。

例 3.3. 如果 A 是 3×3 阶矩阵, 根据线性方程组解的结构定理, 即定理 1.4, 我们可以发现 $\ker A$ 在 \mathbb{R}^3 中的形式与 $\text{rank } A$ 关系密切:

- (1) $\text{rank } A = 0$, 此时 A 是零矩阵, 从而 $\ker A = \mathbb{R}^3$ 。

³这里的黑体 $\mathbf{0}$ 指代零向量, 之后可能会用 0 指实数零, 请读者注意自己仔细区分。

(2) $\text{rank } A = 1$, 此时 $\ker A$ 是通过原点的平面.

(3) $\text{rank } A = 2$, 此时 $\ker A$ 是通过原点的直线.

(4) $\text{rank } A = 3$, 此时 A 可逆, 从而 $\ker A = \{0\}$.

定义 3.3. 给定 $v_1, \dots, v_n \in \mathbb{R}^m$, 则考虑所有的线性组合

$$\text{span}_{\mathbb{R}}\{v_1, \dots, v_n\} := \{x_1v_1 + \dots + x_nv_n \mid x_i \in \mathbb{R}\}$$

称为 v_1, \dots, v_n 的**线性生成** (linear span). 由于线性组合的复合仍然是原向量的线性组合 (命题 1.2), 可以验证 $\text{span}_{\mathbb{R}}\{v_1, \dots, v_n\}$ 是子空间.

注 3.3. 更一般的, 我们也可以定义无穷多个向量的线性生成, 假设 $\{v_i \mid v_i \in \mathbb{R}^n\}_{i \in I}$ 是一族由指标集 I 为下标的列向量, 其中 $v_i \in \mathbb{R}^n$, 则定义

$$\text{span}_{\mathbb{R}}\{v_i\}_{i \in I} := \{x_{i_1}v_{i_1} + \dots + x_{i_k}v_{i_k} \mid x_{i_1}, \dots, x_{i_k} \in \mathbb{R}, k \in \mathbb{Z}_{\geq 0}, i_1, \dots, i_k \in I\}.$$

换言之, 即便指标集 I 是无限集, 我们依然只考虑每次取当中有限个向量的线性组合, 以避免无穷级数的收敛性问题.

现在来看一下线性方程组与线性生成的关系:

命题 3.2. 给定 $A = (v_1, \dots, v_n) \in M_{m \times n}(\mathbb{R})$, 那么 $Ax = b$ 有解当且仅当

$$b \in \text{span}_{\mathbb{R}}\{v_1, \dots, v_n\}.$$

这个时候也称 $\text{span}_{\mathbb{R}}\{v_1, \dots, v_n\}$ 是 A 的**列空间** (column space), 记做 $\text{im } A$. 类似的, 我们也可以定义其**行空间** (row space), 记做 $\text{im } A^T$.

以上我们介绍了两种生成 \mathbb{R}^n 的线性子空间的办法: 矩阵的核以及线性生成. 现在我们来考虑一下这两种操作之间的联系:

3.2.1 零空间写作线性生成

给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, 根据定理 1.4, 线性方程组 $Ax = 0$ 的解可以由自由元 x_{j_1}, \dots, x_{j_k} 以及主元给出, 其中 $k = n - \text{rank}(A)$, 并且在自由元确定后, 主元被唯一确定, 从而

$$\ker A = \text{span}_{\mathbb{R}}\{v_1, \dots, v_k\},$$

其中 v_s 是令自由元 $x_{j_s} = 1$ 、其余自由元为 0 后得到的解向量. 例如取例子 1.7 中的矩阵

$$A = \begin{pmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

则 $\text{rref}(A) = A$, 并且其自由元为 x_2, x_4 , 主元为 x_1, x_3, x_5 . 所有的 $A\mathbf{x} = \mathbf{0}$ 的解长成这样:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} -2x_2 - 3x_4 \\ x_2 \\ -4x_4 \\ x_4 \\ 0 \end{pmatrix} = x_2 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} -3 \\ 0 \\ -4 \\ 1 \\ 0 \end{pmatrix}.$$

因此

$$\ker A = \text{span}_{\mathbb{R}} \left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ -4 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

3.2.2 线性生成写作零空间

反之, 任取列向量 $\{v_1, \dots, v_k\} \subset \mathbb{R}^n$, 是否存在矩阵 $A \in M_{m \times n}(\mathbb{R})$ 使得 $\text{span}_{\mathbb{R}}\{v_1, \dots, v_k\} = \ker A$? 答案也是肯定的. 我们用一个具体的例子来描述一种一般的转换方法.

例 3.4. 在 \mathbb{R}^3 中考虑如下的线性生成的子空间:

$$\text{span}_{\mathbb{R}} \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\}.$$

则

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \text{span}_{\mathbb{R}} \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\}$$

当且仅当如下关于 y_1, y_2 的线性方程组

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

有解. 根据定理 1.4, 可知这等价于

$$\text{rank} \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} = \text{rank} \begin{pmatrix} 1 & 4 & x_1 \\ 2 & 5 & x_2 \\ 3 & 6 & x_3 \end{pmatrix}. \quad (7)$$

对增广矩阵做初等行变换我们可以得到

$$\begin{pmatrix} 1 & 4 & x_1 \\ 2 & 5 & x_2 \\ 3 & 6 & x_3 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 4 & x_1 \\ 0 & -3 & x_2 - 2x_1 \\ 0 & -6 & x_3 - 3x_1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 4 & x_1 \\ 0 & -3 & x_2 - 2x_1 \\ 0 & 0 & x_3 - 2x_2 + x_1 \end{pmatrix}.$$

因此可知上述的线性方程有解的条件(7)等价于 $x_3 - 2x_2 + x_1 = 0$, 即当选取矩阵 $A = (1, -2, 1)$ 时, 有

$$\text{span}_{\mathbb{R}} \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\} = \ker A.$$

以上方法说明, 对于任意列向量 $v_1, \dots, v_k \in \mathbb{R}^n$, 我们都可以构造出矩阵 $A \in M_{m \times n}(\mathbb{R})$ 使得

$$\text{span}_{\mathbb{R}} \{v_1, \dots, v_k\} = \ker A.$$

3.2.3 行列变换与零空间, 线性生成的关系

以下我们讨论行列变换与零空间和线性生成的关系. 由线性方程组的理论可知, 行变换不改变线性方程组的解集, 从而不改变矩阵的核.

命题 3.3. 行变换不改变 A 的核.

类似的列变换不改变矩阵的列空间.

命题 3.4. 列变换不改变 A 的列空间. 行变换不改变 A 的行空间.

证明. 不妨将 A 写作 $A = (v_1, \dots, v_n)$, 根据推论2.2, 做列变换等价于右乘可逆矩阵 B , 因此不妨记 A 做列变换得到的矩阵为 $AB = (\bar{v}_1, \dots, \bar{v}_n)$. 根据矩阵乘法的定义, 我们有 $\bar{v}_1, \dots, \bar{v}_n$ 都是 v_1, \dots, v_n 的线性组合, 从而

$$\text{span}_{\mathbb{R}} \{\bar{v}_1, \dots, \bar{v}_n\} \subseteq \text{span}_{\mathbb{R}} \{v_1, \dots, v_n\}$$

并且由于列变换是可逆的, 即 A 也可以由 AB 做列变换得到, 从而

$$\text{span}_{\mathbb{R}} \{v_1, \dots, v_n\} \subseteq \text{span}_{\mathbb{R}} \{\bar{v}_1, \dots, \bar{v}_n\}$$

即列变换不改变 A 的列空间. □

除此之外, 行变换一般会改变列空间, 列变换也会改变核.

3.3 仿射空间

对于非齐次线性方程组 $A\mathbf{x} = \mathbf{b}$, 如果有解, 则其解集可以表示为齐次线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解集加上一个特解 \mathbf{x}_0 :

$$\{\mathbf{x} \mid A\mathbf{x} = \mathbf{b}\} = \{\mathbf{x}_0 + \mathbf{w} \mid \mathbf{w} \in \ker A\} \text{ (也记作 } \{\mathbf{x}_0\} + \ker A \text{)}.$$

一般的, 我们把这种形式的集合称为**仿射空间** (affine space).

定义 3.4. 给定 \mathbb{R}^n 的子空间 W 以及向量 $v \in \mathbb{R}^n$, 则集合

$$v + W := \{v + w \mid w \in W\}$$

称为以 v 为**基点** (base point), W 为**方向空间** (direction space)的**仿射空间** (affine space).

例 3.5. 在 \mathbb{R}^2 中, 过点 $(1, 2)$ 且方向为 $\text{span}_{\mathbb{R}}\{(1, 1)\}$ 的仿射空间为

$$\{(1, 2) + t(1, 1) \mid t \in \mathbb{R}\} = \{(1 + t, 2 + t) \mid t \in \mathbb{R}\},$$

即过点 $(1, 2)$ 且斜率为 1 的直线.

对比子空间一定经过原点, 仿射空间则是对过任意点的点线面这些平直的几何对象在高维空间中的推广.

3.4 \mathbb{R} -线性空间

在实际应用中, 我们不仅会遇见线性方程组, 同时也会遇见微分方程. 例如对于弹簧振子问题, 假设光滑水平面上有一个弹簧, 其一端固定, 另一端连接一个质量为 m 的物体. 设物体在时间 t 时刻的位置为 $f(t)$, 弹簧自由位置定为原点.

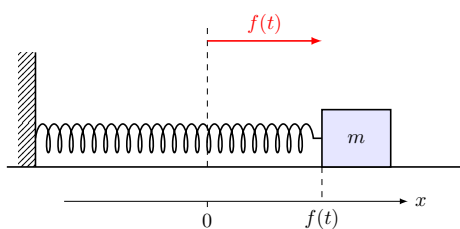


图 12: 弹簧谐振子示意图

在不受外力作用时, 牛顿第二定律和胡克定律得到物体的运动满足一维的自由弹簧方程

$$mf''(t) + kf(t) = 0,$$

其中 k 为弹簧的劲度系数. 为简便起见, 设 $m = k = 1$, 则方程化为

$$f''(t) + f(t) = 0.$$

当求解该方程时, 会发现其解的结构为

$$f(t) = x_1 \sin t + x_2 \cos t, \quad x_1, x_2 \in \mathbb{R}.$$

和有两个自由元的齐次线性方程组的解的结构类似, 都是某两个互不成倍数的解的线性组合. 但是这里的解是定义在实数集上的函数, 并不是 \mathbb{R}^n 中的向量.

假设加上随时间变化的外力 $F = \sin t$ 的弹簧方程

$$f''(t) + f(t) = \sin t$$

的解的结构为

$$f(t) = -\frac{1}{2}t \cos t + x_1 \sin t + x_2 \cos t, \quad x_1, x_2 \in \mathbb{R}.$$

这里和非齐次线性方程组的解的结构类似, 都是某一个特解加上齐次方程的解的形式.

如果我们依然想用线性空间, 子空间, 仿射空间的语言去描述其解的结构, 我们则需要引入更一般的线性空间的定义. 这样一方面我们可以利用 \mathbb{R}^n 的一些几何直觉去处理类似于微分方程组这种更一般的线性问题, 另一方面对于理解 \mathbb{R}^n 中子空间的结构, 以及同取坐标系无关的性质也有帮助.

定义 3.5. 一个 \mathbb{R} -线性空间 (\mathbb{R} -vector space) 是指一个非空集合 V 以及上面定义的加法和数乘两种运算. 其中 V 中的元素通常称为向量. 这两种运算分别是:

1. 加法: $V \times V \rightarrow V, (v_1, v_2) \mapsto v_1 + v_2$;
2. 数乘: $\mathbb{R} \times V \rightarrow V, (c, v) \mapsto cv$;

满足类似于 \mathbb{R}^n 中加法和数乘的以下性质:

- (1) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (加法交换律);
- (2) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$ (加法结合律);
- (3) 存在一个元素 $\mathbf{0}$, 使得对任意 $\mathbf{v} \in V$, 有 $\mathbf{v} + \mathbf{0} = \mathbf{v}$ (加法的单位元), 之后我们会证明满足这样性质的 $\mathbf{0}$ 是唯一的;
- (4) 对任意 $\mathbf{v} \in V$, 存在 $-\mathbf{v} \in V$, 使得 $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$ (加法的逆元), 之后我们会证明满足这样性质的 $-\mathbf{v}$ 是由 \mathbf{v} 唯一确定的;
- (5) $a(b\mathbf{v}) = (ab)\mathbf{v}$ (数乘结合律);
- (6) $1\mathbf{v} = \mathbf{v}$ (数乘的单位元);

(7) $a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$ (数乘对加法的分配律);

(8) $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ (加法对数乘的分配律).

我们有以下常用的例子:

例 3.6. \mathbb{R}^n 以及 \mathbb{R}^n 中的子空间都是 \mathbb{R} -线性空间.

例 3.7. 全体 \mathbb{R} -系数多项式 $\mathbb{R}[x]$ 构成了 \mathbb{R} -线性空间.

例 3.8. 全体次数小于等于 n 的 \mathbb{R} -系数多项式, 记做 $\mathbb{R}[x]_{\leq n}$ 构成了 \mathbb{R} -线性空间, 但次数等于 n 的 \mathbb{R} 系数多项式全体不构成 \mathbb{R} -线性空间, 因为两个次数等于 n 的多项式之和可能次数小于 n .

例 3.9. $C^\infty([a, b]) = \{f(x) \mid f(x) \text{ 是定义在 } [a, b] \text{ 上的光滑函数}\}$ 构成了 \mathbb{R} -线性空间.

例 3.10. $M_{m \times n}(\mathbb{R})$ 构成了 \mathbb{R} -线性空间, 但 n 阶可逆方阵全体 $GL_n(\mathbb{R})$ 不构成 \mathbb{R} -线性空间, 因为可逆矩阵 A 和可逆矩阵 $-A$ 之和 $A + (-A) = 0$ 不是可逆矩阵.

以下我们用这八条公理推导出一些常见的结论, 这些结论在 \mathbb{R}^n 中用直接计算容易验证, 我们这里给出在一般线性空间中的证明.

命题 3.5. 线性空间 V 中的加法零元唯一.

证明. 假设 $\mathbf{0}, \mathbf{0}'$ 都是加法的零元, 从而根据定义有

$$\mathbf{0} + \mathbf{0}' = \mathbf{0}, \quad \mathbf{0}' + \mathbf{0} = \mathbf{0}',$$

从而 $\mathbf{0} = \mathbf{0}'$. □

命题 3.6. 线性空间 V 中的任意向量 \mathbf{v} 的加法逆元由 \mathbf{v} 唯一确定.

证明. 任取 $\mathbf{v} \in V$, 如果 $\mathbf{v} + \mathbf{w}_1 = \mathbf{v} + \mathbf{w}_2 = \mathbf{0}$, 那么

$$\mathbf{w}_1 = \mathbf{w}_1 + (\mathbf{v} + \mathbf{w}_2) = (\mathbf{w}_1 + \mathbf{v}) + \mathbf{w}_2 = \mathbf{w}_2.$$

□

通过数乘零我们可以得到零向量:

命题 3.7. 线性空间中的任意向量 \mathbf{v} 均有 $0\mathbf{v} = \mathbf{0}$.

证明. 根据分配律有

$$0\mathbf{v} = (0 + 0)\mathbf{v} = 0\mathbf{v} + 0\mathbf{v}.$$

两侧同时加上 $-(0\mathbf{v})$ 则有

$$-(0\mathbf{v}) + (0\mathbf{v} + 0\mathbf{v}) = (-0\mathbf{v}) + 0\mathbf{v},$$

从而有 $0\mathbf{v} = \mathbf{0}$. □

通过数乘 $-1 \in \mathbb{R}$ 可以得到加法逆元:

命题 3.8. 线性空间中的任意向量 v 均有 $(-1)v = -v$.

证明. 根据分配律有

$$0v = (1 + (-1))v = 1v + (-1)v,$$

从而

$$0 = v + (-1)v,$$

即 $(-1)v$ 是 v 的加法逆元. □

类似于 \mathbb{R}^n 中的子空间, 我们也有子空间的概念:

定义 3.6. 令 V 是 \mathbb{R} -线性空间, 非空子集 $W \subseteq V$ 称为 V 的一个 \mathbb{R} -子空间, 如果 W 在 V 的加法和数乘运算下封闭.

以下命题说明了 W 自身也做成了一个 \mathbb{R} -线性空间.

命题 3.9. 1. V 的任意子空间 W 均包含 V 的加法零元 0 .

2. 对任意 $v \in W$, 其加法逆元 $-v$ 也在 W 中.

3. V 的任意子空间 W 在原本 V 的加法和数乘运算下均为 \mathbb{R} -线性空间.

证明. (1) 任取 $v \in W$, 由于 W 对于数乘封闭, 那么 $0 = 0 \cdot v \in W$.

(2) 对任意 $v \in W$, 由于 W 对于数乘封闭, 那么 $-v = (-1)v \in W$.

(3) 由于 $W \subseteq V$, 因此 W 中的元素继承了 V 中的加法和数乘运算. 由于 W 对于加法和数乘封闭, 且包含 V 的加法零元 0 , 和 W 中向量的加法逆元. 因此 W 在这两种运算下仍然满足线性空间的八条公理. □

例 3.11. 正如齐次线性方程组的解集构成 \mathbb{R}^n 的子空间一样, 谐振子弹簧的解集也构成了 $V = C^\infty([0, \infty))$ 的子空间. 例如对于自由弹簧方程 $f''(t) + f(t) = 0$, 假设其解集为 W , 则常数函数 $f(t) \equiv 0$ 是 W 中的元素, 所以 W 非空. 对于任意 $f_1, f_2 \in W$ 以及 $c \in \mathbb{R}$, 由于 $f_1''(t) + f_1(t) = 0$ 以及 $f_2''(t) + f_2(t) = 0$, 从而

$$\begin{aligned}(f_1 + f_2)''(t) + (f_1 + f_2)(t) &= f_1''(t) + f_2''(t) + f_1(t) + f_2(t) \\ &= (f_1''(t) + f_1(t)) + (f_2''(t) + f_2(t)) \\ &= 0 + 0 = 0,\end{aligned}$$

以及

$$\begin{aligned}(cf_1)''(t) + (cf_1)(t) &= cf_1''(t) + cf_1(t) \\ &= c(f_1''(t) + f_1(t)) \\ &= c \cdot 0 = 0.\end{aligned}$$

因此 W 是 $C^\infty([0, \infty))$ 的子空间.

由于有加法和数乘运算，我们同样的定义一组向量的线性组合以及线性生成：

定义 3.7. 给定 \mathbb{R} -线性空间 V 中的向量 v_1, \dots, v_n ，则其**线性组合 (linear combination)** 定义为

$$a_1v_1 + \dots + a_nv_n, \quad a_i \in \mathbb{R}.$$

有时候我们也称能写作这样的形式的向量为 v_1, \dots, v_n 的线性表出。

定义 3.8. 给定 \mathbb{R} -线性空间 V 中的向量 $\{v_i\}_{i \in I}$ ，其中 I 是某个指标集。则其**线性生成空间 (linear span)** 定义为

$$\text{span}_{\mathbb{R}}\{v_i\}_{i \in I} = \left\{ \sum_{i \in J} a_i v_i \mid J \subseteq I \text{ 为有限子集, } a_i \in \mathbb{R} \right\}.$$

同样的，用加法和乘法的分配律，我们可以验证一组向量的线性组合的复合仍然是原向量的线性组合，从而线性生成是子空间。

3.5 线性相关性

在上一节中，我们学习了如何用线性组合和 span 来描述子空间。一个自然的问题是：给定的一组生成元是否可以精简？换句话说，我们讨论线性组合的生成元的冗余性问题。例如在 \mathbb{R}^3 中，三个向量 v_1, v_2, v_3 是否都必须用来生成某个子空间？如果其中一个向量可以由另外两个向量线性表出，那么这个向量就是冗余的，我们可以只用另外两个向量来生成这个子空间。这里的冗余性就是线性相关性的概念。我们首先看如下的例子。

例 3.12. 令

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \quad \mathbf{v}_3 = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}.$$

注意到 $\mathbf{v}_3 = 2\mathbf{v}_2 - \mathbf{v}_1$ ，从而

$$\begin{aligned} a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3 &= a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3(2\mathbf{v}_2 - \mathbf{v}_1) \\ &= (a_1 - a_3)\mathbf{v}_1 + (a_2 + 2a_3)\mathbf{v}_2. \end{aligned}$$

即

$$\text{span}_{\mathbb{R}}\{\mathbf{v}_1, \mathbf{v}_2\} = \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\},$$

换言之，在考虑 $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ 的线性生成的时候， \mathbf{v}_3 是多余的向量。

在求解微分方程中，我们也经常碰到具体需要找到多少个解来表达出所有的解的情况。除了列向量空间，线性相关性在函数空间中同样重要，请看下面的例子。

例 3.13. 在弹簧谐振子的例子中, 由于物理规律随时间的不变性, 我们从一个解 $f_0(t) = \sin(t)$ 出发可以通过时间平移得到无穷多组解 $f_s(t) = \sin(t+s)$. 由三角函数的展开我们可以得到 $\text{span}_{\mathbb{R}}\{f_s(t) \mid s \in \mathbb{R}\} = \text{span}_{\mathbb{R}}\{\sin(t), \cos(t)\}$. 但是我们无法将 $\sin(t)$ 和 $\cos(t)$ 其中一个表达成另一个的线性组合, 所以这里由时间平移产生无穷多个解在线性组合意义下本质上应该是两个解.

注 3.4. 对于函数空间中判断线性无关性, 有一个系统的方法叫做 **Wronskian 行列式**: 对于可微函数 f_1, \dots, f_n , 定义

$$W(f_1, \dots, f_n)(t) = \det \begin{pmatrix} f_1(t) & \cdots & f_n(t) \\ f_1'(t) & \cdots & f_n'(t) \\ \vdots & \ddots & \vdots \\ f_1^{(n-1)}(t) & \cdots & f_n^{(n-1)}(t) \end{pmatrix}.$$

如果存在某个 t_0 使得 $W(f_1, \dots, f_n)(t_0) \neq 0$, 则 f_1, \dots, f_n 线性无关. 例如 $W(\sin t, \cos t) = \det \begin{pmatrix} \sin t & \cos t \\ \cos t & -\sin t \end{pmatrix} = -1 \neq 0$, 从而 $\sin t$ 和 $\cos t$ 线性无关. 我们将在后续讨论行列式时回到这个话题.

上面两个例子的共同点是: 某些向量 (或函数) 可以由其他的线性表出, 因此在生成子空间时是“多余的”. 我们用如下定义来精确刻画这种冗余性.

定义 3.9. 在线性空间 V 中, 向量 $v_1, \dots, v_n \in V$ 被称为**线性无关** (*linearly independent*), 如果 $\mathbf{0}$ 表示为 v_1, \dots, v_n 的线性组合的方式唯一, 即如果有

$$\mathbf{0} = a_1 v_1 + \cdots + a_n v_n$$

则必有 $a_1 = \cdots = a_n = 0$.

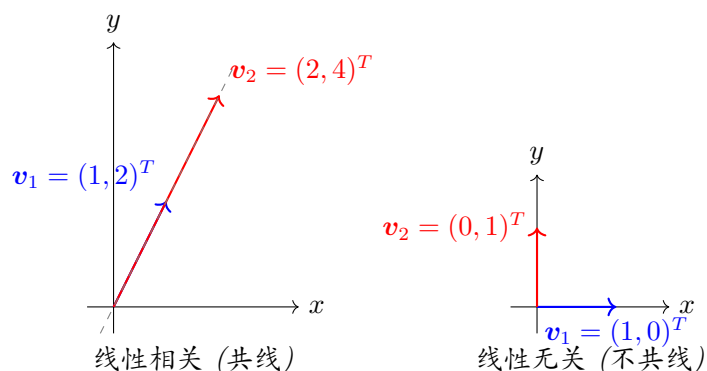
否则 v_1, \dots, v_n 被称为**线性相关** (*linearly dependent*), 或者等价的说, 存在不全为零的 $a_1, \dots, a_n \in \mathbb{R}$ 使得

$$a_1 v_1 + \cdots + a_n v_n = \mathbf{0}.$$

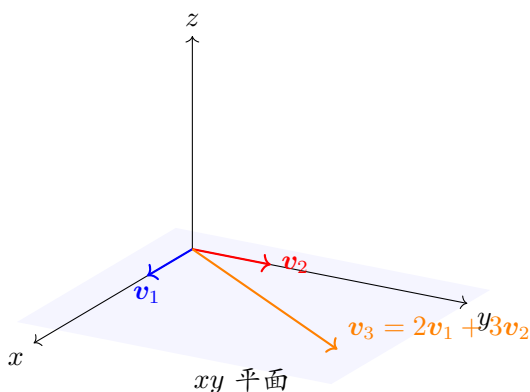
注 3.5. 给定 \mathbb{R} -线性空间 V , 对于无穷个向量 $\{v_i\}_{i \in I} \subseteq V$, 其线性无关性定义为: 任意有限和 $a_{i_1} v_{i_1} + \cdots + a_{i_n} v_{i_n} = \mathbf{0}$ 当且仅当 $a_{i_1} = \cdots = a_{i_n} = 0$, 或者等价的, 其中任意有限个向量组线性无关.

例 3.14 (几何直觉). 在行内叙述中, 我们有时将列向量 $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ 简记为 $(a_1, \dots, a_n)^T$.

1. 在 \mathbb{R}^2 中, 两个非零向量 v_1, v_2 线性相关当且仅当它们共线, 即一个是另一个的常数倍. 例如 $(1, 2)^T$ 和 $(2, 4)^T$ 线性相关, 而 $(1, 0)^T$ 和 $(0, 1)^T$ 线性无关.



2. 在 \mathbb{R}^3 中, 三个向量 v_1, v_2, v_3 线性相关当且仅当它们共面 (即三个向量的端点和原点都在同一个平面内; 这里我们假设其中任意两个不共线). 例如 $(1, 0, 0)^T, (0, 1, 0)^T, (2, 3, 0)^T$ 线性相关, 因为它们都在 xy 平面内.



例 3.15 (多项式空间). 在 $\mathbb{R}[x]_{\leq 2}$ 中, $\{1, x, x^2\}$ 线性无关 (因为 $a + bx + cx^2 = 0$ 对所有 x 成立当且仅当 $a = b = c = 0$), 但 $\{1 + x, 1 - x, 2\}$ 线性相关, 因为

$$(1 + x) + (1 - x) - 2 = 0.$$

这个例子说明线性相关性不仅适用于列向量, 也适用于一般的线性空间中的元素.

线性相关性和前面例子中向量之间线性组合的表达之间的关系如下:

命题 3.10. 实线性空间 V 中的向量 v_1, \dots, v_n 线性相关当且仅当其中至少有一个向量可以表达成其他向量的线性组合. 这里约定空线性组合等于零向量, 因此单个零向量也符合这个表述.

证明. 假设 v_1, \dots, v_n 线性相关, 则存在不全为零的 $a_1, \dots, a_n \in \mathbb{R}$ 使得

$$a_1 v_1 + \dots + a_n v_n = \mathbf{0}.$$

不妨假设 $a_n \neq 0$, 从而

$$\mathbf{v}_n = -a_n^{-1}(a_1\mathbf{v}_1 + \cdots + a_{n-1}\mathbf{v}_{n-1}),$$

即 \mathbf{v}_n 可以表达成其他向量的线性组合. 另一方面, 假设 \mathbf{v}_n 可以表达成其他向量的线性组合, 即存在 $a_1, \dots, a_{n-1} \in \mathbb{R}$ 使得

$$\mathbf{v}_n = a_1\mathbf{v}_1 + \cdots + a_{n-1}\mathbf{v}_{n-1},$$

此时

$$a_1\mathbf{v}_1 + \cdots + a_{n-1}\mathbf{v}_{n-1} + (-1)\mathbf{v}_n = \mathbf{0},$$

其中 $a_1, \dots, a_{n-1}, -1$ 不全为零, 从而 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 线性相关. □

定理 3.1. 假设线性空间 V 中的向量 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 线性无关, 则 $\mathbf{v}_1, \dots, \mathbf{v}_n, \mathbf{v}_{n+1}$ 线性相关等价于 $\mathbf{v}_{n+1} \in \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$.

证明. 如果 $\mathbf{v}_{n+1} \in \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, 则显然 $\mathbf{v}_1, \dots, \mathbf{v}_{n+1}$ 线性相关. 另一方面, 假设

$$a_1\mathbf{v}_1 + \cdots + a_{n+1}\mathbf{v}_{n+1} = \mathbf{0}$$

的系数 a_1, \dots, a_{n+1} 不全为零, 那么一定有 $a_{n+1} \neq 0$, 否则有

$$a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$$

并且 a_1, \dots, a_n 不全为零, 这与线性无关相矛盾, 从而

$$\mathbf{v}_{n+1} = -a_{n+1}^{-1}(a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n) \in \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$$

□

3.5.1 列向量空间中的线性相关性

以上关于线性相关性的讨论对一般的线性空间都成立. 当我们回到列向量空间 \mathbb{R}^m 时, 线性相关性可以通过矩阵的秩给出简洁的计算判据.

定理 3.2. 向量组 $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{R}^m$ 线性无关当且仅当 $\text{rank } A = n$, 其中 $A = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ 是 $m \times n$ 阶矩阵, 此时也称 A 是列满秩的.

证明. 注意到 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 线性无关当且仅当 $Ax = 0$ 只有零解, 根据定理1.4可知这当且仅当 $\text{rank } A = n$. □

例 3.16.

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$$

是线性无关的: 根据定义, $\{\mathbf{v}_1, \mathbf{v}_2\}$ 线性无关当且仅当

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

有唯一解 $(0, 0)$, 这等价于

$$\text{rank} \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} = 2.$$

推论 3.1. 如果 $k > m$, 线性空间 \mathbb{R}^m 中 k 个列向量一定线性相关.

证明. \mathbb{R}^m 中 k 个列向量组成的矩阵 A 的秩在 $k > m$ 时最大为 m . □

注 3.6. 上述推论告诉我们 \mathbb{R}^m 中最多只能找到 m 个线性无关的向量. 这暗示了 \mathbb{R}^m 的“大小”本质上是由 m 这个数字决定的——这正是我们下一节将要定义的“维数”概念的前兆.

推论 3.2. 列变换不改变矩阵 $A = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ 的列向量组 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 的线性相关性, 行变换不改变矩阵 A 中任意一组列向量组 $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}$ 的线性相关性.

证明. 根据定理 2.2, 列变换不改变矩阵的秩, 从而不改变所有列向量组成的向量组的线性相关性. 行变换不改变任意一组列向量组成的子矩阵的秩, 从而不改变任意列向量组的线性相关性. □

3.5.2 线性表出和极大线性无关组

以下命题说明了线性无关性保证了线性表出的唯一性.

命题 3.11. 假设 V 是一个线性空间, 若 $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$ 线性无关, 则对于 $\mathbf{v} \in \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, 其被写成 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 线性组合式子的系数是唯一的.

证明. 不妨假设

$$\begin{aligned} \mathbf{v} &= a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n \\ &= b_1 \mathbf{v}_1 + \dots + b_n \mathbf{v}_n \end{aligned}$$

则

$$0 = (a_1 - b_1) \mathbf{v}_1 + \dots + (a_n - b_n) \mathbf{v}_n$$

根据线性无关的定义可知 $a_i = b_i$ 对任意的 $1 \leq i \leq n$ 成立. □

回顾线性无关性的一个目的是为了在线性生成 $\text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ 中找到最经济的表示方式. 以下极大线性无关组的定义就可以找到这种最经济的表达.

定义 3.10. 对于线性空间 V 中的向量组 v_1, \dots, v_n , 称 v_{i_1}, \dots, v_{i_k} 是**极大线性无关组** (*maximal linearly independent set*), 如果

- (1) v_{i_1}, \dots, v_{i_k} 线性无关.
- (2) 任何包含 v_{i_1}, \dots, v_{i_k} 的 $\{v_1, \dots, v_n\}$ 的子集中的向量都线性相关.

注 3.7. 若 v_1, \dots, v_n 不全为零, 则其一定存在极大线性无关组: 假设 $v_1 \neq 0$, 考虑 v_1, v_2 是否线性相关, 如线性相关则剔除 v_2 , 线性无关则保留 v_2 . 再依次考虑 v_3, v_4, \dots 即可. 比如如下的例子中的做法.

例 3.17. 考虑 \mathbb{R}^3 中的五个向量:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad v_5 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

如果我们按照 v_1, v_2, v_3, v_4, v_5 的顺序来寻找极大线性无关组:

- $v_1 \neq 0$, 保留 v_1 .
- v_2 不能由 v_1 线性表出, 保留 v_2 . 此时极大线性无关组候选为 $\{v_1, v_2\}$.
- $v_3 = v_1 + v_2$, 可以由之前的向量线性表出, 剔除 v_3 .
- v_4 不能由 $\{v_1, v_2\}$ 线性表出, 保留 v_4 . 极大线性无关组候选为 $\{v_1, v_2, v_4\}$.
- $v_5 = v_1 + v_2 + v_4$, 可以由之前的向量线性表出, 剔除 v_5 .

最终我们得到的极大线性无关组为 $\{v_1, v_2, v_4\}$, 一共包含 3 个向量.

现在我们换一个顺序, 考虑按照逆序 v_5, v_4, v_3, v_2, v_1 的顺序来寻找:

- $v_5 \neq 0$, 保留 v_5 .
- v_4 不能由 v_5 线性表出, 保留 v_4 . 此时极大线性无关组候选为 $\{v_5, v_4\}$.
- $v_3 = v_5 - v_4$, 可以由之前的向量线性表出, 剔除 v_3 .
- v_2 不能由 $\{v_5, v_4\}$ 线性表出, 保留 v_2 . 极大线性无关组候选为 $\{v_5, v_4, v_2\}$.
- $v_1 = v_5 - v_4 - v_2$, 可以由之前的向量线性表出, 剔除 v_1 .

最终我们得到的极大线性无关组为 $\{v_5, v_4, v_2\}$. 可以看到, 虽然通过不同顺序找到的极大线性无关组中的具体向量集合不完全相同, 但它们所包含的向量个数是相同的 (都是 3 个). 我们马上会证明极大线性无关组的向量个数完全由向量组本身决定, 而与选取的顺序和具体向量无关.

实际上, 对于 \mathbb{R}^m 中的向量组, 高斯消元法提供了一种系统地寻找极大线性无关组的方法.

例 3.18 (用行化简寻找极大线性无关组). 推论 3.2 告诉我们, 对矩阵做行变换不改变任意列向量组的线性相关性, 从而我们可以通过行化简来寻找极大线性无关组. 对于上例中的五个向量, 将它们排成矩阵并做行化简:

$$A = (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{\text{行化简}} \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

该矩阵已经是行最简形, 主元所在的列是第 1, 2, 4 列. 因此 $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4\}$ 恰好构成一个极大线性无关组, 而非主元列 $\mathbf{v}_3, \mathbf{v}_5$ 可以由主元列线性表出 (从行最简形直接读出 $\mathbf{v}_3 = \mathbf{v}_1 + \mathbf{v}_2$, $\mathbf{v}_5 = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_4$). 一般地, 对矩阵做行化简后, 主元所在列对应的原始列向量总构成向量组的一个极大线性无关组.

线性无关性保证了没有冗余的向量, 而极大性则保证了生成的是相同的空间, 这便是如下的定理.

定理 3.3. 对于 $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{R}^m$, $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}$ 是其极大线性无关组, 则

$$\text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \text{span}_{\mathbb{R}}\{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}\}$$

证明. 显然 $\text{span}_{\mathbb{R}}\{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}\} \subseteq \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, 并且根据定理 3.1 以及极大线性无关组的定义可知任取 $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}$ 有

$$\mathbf{v}_i \in \text{span}_{\mathbb{R}}\{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}\}$$

从而 $\text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \text{span}_{\mathbb{R}}\{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}\}$. □

对于一组向量来说, 其极大线性无关组可能有很多, 但是任何两个极大线性无关组中向量的个数是一样的, 极大线性无关组不仅仅是包含意义下极大, 也是绝对数目的极大. 我们先证明以下结论.

定理 3.4. 假设 $V = \text{span}\{\mathbf{w}_1, \dots, \mathbf{w}_k\}$, 则 V 中的任意个数大于 k 个的向量组 $\mathbf{v}_1, \dots, \mathbf{v}_l$ 一定线性相关.

证明. 由于 $V = \text{span}\{\mathbf{w}_1, \dots, \mathbf{w}_k\}$, 从而任取 $j \in \{1, \dots, l\}$, 都有

$$\mathbf{v}_j = a_{j1}\mathbf{w}_1 + \dots + a_{jk}\mathbf{w}_k,$$

写作矩阵形式

$$(\mathbf{v}_1, \dots, \mathbf{v}_l) = (\mathbf{w}_1, \dots, \mathbf{w}_k)A,$$

其中 $A \in M_{k \times l}(\mathbb{R})$, 这里右边的乘法表达的是以 A 的每一列系数做的 $\mathbf{w}_1, \dots, \mathbf{w}_k$ 的线性组合。从而

$$x_1 \mathbf{v}_1 + \cdots + x_l \mathbf{v}_l = (\mathbf{v}_1, \dots, \mathbf{v}_l) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_l \end{pmatrix} = (\mathbf{w}_1, \dots, \mathbf{w}_k) A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_l \end{pmatrix}$$

由于 $l > k$, 从而根据线性方程组解的结构定理1.4可知 $Ax = 0$ 有非零解, 从而 $\mathbf{v}_1, \dots, \mathbf{v}_l$ 线性相关. \square

利用这个定理, 我们证明极大线性无关组的向量个数是一定的。

推论 3.3. 向量空间 V 中的任意向量组 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 中的极大线性无关组中向量的数目是确定的。

证明. 假设 $\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}$ 和 $\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_l}$ 是 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 的两组极大线性无关组, 则

$$\text{span}_{\mathbb{R}}\{\mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_k}\} = \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \text{span}_{\mathbb{R}}\{\mathbf{v}_{j_1}, \dots, \mathbf{v}_{j_l}\}$$

根据定理3.4以及这两组向量都线性无关可知 $k \leq l$ 且 $l \leq k$, 所以 $k = l$. \square

这里我们对有限组向量讨论了极大线性无关组的概念, 但是对于无穷组向量我们同样可以定义极大线性无关组, 但是在无穷的情况下, 我们无法确定注记3.7中的方法是否可以在有限步停止, 从而无法保证极大线性无关组的存在. 但是如果 V 由有限个向量线性生成, 定理3.4仍然适用, 从而在添加新的线性无关的向量时, 有限步就可以终止, 也即存在极大的线性无关组. 特别的, 我们给出线性空间 V 中任意子集的极大线性无关组的定义

定义 3.11. 对于 \mathbb{R} -线性空间 V 中的任意子集 S , 称 S 的**极大线性无关组**是指 S 的一个子集 $B \subseteq S$, 满足

- (1) B 线性无关;
- (2) 对于 S 的任意子集 $S' \subseteq S$ 满足 $B \subseteq S'$, S' 中的向量线性相关.

我们可以得到以下的结论, 如果 V 由有限个向量线性生成, 则 V 中任意子集的极大线性无关组存在, 并且任意两个极大线性无关组中向量的个数相同, 且小于 V 的生成元组的向量个数.

3.6 基与维数

上一节中, 我们看到极大线性无关组既能无冗余地生成空间, 又能唯一确定线性组合的系数, 而且其中向量的个数是确定的. 我们现在将这一概念提升为线性空间自身的内在属性

——基与维数. 粗略地说, ”基”是线性空间中最经济的生成元组, ”维数”则是基中向量的个数, 它度量了线性空间的”大小”.

从应用角度看, 选择一组基也可以理解为给同一个对象挑选一套更会说话的坐标系. 例如, 一段音乐既可以用时域采样值表示, 也可以用频域系数表示; 一张图像既可以用像素基表示, 也可以用更适合压缩的基表示. 因此基不是额外的装饰, 而是一种表达、压缩和组织信息的方式. 维数则告诉我们: 若想无损地描述这个空间中的对象, 至少需要多少个彼此独立的参数. 这一观点在后面的正交基、特征向量和奇异值分解中都会不断出现.

定义 3.12. 令 V 是一个 \mathbb{R} -线性空间, 如果 V 中的一组向量满足

(1) $\{v_i\}_{i \in I}$ 线性无关;

(2) $V = \text{span}_{\mathbb{R}}\{v_i\}_{i \in I}$,

则称 $\{v_i\}_{i \in I}$ 是 V 的一组基 (*basis*).

注 3.8. $\{v_i\}_{i \in I}$ 构成了 V 的一组基当且仅当任取 $v \in V$, v 是 $\{v_i\}_{i \in I}$ 的线性组合, 并且组合系数唯一.

定理 3.5 (基的存在性). 如果 \mathbb{R} -线性空间 V 可以由有限个向量线性生成, 则 V 存在一组 (有限的) 基. 具体地, 如果 $V = \text{span}_{\mathbb{R}}\{w_1, \dots, w_k\}$, 则 w_1, \dots, w_k 的一个极大线性无关组就是 V 的一组基.

证明. 设 w_{i_1}, \dots, w_{i_l} 是 w_1, \dots, w_k 的一个极大线性无关组. 由上一节知 $\text{span}_{\mathbb{R}}\{w_{i_1}, \dots, w_{i_l}\} = \text{span}_{\mathbb{R}}\{w_1, \dots, w_k\} = V$, 且 w_{i_1}, \dots, w_{i_l} 线性无关, 因此它们构成 V 的一组基. \square

定义 3.13. 对于 \mathbb{R} -线性空间 V , 如果 V 存在一组有限基, 则其基中向量个数被称为 V 的实维数 (*dimension*), 记做 $\dim_{\mathbb{R}} V$. 如果 V 不存在有限基, 则称 V 是无限维的.

注 3.9. 有限维 \mathbb{R} -线性空间 V 的维数是良好定义的: 因为 V 的一组基构成了一个极大线性无关组, 根据引理 3.3 可知其中向量个数是不依赖于基的选取的. 本书中凡是使用具体维数公式的地方, 默认空间是有限维的, 除非另有说明.

注 3.10 (判断基的简便方法). 根据推论 3.3 可知 V 的维数是良定义的, 并且如下三条中任意满足两条即可说明 v_1, \dots, v_k 是 V 的基:

(1) $V = \text{span}_{\mathbb{R}}\{v_1, \dots, v_k\}$.

(2) v_1, \dots, v_k 线性无关.

(3) $\dim_{\mathbb{R}} V = k$.

例如, 如果我们已经知道 $\dim_{\mathbb{R}} V = n$, 那么只需要验证 n 个向量线性无关 (或者生成 V) 就能断定它们是 V 的一组基, 而不需要两个条件都验证. 这在实际计算中非常方便.

注 3.11 (维数的意义). 维数是线性空间最重要的不变量之一. 直觉上, 所有 n 维实线性空间在结构上都与 \mathbb{R}^n ”本质相同”(即线性同构), 这也是为什么维数如此重要: 它完全分类了有限维实线性空间. 我们将在后续章节中精确地阐述这一点.

下面我们通过一系列例子来看不同线性空间中基和维数的具体表现.

例 3.19. 对 \mathbb{R} -线性空间 \mathbb{R}^n ,

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad \mathbf{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

是 \mathbb{R}^n 的一组基, 从而 $\dim_{\mathbb{R}} \mathbb{R}^n = n$.

例 3.20 (非标准基与坐标). \mathbb{R}^n 的基远不止标准基一种. 例如在 \mathbb{R}^2 中,

$$\mathbf{u}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \mathbf{u}_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

也构成 \mathbb{R}^2 的一组基 (因为它们线性无关, 且个数等于 $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$, 根据注记 3.10 即可). 同一个向量在不同基下有不同的坐标表示: 例如

$$\mathbf{v} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 3\mathbf{e}_1 + \mathbf{e}_2 = 2\mathbf{u}_1 + \mathbf{u}_2.$$

即 \mathbf{v} 在标准基 $\{\mathbf{e}_1, \mathbf{e}_2\}$ 下的坐标是 $(3, 1)^T$, 而在基 $\{\mathbf{u}_1, \mathbf{u}_2\}$ 下的坐标是 $(2, 1)^T$. 基的选取本质上就是选取一种”坐标系”, 这一观点将在后续讨论基变换时变得更加重要.

例 3.21. 对于 \mathbb{R} -线性空间 $M_{m \times n}(\mathbb{R})$, $\{E_{ij}\}$ 构成了一组基, 其中 E_{ij} 是 (i, j) 位置为 1, 其余位置为 0 的矩阵, 从而 $\dim_{\mathbb{R}} M_{m \times n}(\mathbb{R}) = mn$.

例 3.22. 对于全体次数小于等于 n 的 \mathbb{R} 系数多项式组成的 \mathbb{R} -线性空间 $\mathbb{R}[x]_{\leq n}$, $\{1, x, x^2, \dots, x^n\}$ 构成了一组基, 从而 $\dim_{\mathbb{R}} \mathbb{R}[x]_{\leq n} = n + 1$.

例 3.23. 对于一维自由弹簧方程 $f''(t) + f(t) = 0$ 的解构成的 \mathbb{R} -线性空间, $\{\sin t, \cos t\}$ 构成了一组基, 从而解空间的实维数为 2.

以上例子表明, ”维数”统一地度量了一个线性空间的”大小”, 无论它是列向量空间 (\mathbb{R}^n)、矩阵空间 ($M_{m \times n}(\mathbb{R})$)、多项式空间 ($\mathbb{R}[x]_{\leq n}$) 还是微分方程的解空间.

下面这个例子展示了同一个空间可以有完全不同的基, 而不同的基在实际问题中各有用处.

例 3.24 (部分分式分解). $V = \left\{ \frac{ax^2+bx+c}{x^3-x} \mid a, b, c \in \mathbb{R} \right\}$ 构成了一个 \mathbb{R} -线性空间, 其有如下两组不同的基:

$$B = \left\{ \frac{x^2}{x^3-x}, \frac{x}{x^3-x}, \frac{1}{x^3-x} \right\}$$

$$C = \left\{ \frac{1}{x}, \frac{1}{x-1}, \frac{1}{x+1} \right\}$$

基 B 是“自然”的: 分子分别取 $x^2, x, 1$. 基 C 则来自部分分式分解: 注意到 $x^3 - x = x(x-1)(x+1)$, 从而 V 中的每个元素都可以唯一地写成

$$\frac{ax^2+bx+c}{x^3-x} = \frac{\alpha}{x} + \frac{\beta}{x-1} + \frac{\gamma}{x+1}.$$

基 C 在计算积分 $\int \frac{ax^2+bx+c}{x^3-x} dx$ 时尤为方便, 因为每个基向量 $\frac{1}{x}, \frac{1}{x-1}, \frac{1}{x+1}$ 都可以直接积分为对数函数. 这个例子也说明“选择好的基”可以极大地简化问题——这是线性代数中一个反复出现的主题.

对于一般的 \mathbb{R} -线性空间 V , 其维数不一定有限, 比如下面的例子:

例 3.25. 对于 \mathbb{R} 系数多项式全体组成的 \mathbb{R} -线性空间 $\mathbb{R}[x], \{1, x, x^2, \dots\}$ 构成了一组基, 因此 $\dim_{\mathbb{R}} \mathbb{R}[x] = \infty$.

但是在这门课程中, 我们主要关心有限维的线性空间. 在之后, 如果不加特殊说明, 我们总假设线性空间是有限维的.

例 3.26 (子空间的维数). 考虑 \mathbb{R}^3 中过原点的平面 $W = \{(x, y, z)^T \in \mathbb{R}^3 \mid x + y + z = 0\}$. 由 $z = -x - y$ 可知

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ -x-y \end{pmatrix} = x \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}.$$

因此 $W = \text{span}_{\mathbb{R}}\{(1, 0, -1)^T, (0, 1, -1)^T\}$, 而这两个向量线性无关, 所以它们构成 W 的一组基, $\dim_{\mathbb{R}} W = 2$. 这与几何直觉一致: 过原点的平面是“二维”的.

例 3.27 (维数公式预告). 在 \mathbb{R}^3 中, 令

$$W_1 = \text{span}_{\mathbb{R}}\{(1, 0, 0)^T, (0, 1, 0)^T\}, \quad W_2 = \text{span}_{\mathbb{R}}\{(0, 1, 0)^T, (0, 0, 1)^T\}.$$

则 W_1 是 xy 平面, W_2 是 yz 平面, $W_1 \cap W_2$ 是 y 轴, $W_1 + W_2 = \mathbb{R}^3$. 注意到

$$\dim(W_1 + W_2) = 3 = 2 + 2 - 1 = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2).$$

这不是巧合——我们将在后续章节中证明一般的**维数公式**: $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$, 它是线性代数中的一个基本工具.

命题 3.12. 给定 \mathbb{R} -向量空间 W_1, W_2 , 满足 $W_1 \subseteq W_2$, 则

(1) $\dim_{\mathbb{R}} W_1 \leq \dim_{\mathbb{R}} W_2$, 并且等号成立当且仅当 $W_1 = W_2$.

(2) W_1 的基可以扩充为 W_2 的基.

证明. (1). 由于 W_1 中的线性无关组一定是 W_2 中的线性无关组, 从而 $\dim W_1 \leq \dim W_2$. 若 $W_1 = W_2$ 则等号显然成立. 反过来, 若 $\dim W_1 = \dim W_2 = k$, 取 W_1 的一组基 v_1, \dots, v_k , 则 v_1, \dots, v_k 是 W_2 中 k 个线性无关的向量, 由注记3.10知它们也是 W_2 的一组基, 从而 $W_2 = \text{span}_{\mathbb{R}}\{v_1, \dots, v_k\} = W_1$.

(2). 假设 W_1 的基是 v_1, \dots, v_k , W_2 的基是 w_1, \dots, w_l . 我们在取 $v_1, \dots, v_k, w_1, \dots, w_l$ 的极大线性无关组的时候仔细一些: 即前 k 个向量取 v_1, \dots, v_k , 这是可以做到的, 因为 v_1, \dots, v_k 本身线性无关. 这样取出的极大线性无关组就是由 v_1, \dots, v_k 扩充得到的 W_2 的基. \square

有了维数的概念, 我们可以回过头来理解第一章中矩阵的秩的几何意义: 秩正好是矩阵行空间 (或列空间) 的维数.

定理 3.6. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, $\text{rank } A$ 是行空间维数, $\text{rank } A^T$ 是列空间维数.

证明. 根据推论3.4可知行变换不改变行空间, 因此我们通过行变换将其化作最简行阶梯型, 此时主元所在的行向量构成了行空间的一组基, 因此 $\text{rank } A$ 是行空间维数. 类似的可以证明 $\text{rank } A^T$ 是列空间维数. \square

推论 3.4. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, $\dim_{\mathbb{R}} \text{im } A = \text{rank } A$.

证明. 根据推论2.3即可. \square

在第一章中, 我们将矩阵 $A \in M_{m \times n}(\mathbb{R})$ 的零度 $\text{null}(A)$ 定义为 $\text{rref}(A)$ 中自由元的个数, 即 $\text{null}(A) = n - \text{rank } A$. 现在有了维数的工具, 我们可以揭示零度的内在含义: 它正是核 (零空间) 的维数.

定理 3.7. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 有

$$\text{null}(A) = \dim_{\mathbb{R}} \ker A.$$

即 A 的零度等于 $\ker A$ 的维数.

证明. 将 A 通过行变换化为最简行阶梯型 $\text{rref}(A)$. 行变换不改变核 (推论3.3), 因此 $\ker A = \ker \text{rref}(A)$. 设 $\text{rank } A = r$, 则 $\text{rref}(A)$ 有 r 个主元列和 $n - r$ 个自由列. 根据定理1.4, 令每个自由元 x_{i_j} 分别取 1、其余自由元取 0, 主元由回代唯一确定, 由此得到 $n - r$ 个解向量 v_1, \dots, v_{n-r} .

生成性: 对于 $\ker A$ 中任一向量 \mathbf{x} , 其自由元分量为 $(x_{i_1}, \dots, x_{i_{n-r}})$, 由回代可知 $\mathbf{x} = x_{i_1}\mathbf{v}_1 + \dots + x_{i_{n-r}}\mathbf{v}_{n-r}$, 因此 $\ker A = \text{span}_{\mathbb{R}}\{\mathbf{v}_1, \dots, \mathbf{v}_{n-r}\}$.

线性无关性: 若 $c_1\mathbf{v}_1 + \dots + c_{n-r}\mathbf{v}_{n-r} = \mathbf{0}$, 注意到 \mathbf{v}_j 的第 i_j 个分量为 1 而 $\mathbf{v}_k (k \neq j)$ 的第 i_j 个分量为 0, 因此 $c_j = 0$ 对所有 j 成立.

综上 $\mathbf{v}_1, \dots, \mathbf{v}_{n-r}$ 构成 $\ker A$ 的一组基, 从而 $\dim_{\mathbb{R}} \ker A = n - r = \text{null}(A)$. \square

推论 3.5. 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, $\dim_{\mathbb{R}} \ker A = n - \text{rank } A$.

将推论 3.4 ($\dim_{\mathbb{R}} \text{im } A = \text{rank } A$) 和推论 3.5 ($\dim_{\mathbb{R}} \ker A = n - \text{rank } A$) 合并, 便得到线性代数中最基本的等式之一:

定理 3.8 (秩-零度定理 (rank-nullity theorem)). 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 有

$$\dim_{\mathbb{R}} \ker A + \dim_{\mathbb{R}} \text{im } A = n,$$

即 $\text{null}(A) + \text{rank } A = n$. 换言之, 核的维数与像 (列空间) 的维数之和等于 A 的列数.

注 3.12. 秩-零度定理的直观含义是: 矩阵 $A: \mathbb{R}^n \rightarrow \mathbb{R}^m$ 将 n 维空间”分成”两部分——被映到零的部分 (核, 维数为 $n - r$) 和有效输出的部分 (像, 维数为 r), 二者的维数恰好加起来等于定义域 \mathbb{R}^n 的维数 n . 在后续讨论一般线性映射时, 这一等式将推广为更一般的形式.

例 3.28. 设 $A = \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in M_{3 \times 4}(\mathbb{R})$, 则 $\text{rank } A = 2$, $\text{null}(A) = 4 - 2 = 2$. 由上述定理,

$$\dim_{\mathbb{R}} \text{im } A = 2, \quad \dim_{\mathbb{R}} \ker A = 2.$$

这意味着 A 的列空间是 \mathbb{R}^3 中的一个 2 维子空间 (即过原点的平面), 而 A 的核是 \mathbb{R}^4 中的一个 2 维子空间.

推论 3.6. 给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, $B \in M_{n \times \ell}(\mathbb{R})$, 则

$$\text{rank}(AB) \leq \text{rank}(A).$$

证明. 只需要注意到 $\text{im } AB \subseteq \text{im } A$. \square

3.7 向量的坐标表达

在上一节中我们看到, 给定线性空间 V 的一组基 B , V 中每个向量都可以**唯一地**表示为基向量的线性组合. 这意味着我们可以用这组系数来”代表”该向量——这就是坐标的概念. 通过坐标, 我们把抽象线性空间中的问题翻译成 \mathbb{R}^n 中列向量的计算, 这正是基的核心用途之一. 我们已经在非标准基与坐标的例子中初步见到了这一思想, 现在给出正式的定义.

定义 3.14. 令 V 是 \mathbb{R} -线性空间, $B = \{v_1, \dots, v_n\}$ 是其一组基, 则对于 $v \in V$, 有唯一的表达

$$v = a_1 v_1 + \dots + a_n v_n$$

其中 $a_i \in \mathbb{R}$. 列向量

$$[v]_B = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n$$

被称为 v 在基 B 下的**坐标** (*coordinate*).

注 3.13. 对于 \mathbb{R} -线性空间 V , $v \in V$ 在不同基下的坐标往往有不同的优势: 在例 3.24 中, 考虑

$$v = \frac{3x^2 + x + 2}{x^3 - x}.$$

我们可以很轻易地写出其在 B 下的坐标 (只需读出分子的系数)

$$[v]_B = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}.$$

然而很难直接写出 $[v]_C$, 因为这需要做部分分式分解. 另一方面, 基 C 便于积分, 因此如果我们有 $[v]_C$, 则可以很轻易地将 v 的积分写出来. 因此搞清楚同一个向量在不同基下坐标的变换关系是非常有意义的问题——这便是转移矩阵的动机.

一个自然的问题是: 如果已知向量 v 在基 B 下的坐标 $[v]_B$, 如何求 v 在另一组基 C 下的坐标 $[v]_C$? 为此我们引入转移矩阵的概念.

对于 \mathbb{R} -线性空间 V , 给定其一组基 $B = \{v_1, \dots, v_n\}$, 为简化符号, 我们有时也将基 B 视作矩阵 $B = (v_1, \dots, v_n)$ ⁴, 此时坐标的定义可以简洁地写为

$$v = B[v]_B.$$

现在对于另一组基 $C = \{w_1, \dots, w_n\}$, 将 C 的每个基向量用 B 的基向量表示: 对任取 $1 \leq i \leq n$, 有

$$w_i = p_{1i} v_1 + \dots + p_{ni} v_n.$$

定义 3.15. 上述矩阵 $P_{B \leftarrow C} = (p_{ij})_{n \times n}$ 被称为从基 C 到基 B 的**转移矩阵** (*transition matrix*). 用矩阵记号, 即

$$C = B P_{B \leftarrow C}.$$

⁴严格来说, 当 $V \neq \mathbb{R}^m$ 时, 这里的“矩阵”只是一种形式记号, 其含义是: $B\mathbf{x}$ 表示以 \mathbf{x} 的分量为系数对基向量做线性组合.

我们先通过一个 \mathbb{R}^2 中的简单例子来熟悉转移矩阵的计算.

例 3.29. 取 \mathbb{R}^2 的标准基 $B = \{e_1, e_2\}$ 和基 $C = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$. 由于

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 \cdot e_1 + 1 \cdot e_2, \quad \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot e_1 + (-1) \cdot e_2,$$

转移矩阵为

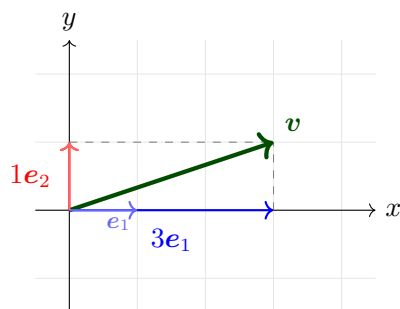
$$P_{B \leftarrow C} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

对于 $v = (3, 1)^T$, 我们有 $[v]_B = (3, 1)^T$ (在标准基下坐标就是自身), 从而

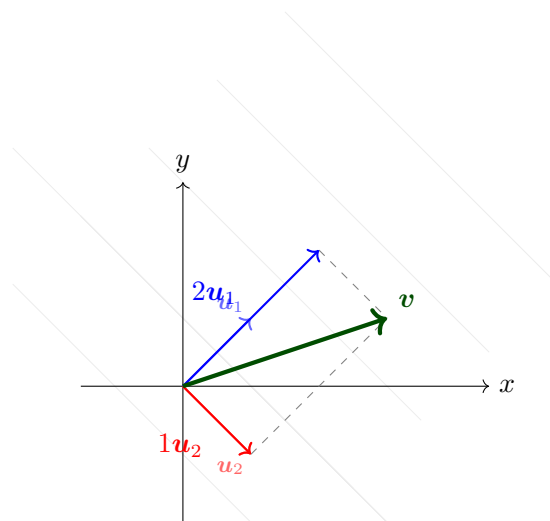
$$[v]_C = P_{B \leftarrow C}^{-1} [v]_B = P_{C \leftarrow B} [v]_B = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

验证: $2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$. \checkmark 这与我们之前在非标准基的例子中得到的结果一致.

下面的图展示了同一个向量 $v = (3, 1)^T$ 在两组基下的平行四边形分解:



基 B 下: $[v]_B = (3, 1)^T$



基 C 下: $[v]_C = (2, 1)^T$

左图中, v 沿标准基方向分解为 $v = 3e_1 + 1e_2$, 对应平行四边形的两条边分别平行于 x 轴和 y 轴. 右图中, 同一个 v 沿基 $C = \{u_1, u_2\}$ 的方向分解为 $v = 2u_1 + 1u_2$, 对应平行四

边形的两条边分别平行于 $\mathbf{u}_1 = (1, 1)^T$ 和 $\mathbf{u}_2 = (1, -1)^T$ 的方向. 向量本身没有变化, 改变的只是“分解方式”——这正是坐标变换的几何含义.

命题 3.13. 对于转移矩阵, 我们有如下性质.

$$(1) [v]_B = P_{B \leftarrow C} [v]_C.$$

$$(2) P_{B_1 \leftarrow B_3} = P_{B_1 \leftarrow B_2} P_{B_2 \leftarrow B_3}.$$

$$(3) P_{B \leftarrow B} = I_n.$$

$$(4) P_{B \leftarrow C} \text{ 是可逆矩阵, 并且 } P_{B \leftarrow C}^{-1} = P_{C \leftarrow B}.$$

证明. (1). 由 $v = C[v]_C = B P_{B \leftarrow C} [v]_C$ 以及 $v = B[v]_B$, 根据坐标的唯一性即得 $[v]_B = P_{B \leftarrow C} [v]_C$.

(4). 由 (2) 和 (3) 可知 $P_{B \leftarrow C} P_{C \leftarrow B} = P_{B \leftarrow B} = I_n$, 从而 $P_{B \leftarrow C}$ 可逆且逆为 $P_{C \leftarrow B}$.

(2) 和 (3) 的证明类似, 留做练习. \square

注 3.14. 由性质 (1) 可知, 如果已知 $[v]_C$, 只需左乘转移矩阵 $P_{B \leftarrow C}$ 即可得到 $[v]_B$. 反过来, 由性质 (4) 可知 $[v]_C = P_{C \leftarrow B} [v]_B = P_{B \leftarrow C}^{-1} [v]_B$.

下面回到部分分式分解的例子来演示更复杂的转移矩阵计算.

例 3.30. 在例 3.24 中,

$$B = \left\{ \frac{x^2}{x^3 - x}, \frac{x}{x^3 - x}, \frac{1}{x^3 - x} \right\}, \quad C = \left\{ \frac{1}{x}, \frac{1}{x-1}, \frac{1}{x+1} \right\}.$$

将 C 的每个基向量用 B 的基向量表示. 注意到 $x^3 - x = x(x-1)(x+1)$, 从而

$$\begin{aligned} \frac{1}{x} &= \frac{x^2 - 1}{x^3 - x} = 1 \cdot \frac{x^2}{x^3 - x} + 0 \cdot \frac{x}{x^3 - x} + (-1) \cdot \frac{1}{x^3 - x}, \\ \frac{1}{x-1} &= \frac{x^2 + x}{x^3 - x} = 1 \cdot \frac{x^2}{x^3 - x} + 1 \cdot \frac{x}{x^3 - x} + 0 \cdot \frac{1}{x^3 - x}, \\ \frac{1}{x+1} &= \frac{x^2 - x}{x^3 - x} = 1 \cdot \frac{x^2}{x^3 - x} + (-1) \cdot \frac{x}{x^3 - x} + 0 \cdot \frac{1}{x^3 - x}. \end{aligned}$$

因此转移矩阵为

$$P_{B \leftarrow C} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -1 & 0 & 0 \end{pmatrix}.$$

其逆矩阵为

$$P_{C \leftarrow B} = P_{B \leftarrow C}^{-1} = \frac{1}{2} \begin{pmatrix} 0 & 0 & -2 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}.$$

对于 $v = \frac{3x^2+x+2}{x^3-x}$, 其在基 B 下的坐标为 $[v]_B = (3, 1, 2)^T$, 从而

$$[v]_C = P_{C \leftarrow B}[v]_B = \frac{1}{2} \begin{pmatrix} 0 & 0 & -2 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 3 \\ 2 \end{pmatrix}.$$

即 $\frac{3x^2+x+2}{x^3-x} = \frac{-2}{x} + \frac{3}{x-1} + \frac{2}{x+1}$, 读者可以自行验证. 有了这个坐标, 积分变得直接了:

$$\int \frac{3x^2+x+2}{x^3-x} dx = -2 \ln|x| + 3 \ln|x-1| + 2 \ln|x+1| + C.$$

3.8 线性空间的构造, 和, 交

有了基和维数的工具之后, 我们自然希望从已有的线性空间出发构造新的线性空间, 并用维数来度量它们的“大小”. 本节讨论三种基本构造: 子空间的交与和、直和、以及商空间.

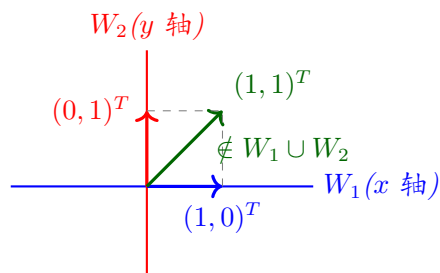
3.8.1 子空间的和与交

给定线性空间 V 的两个子空间 W_1, W_2 , 从集合论的角度, 我们自然会考虑它们的交 $W_1 \cap W_2$ 和并 $W_1 \cup W_2$. 然而, 两个子空间的并通常不再是子空间:

例 3.31. 在 \mathbb{R}^2 中, 令 W_1 为 x 轴, W_2 为 y 轴. 向量 $(1, 0)^T \in W_1$, $(0, 1)^T \in W_2$, 但它们的和

$$(1, 0)^T + (0, 1)^T = (1, 1)^T \notin W_1 \cup W_2,$$

因此 $W_1 \cup W_2$ 对加法不封闭, 从而不是子空间.



为了得到包含 W_1 和 W_2 的“最小”子空间, 我们需要用**和**来代替并. 具体来说, 给定 \mathbb{R} -线性空间 V 以及 \mathbb{R} -线性子空间 W_1, W_2 , 我们有以下两种得到新的子空间的方法:

- (1) $W_1 \cap W_2$ 是 V 的 \mathbb{R} -线性子空间, 称为 W_1 与 W_2 的**交** (intersection). 这可以直接验证: 若 $v_1, v_2 \in W_1 \cap W_2$, 则 v_1, v_2 同时属于 W_1 和 W_2 , 从而 $v_1 + v_2$ 和 cv_1 也同时属于 W_1 和 W_2 .

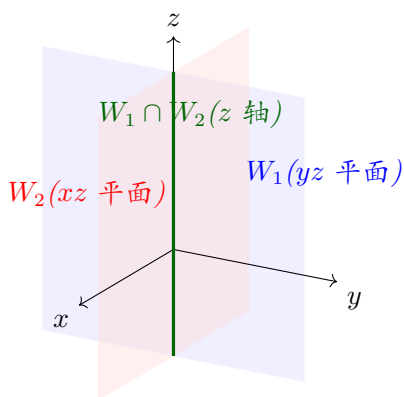
(2)

$$W_1 + W_2 := \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$$

是 V 的 \mathbb{R} -线性子空间, 称为 W_1 与 W_2 的**和** (sum). 容易验证 $W_1 + W_2 = \text{span}(W_1 \cup W_2)$, 即 $W_1 + W_2$ 是包含 W_1 和 W_2 的最小子空间.

例 3.32. 考虑 \mathbb{R}^3 中的子空间 $W_1 = \{(x_1, x_2, x_3)^T \mid x_1 = 0\}$ (即 yz 平面) 和 $W_2 = \{(x_1, x_2, x_3)^T \mid x_2 = 0\}$ (即 xz 平面), 则

$$W_1 + W_2 = \mathbb{R}^3, \quad W_1 \cap W_2 = \{(x_1, x_2, x_3)^T \mid x_1 = x_2 = 0\} \quad (\text{即 } z \text{ 轴}).$$



定理 3.9 (维数公式). 给定 \mathbb{R} -线性空间 V 以及 \mathbb{R} -线性子空间 W_1, W_2 . 假设 $\dim W_i < \infty$, 则

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2.$$

证明. 假设 $W_1 \cap W_2$ 有一组基 v_1, \dots, v_k , 并且 v_1, \dots, v_k 添加 u_1, \dots, u_n 扩充成 W_1 的一组基, 添加 w_1, \dots, w_m 扩充成 W_2 的一组基, 则我们断言

$$v_1, \dots, v_k, u_1, \dots, u_n, w_1, \dots, w_m$$

构成了 $W_1 + W_2$ 的一组基.

首先根据 $W_1 + W_2$ 的定义不难发现 $W_1 + W_2$ 可以由 $v_1, \dots, v_k, u_1, \dots, u_n, w_1, \dots, w_m$ 生成, 因此只需要证明其线性无关性. 假设

$$a_1 v_1 + \dots + a_k v_k + b_1 u_1 + \dots + b_n u_n + c_1 w_1 + \dots + c_m w_m = 0.$$

令

$$r_1 = a_1 v_1 + \dots + a_k v_k + b_1 u_1 + \dots + b_n u_n \in W_1$$

$$r_2 = c_1 w_1 + \dots + c_m w_m \in W_2,$$

从而有 $r_1 = -r_2$. 由于 $r_1 \in W_1$ 且 $-r_2 \in W_2$, 有 $r_1 \in W_1 \cap W_2$, 不妨记

$$r_1 = d_1 v_1 + \dots + d_k v_k,$$

则

$$(a_1 - d_1)v_1 + \cdots + (a_k - d_k)v_k + b_1u_1 + \cdots + b_nu_n = 0.$$

根据 $v_1, \dots, v_k, u_1, \dots, u_n$ 的线性无关性有 $b_1 = \cdots = b_n = 0$, 从而有

$$a_1v_1 + \cdots + a_kv_k + c_1w_1 + \cdots + c_mw_m = 0,$$

再利用 $v_1, \dots, v_k, w_1, \dots, w_m$ 的线性无关性有 $a_1 = \cdots = a_k = c_1 = \cdots = c_m = 0$. \square

例 3.33. 在 \mathbb{R}^4 中, 令

$$W_1 = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\}, \quad W_2 = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right\}.$$

显然 $\dim W_1 = \dim W_2 = 2$. 为了求 $W_1 \cap W_2$, 设 $v \in W_1 \cap W_2$, 则

$$v = a \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = c \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

即 $a = c, b = c, a = d, b = d$, 解得 $a = b = c = d$, 从而 $W_1 \cap W_2 = \text{span}\{(1, 1, 1, 1)^T\}$, $\dim(W_1 \cap W_2) = 1$. 由维数公式,

$$\dim(W_1 + W_2) = 2 + 2 - 1 = 3.$$

注 3.15. 给定 \mathbb{R} -线性空间 V 以及 \mathbb{R} -线性子空间 W_1, W_2, W_3 , 以下公式不成立:

$$\dim(W_1 + W_2 + W_3) = \sum_{i=1}^3 \dim W_i - \dim W_1 \cap W_2 - \dim W_1 \cap W_3 - \dim W_2 \cap W_3 + \dim W_1 \cap W_2 \cap W_3.$$

另一方面, 如下等式一般也不成立

$$(W_1 + W_2) \cap W_3 = W_1 \cap W_3 + W_2 \cap W_3.$$

考虑 \mathbb{R}^2 中 $W_1 = \text{span}\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$, $W_2 = \text{span}\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$, $W_3 = \text{span}\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\}$, 则以上两条均不满足.

3.8.2 直和

在子空间的和 $V = W_1 + W_2$ 中, 一个向量 $v \in V$ 的分解 $v = w_1 + w_2 (w_i \in W_i)$ 一般不唯一. 当 $W_1 \cap W_2 = \{0\}$ 时, 这种分解是唯一的, 此时 $W_1 + W_2$ 具有特别好的结构——这便是直和的概念. 我们先从外部构造的角度定义直和, 再给出内部判据.

定义 3.16. 给定 \mathbb{R} -线性空间 V, W , 定义线性空间的**外直和** (*external direct sum*)为集合 $V \times W$, 其上带有结构

$$(1) (v_1, w_1) + (v_2, w_2) := (v_1 + v_2, w_1 + w_2), \text{ 其中 } v_1, v_2 \in V, w_1, w_2 \in W.$$

$$(2) c(v, w) := (cv, cw), \text{ 其中 } v \in V, w \in W, c \in \mathbb{R}.$$

使得其成为一个 \mathbb{R} -线性空间, 记做 $V \oplus W$. 其零向量为 $(0_V, 0_W)$, 维数为 $\dim V + \dim W$.

例 3.34. \mathbb{R}^n 可以视作 n 个 \mathbb{R} 的外直和.

定义 3.17. 给定 \mathbb{R} -线性空间 V 及其子空间 V_1, V_2 , 如果

$$(1) V = V_1 + V_2, \text{ 即任何 } V \text{ 中的向量可以表示成 } V_1, V_2 \text{ 中向量的组合.}$$

$$(2) V_1 \cap V_2 = \{0\}.$$

则称 V 是 V_1 和 V_2 的**内直和** (*internal direct sum*).

注 3.16. $V = V_1 \oplus V_2$ (内直和) 的一个等价刻画是: 任意 $v \in V$ 可以**唯一地**写成 $v = v_1 + v_2$, 其中 $v_i \in V_i$. 事实上, 条件 (1) 保证了分解的存在性, 而条件 (2) 保证了唯一性: 若 $v = v_1 + v_2 = v'_1 + v'_2$, 则 $v_1 - v'_1 = v'_2 - v_2 \in V_1 \cap V_2 = \{0\}$, 从而 $v_1 = v'_1, v_2 = v'_2$.

命题 3.14. 给定 \mathbb{R} -线性空间 V 及其子空间 V_1, V_2 , 如果 V 是 V_1 和 V_2 的内直和, 那么

$$\begin{aligned} T: V_1 \oplus V_2 &\rightarrow V_1 + V_2 \\ (v_1, v_2) &\mapsto v_1 + v_2 \end{aligned}$$

是线性同构, 即 $V \cong V_1 \oplus V_2$.

证明. 线性映射 T 显然是满射, 并且根据内直和的定义有 $\ker T = V_1 \cap V_2 = \{0\}$. □

注 3.17. 这意味着内直和与外直和是一体两面, 因此我们之后并不再区分内外直和, 而统称为直和.

例 3.35 (直和的几何例子). 在 \mathbb{R}^3 中, 令 W_1 为 xy 平面, W_2 为 z 轴, 则 $\mathbb{R}^3 = W_1 \oplus W_2$: 任何向量 $(a, b, c)^T$ 可以唯一分解为

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \underbrace{\begin{pmatrix} a \\ b \\ 0 \end{pmatrix}}_{\in W_1} + \underbrace{\begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix}}_{\in W_2}.$$

这种分解的唯一性来源于 $W_1 \cap W_2 = \{0\}$.

定义 3.18. 给定 \mathbb{R} -线性空间 V 以及子空间 V_1 , 如果存在子空间 V_2 满足 $V = V_1 \oplus V_2$, 则称 V_2 是 V_1 的补空间 (complement space).

注 3.18. 根据命题 3.12, 我们总可以将子空间的一组基延拓成全空间的一组基, 因此补空间总是存在的. 但是补空间不唯一: 例如在 \mathbb{R}^2 中, $W_1 = \text{span}\{(1, 0)^T\}$ (即 x 轴) 的补空间可以是 $\text{span}\{(0, 1)^T\}$ (即 y 轴), 也可以是 $\text{span}\{(1, 1)^T\}$, 或者更一般地 $\text{span}\{(a, b)^T\}$ (只要 $b \neq 0$).

命题 3.15. \mathbb{R} -线性空间 $V = V_1 \oplus \cdots \oplus V_k$ 当且仅当如下两条满足:

- (1) $V = V_1 + \cdots + V_k$.
- (2) 对任意 $1 \leq i \leq k$, 有 $V_i \cap \sum_{j \neq i} V_j = \{0\}$.

证明. 留做练习. □

例 3.36 (非直和的例子). 在 \mathbb{R}^2 中, 令 $W_1 = \text{span}\{(1, 0)^T\}$, $W_2 = \text{span}\{(0, 1)^T\}$, $W_3 = \text{span}\{(1, 1)^T\}$, 则 $\mathbb{R}^2 = W_1 + W_2 + W_3$, 但这不是直和. 例如, $(1, 1)^T$ 有多种分解:

$$(1, 1)^T = \underbrace{(1, 0)^T}_{\in W_1} + \underbrace{(0, 1)^T}_{\in W_2} + \underbrace{(0, 0)^T}_{\in W_3} = \underbrace{(0, 0)^T}_{\in W_1} + \underbrace{(0, 0)^T}_{\in W_2} + \underbrace{(1, 1)^T}_{\in W_3}.$$

这是因为 $W_3 \cap (W_1 + W_2) = W_3 \neq \{0\}$, 违反了上述命题中的条件 (2).

命题 3.16. 给定 \mathbb{R} -线性空间 V, W , 有

$$\dim_{\mathbb{R}} V \oplus W = \dim_{\mathbb{R}} V + \dim_{\mathbb{R}} W$$

证明. 假设 $\{v_1, \dots, v_n\}$ 是 V 的一组基, $\{w_1, \dots, w_m\}$ 是 W 的一组基. 令

$$\mathcal{B} = \{(v_1, 0), \dots, (v_n, 0)\} \cup \{(0, w_1), \dots, (0, w_m)\}.$$

直接验证 \mathcal{B} 构成了 $V \oplus W$ 的一组基. □

3.9 商空间

直和是将线性空间”拆分”为两个互不干扰的部分, 而商空间则是一种”压缩”操作: 把某个子空间 W 中的所有向量都”视为零”, 或者等价地说, 把相差一个 W 中元素的向量都视为同一个. 这类似于整数中的”模 n 同余”: 在 $\mathbb{Z}/n\mathbb{Z}$ 中, 两个整数 a, b 被视为相同当且仅当 $n \mid (a - b)$. 在线性空间中, 我们用 $v_1 - v_2 \in W$ 来代替整除关系.

商空间：把某些方向压扁

商空间可以理解为“故意忽略某些差异”。例如在平面中如果把同一条竖直线上的点都看成等价，那么我们只剩下横坐标这一维信息；这相当于把竖直方向整体压扁。更抽象地说， V/W 中的一个元素不是单个向量，而是一整条形如 $v+W$ 的平行副本。学习商空间时，最好始终记住这个图像：被模掉的子空间 W 变成了零方向。

在正式给出定义之前，我们先解释记号。对于 V 的子空间 W 和 $v \in V$ ，集合

$$v + W := \{v + w \mid w \in W\}$$

称为 v 所在的**陪集** (coset)。不难验证

$$v_1 + W = v_2 + W \iff v_1 - v_2 \in W.$$

换句话说，两个向量属于同一个陪集当且仅当它们之差在 W 中。这样， V 被划分成了互不相交的陪集的并，而商空间 V/W 就是以这些陪集为元素的集合。

定义 3.19. 给定 \mathbb{R} -线性空间 V 及其子空间 W ，**商空间** (quotient space) 定义为陪集的集合 $V/W = \{v + W \mid v \in V\}$ ，其上带有如下运算：

(1) $(v_1 + W) + (v_2 + W) := (v_1 + v_2) + W$ ，其中 $v_1, v_2 \in V$ 。

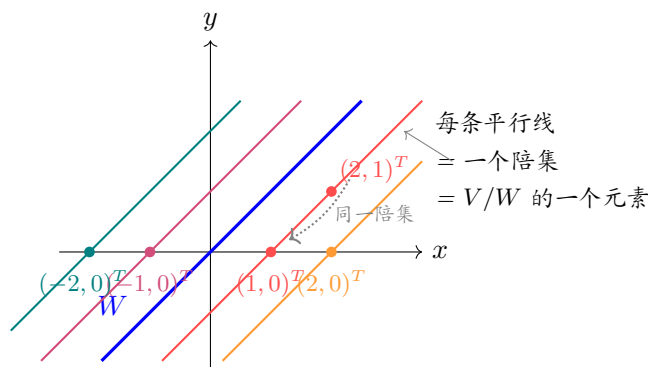
(2) $c(v + W) := cv + W$ ，其中 $c \in \mathbb{R}$ 。

使得其成为一个 \mathbb{R} -线性空间，其零向量为 $0 + W = W$ 。

注 3.19. 上述运算的**良定义性** (well-definedness) 需要验证，即运算的结果不依赖于陪集代表元的选取。以加法为例：若 $v_1 + W = v'_1 + W$ 且 $v_2 + W = v'_2 + W$ ，则 $v_1 - v'_1 \in W$ 且 $v_2 - v'_2 \in W$ ，从而 $(v_1 + v_2) - (v'_1 + v'_2) = (v_1 - v'_1) + (v_2 - v'_2) \in W$ ，即 $(v_1 + v_2) + W = (v'_1 + v'_2) + W$ 。数乘的验证类似。

例 3.37. 令 $V = \mathbb{R}^2$ ， $W = \text{span}\{(1, 1)^T\}$ ，即过原点的方向为 $(1, 1)^T$ 的直线。则 V/W 中的一个元素 (即陪集) $v + W$ 在几何上就是一条平行于 $(1, 1)^T$ 方向的直线。例如， $(1, 0)^T + W$ 是过 $(1, 0)^T$ 且方向为 $(1, 1)^T$ 的直线，而 $(2, 1)^T + W$ 是过 $(2, 1)^T$ 的平行直线。由于 $(1, 0)^T - (2, 1)^T = (-1, -1)^T = -1 \cdot (1, 1)^T \in W$ ，这两条直线其实是同一条，即 $(1, 0)^T + W = (2, 1)^T + W$ 。

因此 V/W 可以想象为：将 \mathbb{R}^2 中所有平行于 $(1, 1)^T$ 方向的直线各“压缩”成一个点。每条这样的直线恰好与 x 轴交于一点 $(a, 0)^T$ ，从而 $V/W \cong \mathbb{R}$ ，维数为 1。



例 3.38 (多项式的商空间). 考虑 $V = \mathbb{R}[x]_{\leq 3}$ (次数 ≤ 3 的多项式) 和 $W = \text{span}\{1, x\}$ (次数 ≤ 1 的多项式). 则 V/W 中, 两个多项式 $p(x), q(x)$ 属于同一个陪集当且仅当 $p(x) - q(x) \in W$, 即它们的 x^2 项和 x^3 项系数相同. 换句话说, 在 V/W 中我们“忽略了低次项”, 只关心高次项. 因此 V/W 可以用 $\{x^2 + W, x^3 + W\}$ 作为基, $\dim V/W = 2$.

命题 3.17. 给定 \mathbb{R} -线性空间 V 及其子空间 W , 自然投射 (canonical projection)

$$\begin{aligned} \pi: V &\rightarrow V/W \\ v &\mapsto v + W \end{aligned}$$

是满射的线性映射, 并且 $\ker \pi = W$.

命题 3.18. 给定 \mathbb{R} -线性空间 V 及其子空间 W , 有

$$\dim_{\mathbb{R}} V/W = \dim_{\mathbb{R}} V - \dim_{\mathbb{R}} W.$$

证明. 假设 w_1, \dots, w_m 是 W 的一组基. 根据命题 3.12 可以将其扩充为 V 的一组基

$$w_1, \dots, w_m, v_1, \dots, v_n.$$

我们证明

$$\{v_1 + W, \dots, v_n + W\}$$

构成 V/W 的一组基.

生成性: 任取 $v \in V$, 有 $v = \sum_{i=1}^m a_i w_i + \sum_{j=1}^n b_j v_j$, 从而

$$v + W = \sum_{j=1}^n b_j (v_j + W),$$

因为 $\sum_{i=1}^m a_i w_i \in W$, 在商空间中它属于零元 W .

线性无关性: 若 $\sum_{j=1}^n b_j (v_j + W) = W$ (即商空间的零向量), 则 $\sum_{j=1}^n b_j v_j \in W$, 从而 $\sum_{j=1}^n b_j v_j = \sum_{i=1}^m a_i w_i$ 对某些 a_i 成立. 由 $w_1, \dots, w_m, v_1, \dots, v_n$ 的线性无关性知 $b_1 = \dots = b_n = 0$.

因此 $\dim V/W = n = \dim V - \dim W$. □

注 3.20. 将维数公式 $\dim V = \dim W + \dim V/W$ 与直和的维数公式 $\dim(V_1 \oplus V_2) = \dim V_1 + \dim V_2$ 对比, 可以发现: 如果 V_2 是 W 在 V 中的补空间 (即 $V = W \oplus V_2$), 则 $\dim V/W = \dim V_2$. 事实上可以证明 $V/W \cong V_2$, 但这个同构依赖于补空间 V_2 的选取, 不是典范的 (*canonical*).

3.10 习题

3.10.1 练习题

习题 3.1 (子空间的和与交). 在 \mathbb{R}^3 中设

$$U = \text{span}\{(1, 0, 1)^T, (0, 1, 1)^T\}, \quad W = \text{span}\{(1, 1, 2)^T, (1, -1, 0)^T\}.$$

1. 分别求 U 和 W 的维数.
2. 求 $U \cap W$ 的一组基.
3. 求 $U + W$ 的维数, 并验证公式

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

习题 3.2 (商空间的直观). 设 $V = \mathbb{R}^2$, $W = \text{span}\{(0, 1)^T\}$.

1. 描述陪集 $(a, b)^T + W$ 在平面中的几何形状.
2. 判断 $(1, 2)^T + W$ 与 $(1, -5)^T + W$ 是否相同.
3. 判断 $(1, 2)^T + W$ 与 $(2, 2)^T + W$ 是否相同.
4. 说明为什么 V/W 可以自然地看成一维空间.

习题 3.3. 请判断以下向量组是否线性无关, 并找出下述向量组生成的子空间的一组数目最少的生成元.

1. $a_1 = (1, 2, 3), a_2 = (3, 6, 7)$;
2. $a_1 = (2, -3, 1), a_2 = (3, -1, 5), a_3 = (1, -4, 3)$;
3. $a_1 = (4, -5, 2, 6), a_2 = (2, -2, 1, 3), a_3 = (6, -3, 3, 9), a_4 = (4, -1, 5, 6)$;
4. $a_1 = (1, 0, 0, 2, 5), a_2 = (0, 1, 0, 3, 4), a_3 = (0, 0, 1, 4, 7), a_4 = (2, -3, 4, 11, 12)$.

习题 3.4. 请将 $\text{span}_{\mathbb{R}}\{v_1, v_2\}$ 写成某个矩阵的核. 其中 $v_1 = (1, 2, 3, 4)^T$, $v_2 = (5, 6, 7, 8)^T$.

习题 3.5. 令 $S = \{v \in \mathbb{R}^3 : v = (r - 2s, 3r + s, s)^T, r, s \in \mathbb{R}\}$.

1. 请验证 S 是 \mathbb{R}^3 的子空间.
2. 证明 S 是平面 $3x - y + 7z = 0$.

习题 3.6. 判断以下集合和运算是否构成 \mathbb{R} -线性空间.

1. n -阶实对称矩阵 $A = A^T$ 全体, 在矩阵的加法和数乘下.
2. n -阶实反对称矩阵 $A = -A^T$ 全体, 在矩阵的加法和数乘下.
3. 满足 $p(1) = p(2)$ 的所有实系数多项式, 在通常多项式的加法和数乘下.
4. 秩小于或等于 1 的三阶方阵全体, 在矩阵的加法和数乘下.
5. 在实轴上定义的周期等于 1 的全体实值函数, 在通常函数的加法和数乘下.
6. \mathbb{R}^2 中满足方程 $x^2 = y^2$ 的点集, 在 \mathbb{R}^2 的加法和数乘下.
7. 实轴上的光滑函数, 满足 $f'(t) + f(t) = \cos t$, 在通常函数的加法和数乘下.

习题 3.7.

1. 请举出 \mathbb{R}^2 中满足加法封闭, 但是数乘不封闭的非空集合的例子.
2. 请举出 \mathbb{R}^2 中满足数乘封闭, 但是加法不封闭的非空集合的例子.

习题 3.8. 在 \mathbb{R} -线性空间 V 中,

1. 验证对任意 $v \in V$, $-1 \cdot v = -v$.
2. 验证对任意 $c \in \mathbb{R}$, $c\mathbf{0} = \mathbf{0}$, 这里 $\mathbf{0}$ 指的是 V 中的加法单位元.

习题 3.9. 固定某个向量 $w \in \mathbb{R}^n$. 对于 $a \in \mathbb{R}$ 且 $u \in \mathbb{R}^n$, 定义

$$a \otimes u = a(u - w) + w.$$

$$u \oplus v = u + v - w.$$

请判断并证明 $V = \mathbb{R}^n$ 在数乘 \otimes 和加法 \oplus 下是否做成 \mathbb{R} 线性空间. 如果是, 其中零向量是什么? (说明: 我们用记号 \otimes 和 \oplus 来和 \mathbb{R}^n 上的通常加法和数乘做区分).

习题 3.10. 决定以下向量组是否组成 \mathbb{R}^3 的基.

$$\left\{ \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \right\}.$$

习题 3.11. 判定以下 $M_{2 \times 2}(\mathbb{R})$ 中的向量组是否线性无关:

$$A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 3 & 6 \\ 0 & 1 \end{bmatrix}.$$

习题 3.12. $C^\infty(\mathbb{R})$ (\mathbb{R} 上的光滑函数) 是 (无穷维) \mathbb{R} -线性空间. 证明, 函数

$$\sin(t), \sin(2t), \dots, \sin(Nt)$$

线性无关.

习题 3.13. 如果矩阵 $A = A^T$, 则称 A 是对称矩阵. 如果 $A = -A^T$, 则称 A 是反对称矩阵. 分别证明对称矩阵和反对称矩阵构成 $M_n(\mathbb{R})$ 的子空间, 计算这两个子空间的维数.

习题 3.14. 记 $V = C^\infty(\mathbb{R})$ 是 \mathbb{R} 上的光滑函数组成的 \mathbb{R} -线性空间. 验证两组元素 B, C 满足 $\text{Span}_{\mathbb{R}} B = \text{Span}_{\mathbb{R}} C = W$, 且 B, C 均为 W 的基. 请写出 B, C 的转换矩阵 $P_{B \leftarrow C}$ 和 $P_{C \leftarrow B}$.

1. $B = (1, \cos x, \cos 2x, \cos 3x), C = (1, \cos x, \cos^2 x, \cos^3 x)$.

2. $B = (1, x, x^2, x^3), C = (1, x - a, (x - a)^2, (x - a)^3)$ ($a \in \mathbb{R}$ 为常数)

习题 3.15. 找到一个 4×3 矩阵 A 使得 A 的列空间有基向量 $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$, 行空间有基向量 $\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$.

习题 3.16. 设 A 是一个 3×3 矩阵, 假设对于任意 3 维列向量 x , 都有某个依赖于 x 的实数, 使得 $Ax = c(x)x$. 证明 $A = cI_3$.

习题 3.17. 请写出一个 3×3 矩阵 A , 使得 A 的 *kernel* 是 $\text{span}_{\mathbb{R}}\left\{\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}\right\}$.

习题 3.18. 设 A 是一个 $m \times n$ 矩阵, 秩为 r . 假设 $Ax = b$ 对于某些右端 b 没有解, 而对于另一些右端 b 有无穷多解.

1. 决定 A 的零空间是否只包含零向量, 并说明原因.
2. 决定 A 的列空间是否是 \mathbb{R}^m , 并说明原因.
3. 是否存在某个右端 b 使得 $Ax = b$ 有且只有一个解? 为什么?
4. 找出 r, m 和 n 之间的大小关系.

习题 3.19. 判断下列集合是否为 \mathbb{R}^2 的子空间。

$$S_1 = \{(x, y) : x + y = 0\}, \quad S_2 = \{(x, y) : x + y = 1\}.$$

习题 3.20. 判断向量

$$(3, 5)$$

是否属于 $\text{span}\{(1, 1), (1, 2)\}$ 。若属于，写出线性组合。

习题 3.21. 判断下列向量组是否线性无关。

$$(1, 0, 1), \quad (0, 1, 1), \quad (1, 1, 2).$$

习题 3.22. 求向量组

$$(1, 2, 0), \quad (2, 4, 0), \quad (0, 1, 1)$$

张成空间的一组基，并写出该空间的维数。

习题 3.23. 在 \mathbb{R}^3 中，设

$$u_1 = (1, 0, 1), \quad u_2 = (0, 1, 1).$$

求 $\text{span}\{u_1, u_2\}$ 中满足第三个坐标等于 5 的所有向量。

习题 3.24. 设

$$B = \{(1, 1), (1, -1)\}$$

是 \mathbb{R}^2 的一组基。求向量 $(3, 1)$ 在基 B 下的坐标。

习题 3.25. 给出 \mathbb{R}^3 中一个维数为 1 的子空间、一个维数为 2 的子空间，并分别写出它们的一组基。

3.10.2 思考题

习题 3.26. 设 V 是 \mathbb{R} 上有限维向量空间， W_1, W_2, \dots, W_n 是 V 的真子空间，证明：

$$W_1 \cup W_2 \cup \dots \cup W_n \neq V.$$

习题 3.27. 考虑 “Shifted Legendre polynomial”

$$\tilde{P}_n(x) = \frac{1}{n!} \frac{d^n}{dx^n} (x^2 - x)^n$$

证明 $\tilde{P}_0, \tilde{P}_1, \dots$ 构成 $\mathbb{R}[x]$ 的一组基。

习题 3.28 (两个或多个子空间配置). 设 V 是一个向量空间。

1. 设 V_1, V_2 和 V'_1, V'_2 是 V 的子空间, 且满足

$$\dim(V_i \cap V_j) = \dim(V'_i \cap V'_j)$$

对所有可能的 i, j 成立。证明存在一个同构 $T: V \rightarrow V$ 使得 $T(V_i) = V'_i$ 。

2. 设 V_1, V_2, V_3 和 V'_1, V'_2, V'_3 是 V 的子空间, 且满足题中相应的三重交与和空间维数条件。是否总存在同构 $T: V \rightarrow V$ 使得 $T(V_i) = V'_i$?

3. 如果是四个或更多子空间, 结论如何?

习题 3.29 (有限群表示中的不变子空间补空间)。设 G 是有限群, p 是素数。令 V 为有限维 \mathbb{F}_p -向量空间, 且 G 作用在 V 上。假设 $|G|$ 与 p 互素。证明: 若 $W \subseteq V$ 是 G -不变子空间, 则存在另一个 G -不变子空间 U , 使得

$$V = W \oplus U.$$

4 线性映射

在上一节中, 我们系统地研究了线性空间的内部结构——基与维数、子空间的和与交、直和与商空间. 然而, 数学中不仅要研究对象本身, 还要研究对象之间保持结构的映射. 正如研究群时要考虑群同态、研究拓扑空间时要考虑连续映射一样, 研究线性空间时, 最自然的映射就是保持加法和数乘的映射——线性映射. 线性映射是连接不同线性空间的桥梁, 也是将抽象的线性代数理论转化为具体矩阵计算的关键工具.

在线性映射最直观的二维几何图景里, 旋转、伸缩、镜像、错切都是线性映射: 它们把直线映为直线, 保持原点, 也保持线性组合的关系. 这正是计算机图形学中最基本的一批操作. 相反, 平移虽然同样常见, 但因为它把原点移走, 不再满足 $T(\mathbf{0}) = \mathbf{0}$, 所以属于仿射变换而不是线性映射. 这一点也说明, 线性映射的定义并不是形式主义, 而是在精确刻画哪些变换真正保持了线性结构.

更贴近日常经验的例子是数字图像中的颜色校正. 一个像素的颜色可以写成 RGB 列向量 $\begin{pmatrix} r \\ g \\ b \end{pmatrix}$, 而相机与显示器之间的颜色空间转换往往由一个 3×3 矩阵给出. 甚至当我们研究一般的非线性映射时, 也常常先在某一点附近用 Jacobian 矩阵给出局部线性近似. 因此线性映射不仅描述“线性的世界”, 也构成理解复杂系统的第一近似语言.

4.1 定义与例子

定义 4.1. 对于 \mathbb{R} -线性空间 V, W , 映射 $T: V \rightarrow W$ 被称为 \mathbb{R} -**线性映射** (*linear map*), 如果

(1) 对任意 $v_1, v_2 \in V$ 有 $T(v_1 + v_2) = Tv_1 + Tv_2$.

(2) 对于任意 $c \in \mathbb{R}, v \in V$ 有 $T(cv) = cTv$.

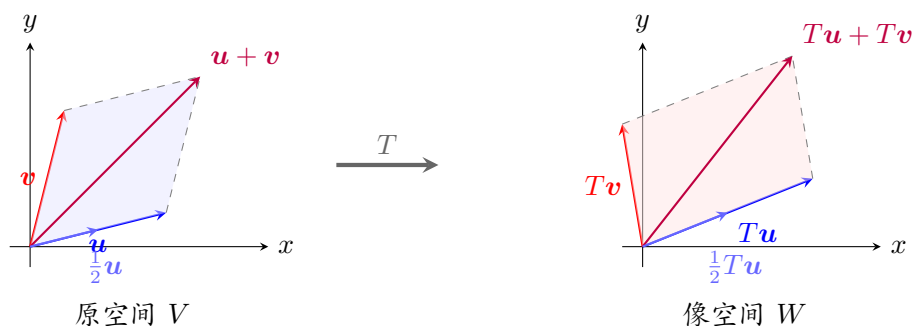
注 4.1. 上述两条可以合并为一条: T 是线性映射当且仅当对任意 $v_1, v_2 \in V$ 和 $c_1, c_2 \in \mathbb{R}$ 有 $T(c_1v_1 + c_2v_2) = c_1Tv_1 + c_2Tv_2$. 也就是说, 线性映射是一种保持加法和数乘规则的操作: 先做线性组合再作用 T , 与先作用 T 再做同样的线性组合, 结果相同. 更一般地, 线性映射保持任意有限线性组合: $T(\sum_{i=1}^k c_i v_i) = \sum_{i=1}^k c_i T v_i$.

注 4.2 (几何直觉). 线性映射有非常直观的几何含义: 它保持平行四边形法则和向量的比例关系. 具体来说:

(1) **保持平行四边形**: 若 u, v 是 V 中的向量, 则以 $\mathbf{0}, u, v, u+v$ 为顶点的平行四边形被 T 映射为以 $\mathbf{0}, Tu, Tv, T(u+v) = Tu + Tv$ 为顶点的平行四边形.

(2) **保持比例**: 若 v 和 cv 共线且长度之比为 $1:|c|$, 则 Tv 和 $T(cv) = cTv$ 也共线且长度之比仍为 $1:|c|$.

下图展示了 \mathbb{R}^2 中这一现象: 左侧是原空间中由 u, v 张成的平行四边形, 右侧是线性映射 T 作用后的像。



可以看到, 虽然平行四边形的形状 (角度和边长) 可能改变, 但平行关系和中点 (比例关系) 得以保持. 反过来说, 一个保持原点不动的映射如果将平行四边形映为平行四边形且保持向量比例, 那么它就是线性映射——这正是线性映射的“几何定义”。

命题 4.1. 设 $T: V \rightarrow W$ 是 \mathbb{R} -线性映射, 则

- (1) $T(\mathbf{0}_V) = \mathbf{0}_W$.
- (2) $T(-v) = -T(v)$, 对任意 $v \in V$.

证明. (1). $T(\mathbf{0}_V) = T(0 \cdot \mathbf{0}_V) = 0 \cdot T(\mathbf{0}_V) = \mathbf{0}_W$. (2). $T(-v) = T((-1) \cdot v) = (-1) \cdot Tv = -Tv$. □

下面我们给出线性映射的一系列例子.

例 4.1 (矩阵乘法). 对于矩阵 $A \in M_{m \times n}(\mathbb{R})$, 映射

$$T_A: \mathbb{R}^n \rightarrow \mathbb{R}^m$$

$$x \mapsto Ax$$

是 \mathbb{R} -线性映射. 这是因为 $A(c_1x_1 + c_2x_2) = c_1Ax_1 + c_2Ax_2$. 事实上, 这是最基本也最重要的线性映射: 我们将在下一节看到, 取定基之后, 每个有限维线性空间之间的线性映射都可以用矩阵乘法来表示.

例 4.2 (零映射与恒等映射). 对于 \mathbb{R} -线性空间 V, W :

- (1) **零映射** $0: V \rightarrow W$, 定义为 $0(v) = \mathbf{0}_W$ 对所有 $v \in V$, 是线性映射.
- (2) **恒等映射** $I_V: V \rightarrow V$, 定义为 $I_V(v) = v$ 对所有 $v \in V$, 是线性映射.

例 4.3 (投影映射). \mathbb{R}^n 到子空间 W 的投影映射是 \mathbb{R} -线性映射. 例如, 设 $V = \mathbb{R}^3$, W 为 xy 平面, 则投影 $\pi: \mathbb{R}^3 \rightarrow W$ 定义为 $\pi(x, y, z)^T = (x, y, 0)^T$, 容易验证 π 保持加法和数乘.

例 4.4 (求导与积分). 考虑 \mathbb{R} -线性空间 $C^\infty(\mathbb{R})$ (无穷次可微函数全体).

(1) 求导算子 $D: C^\infty(\mathbb{R}) \rightarrow C^\infty(\mathbb{R})$, $D(f) = f'$ 是线性映射, 因为 $(f+g)' = f' + g'$ 且 $(cf)' = cf'$.

(2) 积分算子 $I: C^\infty(\mathbb{R}) \rightarrow C^\infty(\mathbb{R})$, $I(f)(x) = \int_0^x f(t) dt$ 也是线性映射.

求导和积分作为线性映射是分析与线性代数之间的桥梁——微分方程的理论在很大程度上依赖于这一观察.

例 4.5 (非线性映射的反例). 映射 $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ 不是线性映射. 例如 $f(1+1) = f(2) = 4$, 而 $f(1) + f(1) = 1 + 1 = 2$, 因此 f 不保持加法. 一般来说, 实函数 $f: \mathbb{R} \rightarrow \mathbb{R}$ 是 \mathbb{R} -线性映射当且仅当 $f(x) = cx$ 对某个常数 $c \in \mathbb{R}$, 即 f 的图像是过原点的直线.

线性映射的一个核心性质是: 它由其在一组基上的取值完全确定. 直觉上, 由于任意向量都是基向量的线性组合, 而线性映射保持线性组合, 因此只要知道每个基向量的像, 就知道了所有向量的像.

命题 4.2 (线性映射由基上的值确定). 设 V 是 \mathbb{R} -线性空间, $\{v_1, \dots, v_n\}$ 是 V 的一组基, W 是 \mathbb{R} -线性空间.

(1) **唯一性**: 若 $T_1, T_2 \in \text{Hom}_{\mathbb{R}}(V, W)$ 满足 $T_1(v_i) = T_2(v_i)$ 对所有 $1 \leq i \leq n$ 成立, 则 $T_1 = T_2$.

(2) **存在性**: 对于 W 中任意给定的 n 个向量 w_1, \dots, w_n , 存在唯一的 $T \in \text{Hom}_{\mathbb{R}}(V, W)$ 满足 $T(v_i) = w_i$.

证明. (1). 任取 $v = \sum_{i=1}^n a_i v_i \in V$, 有 $T_1(v) = \sum_{i=1}^n a_i T_1(v_i) = \sum_{i=1}^n a_i T_2(v_i) = T_2(v)$.

(2). 定义 $T(\sum_{i=1}^n a_i v_i) = \sum_{i=1}^n a_i w_i$. 由于 $\{v_1, \dots, v_n\}$ 是基, 每个 $v \in V$ 的系数 (a_1, \dots, a_n) 唯一确定, 因此 T 是良定义的. 线性性可直接验证: 若 $v = \sum a_i v_i$, $u = \sum b_i v_i$, 则 $T(v+u) = \sum (a_i + b_i) w_i = Tv + Tu$, $T(cv) = \sum ca_i w_i = cTv$. 唯一性由 (1) 保证. \square

注 4.3. 这个命题是下一节中“线性映射与矩阵一一对应”的理论基础: 线性映射 T 由 n 个向量 $Tv_1, \dots, Tv_n \in W$ 确定, 而将这 n 个向量在 W 的基下写成坐标, 恰好就是一个 $m \times n$ 矩阵.

定义 4.2. 给定 \mathbb{R} -线性空间 V, W , 全体 V 到 W 的 \mathbb{R} 线性映射组成的集合记做 $\text{Hom}_{\mathbb{R}}(V, W)$.

注 4.4. $\text{Hom}_{\mathbb{R}}(V, W)$ 上有自然的加法与 \mathbb{R} -数乘结构如下:

(1) $(T_1 + T_2)v = T_1v + T_2v$, 其中 $v \in V$.

(2) $(cT)v = cTv$, 其中 $v \in V, c \in \mathbb{R}$.

可以直接验证上述结构使得 $\text{Hom}_{\mathbb{R}}(V, W)$ 成为 \mathbb{R} -线性空间.

命题 4.3. 给定 \mathbb{R} -线性映射 $T_1: V_1 \rightarrow V_2, T_2: V_2 \rightarrow V_3$, 则 $T_2 \circ T_1 \in \text{Hom}_{\mathbb{R}}(V_1, V_3)$.

证明. 对任意 $u, v \in V_1$ 和 $c \in \mathbb{R}$, 有

$$(T_2 \circ T_1)(u + v) = T_2(T_1u + T_1v) = T_2T_1u + T_2T_1v,$$

以及

$$(T_2 \circ T_1)(cu) = T_2(cT_1u) = cT_2T_1u.$$

因此 $T_2 \circ T_1$ 仍然是线性映射. □

4.2 线性映射与矩阵

根据命题4.2, 线性映射由其在一组基上的取值完全确定. 既然如此, 我们可以把这些取值 (即 Tv_1, \dots, Tv_n 在 W 的基下的坐标) 排成一个矩阵, 从而在线性映射与矩阵之间建立一一对应. 这是将抽象的线性映射问题转化为具体矩阵计算的核心桥梁.

定义 4.3. 设 V 是 n 维 \mathbb{R} -线性空间, W 是 m 维 \mathbb{R} -线性空间, $B = \{v_1, \dots, v_n\}$ 是 V 的一组基, $C = \{w_1, \dots, w_m\}$ 是 W 的一组基. 对于 $T \in \text{Hom}_{\mathbb{R}}(V, W)$, 定义 T 在基 B, C 下的表示矩阵 (representation matrix) 为

$$[T]_B^C = ([Tv_1]_C, \dots, [Tv_n]_C) \in M_{m \times n}(\mathbb{R}),$$

即以 Tv_1, \dots, Tv_n 在基 C 下的坐标为列向量排成的矩阵.

定理 4.1. 设 V 是 n 维 \mathbb{R} -线性空间, W 是 m 维 \mathbb{R} -线性空间, 固定 V 的基 B 和 W 的基 C . 则映射

$$\begin{aligned} \Phi: \text{Hom}_{\mathbb{R}}(V, W) &\rightarrow M_{m \times n}(\mathbb{R}) \\ T &\mapsto [T]_B^C \end{aligned}$$

是 \mathbb{R} -线性空间的同构.

证明. **线性性:** 对于 $T_1, T_2 \in \text{Hom}_{\mathbb{R}}(V, W)$ 和 $c \in \mathbb{R}$, 有

$$[(T_1 + T_2)v_i]_C = [T_1v_i]_C + [T_2v_i]_C, \quad [(cT_1)v_i]_C = c[T_1v_i]_C,$$

因此 $[T_1 + T_2]_B^C = [T_1]_B^C + [T_2]_B^C$, $[cT_1]_B^C = c[T_1]_B^C$, 即 Φ 是线性映射.

单射性: 若 $[T]_B^C = \mathbf{0}$, 则 $[Tv_i]_C = \mathbf{0}$ 对所有 i 成立, 即 $Tv_i = \mathbf{0}_W$. 由命题4.2知 $T = \mathbf{0}$.

满射性: 对任意 $A = (a_1, \dots, a_n) \in M_{m \times n}(\mathbb{R})$, 其中 $a_i \in \mathbb{R}^m$, 令 $w'_i = \sum_{j=1}^m (a_i)_j w_j$ (即以 a_i 为 C 下坐标的向量). 由命题4.2, 存在唯一的 $T \in \text{Hom}_{\mathbb{R}}(V, W)$ 满足 $Tv_i = w'_i$, 从而 $[T]_B^C = A$. □

命题 4.4. 设 $T: V \rightarrow W$ 是 \mathbb{R} -线性映射, B, C 分别是 V 和 W 的一组基, 则对任意 $v \in V$ 有

$$[T(v)]_C = [T]_B^C [v]_B.$$

证明. 设 $v = \sum_{i=1}^n a_i v_i$, 即 $[v]_B = (a_1, \dots, a_n)^T$, 则

$$Tv = \sum_{i=1}^n a_i T v_i.$$

两边取 C 下的坐标, 由坐标映射的线性性有

$$[Tv]_C = \sum_{i=1}^n a_i [T v_i]_C = ([T v_1]_C, \dots, [T v_n]_C) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = [T]_B^C [v]_B.$$

□

注 4.5. 这是一个非常重要的观点: 取定基之后, 线性映射的作用就变成了矩阵乘法. 因此线性空间上线性映射的问题可以转化为矩阵问题来解决, 这使得抽象理论变得具体且可计算.

例 4.6 (标准基下的简单线性映射). 考虑 \mathbb{R}^2 中的线性映射

$$T \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + y \\ y \end{pmatrix}.$$

它把 $e_1 = (1, 0)^T$ 送到 $(2, 0)^T$, 把 $e_2 = (0, 1)^T$ 送到 $(1, 1)^T$. 因此在标准基 $B = \{e_1, e_2\}$ 下,

$$[T]_B^B = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

于是计算 $T(3, 2)^T$ 就等价于矩阵乘法:

$$[T]_B^B \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 8 \\ 2 \end{pmatrix}.$$

习题 4.1. 设 $S(x, y) = (x - y, 2y)$. 求 $S(e_1)$ 和 $S(e_2)$, 写出 S 在标准基下的矩阵, 并计算 $S(2, 3)$.

注意到定理 4.1 中的对应依赖于基的选取. 一个自然的问题是: 同一个线性映射在不同基下的表示矩阵之间有什么关系?

命题 4.5. 假设 B_1, B_2 都是 \mathbb{R} -线性空间 V 的基, C_1, C_2 都是 W 的基, 则对于 $T \in \text{Hom}_{\mathbb{R}}(V, W)$, 有

$$[T]_{B_1}^{C_1} = P_{C_1 \leftarrow C_2} [T]_{B_2}^{C_2} P_{B_2 \leftarrow B_1}$$

证明. 对任意 $v \in V$, 坐标变换给出

$$[v]_{B_2} = P_{B_2 \leftarrow B_1} [v]_{B_1}.$$

先用 B_2, C_2 下的表示矩阵计算 $T(v)$, 再把结果从 C_2 坐标换到 C_1 坐标, 得到

$$[T(v)]_{C_1} = P_{C_1 \leftarrow C_2} [T]_{B_2}^{C_2} P_{B_2 \leftarrow B_1} [v]_{B_1}.$$

另一方面, 根据命题4.4, 也有

$$[T(v)]_{C_1} = [T]_{B_1}^{C_1} [v]_{B_1}.$$

由于这对所有 $v \in V$ 都成立, 两个矩阵相同. \square

定义 4.4. 矩阵 $A, B \in M_n(\mathbb{R})$ 称为**相似** (*similar*), 如果存在可逆矩阵 $P \in M_n(\mathbb{R})$ 使得 $B = PAP^{-1}$.

因此, 对于 \mathbb{R} -线性映射 $T: V \rightarrow V$ (即 $V = W$ 的情形), 其不同基下的矩阵是相似的. 这就是相似矩阵的几何解释: **两个矩阵相似当且仅当它们是同一个线性映射在不同基下的表示**. 这一观点也表明, 如果某个量对于相似矩阵是不变的 (即**相似不变量**), 那么它实际上是线性映射自身的量, 而不依赖于基的选取.

定义 4.5. 对于有限维 \mathbb{R} -线性空间之间的线性映射 $T: V \rightarrow W$, 定义 T 的**秩** (*rank*) 为

$$\text{rank } T := \text{rank}[T]_B^C,$$

其中 B 是 V 的一组基, C 是 W 的一组基.

命题 4.6. $\text{rank } T$ 的定义是良好的, 即不依赖于基 B, C 的选取.

证明. 由命题4.5, 换基只会把表示矩阵变为

$$P_{C_1 \leftarrow C_2} [T]_{B_2}^{C_2} P_{B_2 \leftarrow B_1},$$

其中左右两侧的转移矩阵都可逆. 左乘、右乘可逆矩阵不改变秩, 因此 $\text{rank}[T]_B^C$ 不依赖于基的选择. \square

注 4.6 (行列式和迹的预告). 对于自同态 $T: V \rightarrow V$, 后续行列式一章会正式定义 $\det T$, 并说明迹 $\text{tr } T$ 也可以作为线性映射自身的不变量来理解. 这些量的良定义性同样来自换基公式和相似不变量. 在本章中如果出现行列式或迹, 可以先把它们看成后续章节的预告性语言.

例 4.7. 考虑 \mathbb{R}^2 上由逆时针旋转 θ 给出的线性映射, 并且记 $B = \{e_1, e_2\}$ 是 \mathbb{R}^2 的一组标准基, 则

$$T_\theta(e_1) = \begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix}, \quad T_\theta(e_2) = \begin{pmatrix} -\sin \theta \\ \cos \theta \end{pmatrix}.$$

从而有

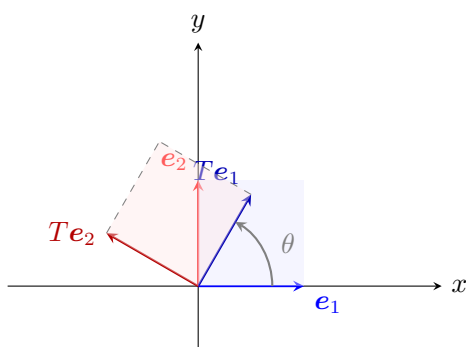
$$[T]_B^B = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

根据旋转的几何直观我们有 $T_{\theta_1} \circ T_{\theta_2} = T_{\theta_1 + \theta_2}$, 从而有如下等式:

$$\begin{pmatrix} \cos \theta_1 & -\sin \theta_1 \\ \sin \theta_1 & \cos \theta_1 \end{pmatrix} \begin{pmatrix} \cos \theta_2 & -\sin \theta_2 \\ \sin \theta_2 & \cos \theta_2 \end{pmatrix} = \begin{pmatrix} \cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) \\ \sin(\theta_1 + \theta_2) & \cos(\theta_1 + \theta_2) \end{pmatrix}.$$

这证明了和角公式.

下图以 $\theta = 60^\circ$ 为例, 展示旋转映射将正方形区域 (由 e_1, e_2 张成) 旋转为一个新的正方形区域. 旋转保持向量的长度和夹角不变, 因此是一类特别”好”的线性映射 (正交变换).



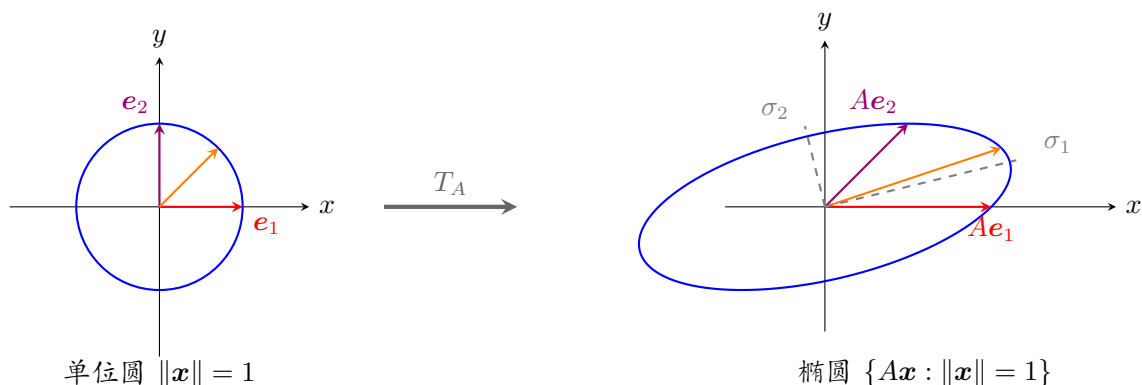
例 4.8 (反射). 考虑 \mathbb{R}^2 上关于过原点的直线 l 的反射 (镜像) 映射. 设 l 与 x 轴正方向的夹角为 α , 记 $B = \{e_1, e_2\}$ 为标准基. 为求 $[R_\ell]_B^B$, 只需计算 $R_\ell(e_1)$ 和 $R_\ell(e_2)$. 利用几何关系 (将 e_1 分解为平行于 l 和垂直于 l 的分量, 再将垂直分量取反) 可得

$$[R_\ell]_B^B = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}.$$

用后续将正式定义的行列式和迹的语言来说, $\det R_\ell = -1$ (反射改变定向), $(R_\ell)^2 = I$ (反射两次回到原位), 且 $\text{tr } R_\ell = 0$.

注 4.7 (线性映射的几何: 圆变椭圆). 旋转和反射是非常特殊的线性映射——它们保持长度不变 (即正交变换). 一般的线性映射 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 会在不同方向上产生不同程度的拉伸或压缩. 这一效应有一个优美的几何表现: \mathbb{R}^2 中的单位圆在线性映射 T 的作用下变为一个椭圆 (可能退化为线段或原点).

下图以矩阵 $A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ 为例, 展示了单位圆 $\{x \in \mathbb{R}^2 : \|x\| = 1\}$ 在 T_A 作用下变为椭圆的过程. 椭圆的两个半轴方向恰好是 A 的两个”主方向”(即 $A^T A$ 的特征向量方向), 半轴长度就是 A 的奇异值 (singular values).



直观地说, 线性映射“在每个方向上拉伸的幅度不同”, 从而将对称的圆变形为椭圆. 奇异值 $\sigma_1 \geq \sigma_2 \geq 0$ 度量了最大和最小拉伸倍率. 这一观察将在奇异值分解 (SVD: Singular Value Decomposition) 中得到严格的陈述和证明: 任何 \mathbb{R} -线性映射都可以分解为“旋转 \rightarrow 沿坐标轴拉伸 \rightarrow 旋转”三步, 即 $A = U\Sigma V^T$, 其中 U, V 为正交矩阵, Σ 为对角矩阵 (对角元即为奇异值).

例 4.9 (求导的表示矩阵). 考虑如下线性映射

$$T: \mathbb{R}[x]_{\leq n} \rightarrow \mathbb{R}[x]_{\leq n}$$

$$f(x) \mapsto \frac{df}{dx}$$

考虑基 $B = \{1, x, \dots, x^n\}$, 则有

$$[T]_B^B = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 2 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & n \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}_{(n+1) \times (n+1)}$$

注 4.8. 在上面的例子中, $T^{n+1} = 0$ (即对 n 次以下多项式求 $n+1$ 次导得零), $\text{rank } T = n$, 且 T 不是可逆映射. 满足 $T^k = 0$ 的线性映射称为**幂零** (nilpotent) 的, 我们将在后续章节中系统讨论.

4.3 线性同构

在上一节中我们看到, 线性映射在取定基之后可以用矩阵来表示. 其中一类特殊的线性映射——双射的线性映射——意味着两个线性空间具有完全相同的结构.

定义 4.6. \mathbb{R} -线性映射 $T: V \rightarrow W$ 称为**线性同构** (*linear isomorphism*), 如果 T 是双射 (即既是单射也是满射). 若存在线性同构 $T: V \rightarrow W$, 则称 V 与 W **线性同构**, 记做 $V \cong W$.

例 4.10. 逆时针旋转角度 θ 是 $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ 的 \mathbb{R} -线性同构, 其逆映射是旋转 $-\theta$.

坐标映射是线性同构最基本、最重要的例子:

命题 4.7. 给定 n 维 \mathbb{R} -线性空间 V 以及其一组基 $B = \{v_1, \dots, v_n\}$, 坐标映射

$$[\cdot]_B: V \rightarrow \mathbb{R}^n$$

$$v = \sum_{i=1}^n a_i v_i \mapsto [v]_B = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

是 \mathbb{R} -线性同构. 即任何 n 维 \mathbb{R} -线性空间都与 \mathbb{R}^n 同构.

证明. 线性性: $[\cdot]_B$ 保持加法和数乘 (因为坐标分量的加法和数乘就是对应系数的加法和数乘). 单射性: 若 $[v]_B = \mathbf{0}$, 则 $v = \sum 0 \cdot v_i = \mathbf{0}$. 满射性: 对任意 $(a_1, \dots, a_n)^T \in \mathbb{R}^n$, 有 $v = \sum_{i=1}^n a_i v_i \in V$ 满足 $[v]_B = (a_1, \dots, a_n)^T$. \square

推论 4.1. \mathbb{R} -线性空间 V, W 之间同构当且仅当 $\dim_{\mathbb{R}} V = \dim_{\mathbb{R}} W$. 即维数是有限维 \mathbb{R} -线性空间在同构意义下的**完全不变量**.

证明. 若 $V \cong W$, 取 V 的基 v_1, \dots, v_n , 其同构 T 下的像 Tv_1, \dots, Tv_n 构成 W 的基 (单射保证线性无关, 满射保证生成), 从而 $\dim V = \dim W$. 反之, 若 $\dim V = \dim W = n$, 则 $V \cong \mathbb{R}^n \cong W$. \square

注 4.9. 虽然任何两个 n 维 \mathbb{R} -线性空间都是同构的, 但这个同构一般**不是典范的** (*canonical*): 它依赖于基的选取. 一个重要的例子是 V 与其**对偶空间** $V^* := \text{Hom}_{\mathbb{R}}(V, \mathbb{R})$: 当 $\dim V = n$ 时, $\dim V^* = n$ (因为 $V^* \cong M_{1 \times n}(\mathbb{R}) \cong \mathbb{R}^n$), 从而 $V \cong V^*$, 但这个同构依赖于 V 的基的选取. 我们将在后续章节 (内积空间) 中看到, 有了额外的结构 (如内积) 之后才能建立典范的同构.

4.4 核, 像与维数公式

线性映射不仅可以用矩阵来表示, 它本身还携带了丰富的“结构信息”——其中最重要的两个子空间是核 (被映到零的向量) 和像 (所有输出向量). 维数公式则揭示了这两个子空间的维数之间的精确关系.

定义 4.7. 对于 \mathbb{R} -线性映射 $T: V \rightarrow W$, 定义

(1) T 的**核** (*kernel*)为

$$\ker T := \{v \in V \mid Tv = \mathbf{0}_W\}.$$

(2) T 的像 (image) 为

$$\text{im } T := \{Tv \in W \mid v \in V\}.$$

命题 4.8. 对于 \mathbb{R} -线性映射 $T: V \rightarrow W$, $\ker T$ 是 V 的子空间, $\text{im } T$ 是 W 的子空间.

证明. $\ker T$ 非空 (因为 $T(\mathbf{0}) = \mathbf{0}$), 且对加法和数乘封闭: 若 $Tv_1 = Tv_2 = \mathbf{0}$, 则 $T(v_1 + v_2) = Tv_1 + Tv_2 = \mathbf{0}$; 若 $Tv = \mathbf{0}$, 则 $T(cv) = cTv = \mathbf{0}$. 类似地验证 $\text{im } T$ 即可. \square

核和像提供了判断线性映射单射性与满射性的简洁判据:

命题 4.9. 设 $T: V \rightarrow W$ 是 \mathbb{R} -线性映射, 则

(1) T 是单射 $\iff \ker T = \{\mathbf{0}\}$.

(2) T 是满射 $\iff \text{im } T = W$.

证明. (2) 是像的定义的直接改写. 对于 (1): 若 T 是单射且 $Tv = \mathbf{0} = T\mathbf{0}$, 则 $v = \mathbf{0}$, 因此 $\ker T = \{\mathbf{0}\}$. 反之, 若 $\ker T = \{\mathbf{0}\}$ 且 $Tv_1 = Tv_2$, 则 $T(v_1 - v_2) = \mathbf{0}$, 从而 $v_1 - v_2 \in \ker T = \{\mathbf{0}\}$, 即 $v_1 = v_2$. \square

定理 4.2 (维数公式). 设 V 是有限维 \mathbb{R} -线性空间, $T: V \rightarrow W$ 是 \mathbb{R} -线性映射, 则

$$\dim_{\mathbb{R}} V = \dim_{\mathbb{R}} \ker T + \dim_{\mathbb{R}} \text{im } T.$$

证明. 设 $\dim \ker T = k$, 取 $\ker T$ 的一组基 $\{v_1, \dots, v_k\}$, 根据命题 3.12 将其扩充为 V 的一组基 $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$. 我们证明 $\{Tv_{k+1}, \dots, Tv_n\}$ 构成 $\text{im } T$ 的一组基.

生成性: 任取 $w \in \text{im } T$, 则 $w = Tv$ 对某个 $v \in V$. 写 $v = \sum_{i=1}^k a_i v_i + \sum_{j=k+1}^n a_j v_j$, 从而

$$w = Tv = \sum_{i=1}^k a_i \underbrace{Tv_i}_{=\mathbf{0}} + \sum_{j=k+1}^n a_j Tv_j = \sum_{j=k+1}^n a_j Tv_j.$$

线性无关性: 若 $\sum_{j=k+1}^n c_j Tv_j = \mathbf{0}$, 则 $T(\sum_{j=k+1}^n c_j v_j) = \mathbf{0}$, 即 $\sum_{j=k+1}^n c_j v_j \in \ker T$. 从而 $\sum_{j=k+1}^n c_j v_j = \sum_{i=1}^k b_i v_i$ 对某些 b_i 成立, 即 $\sum_{i=1}^k (-b_i) v_i + \sum_{j=k+1}^n c_j v_j = \mathbf{0}$. 由 $\{v_1, \dots, v_n\}$ 的线性无关性知 $c_{k+1} = \dots = c_n = 0$.

因此 $\dim \text{im } T = n - k$, 即 $\dim V = \dim \ker T + \dim \text{im } T$. \square

注 4.10. 当 $V = \mathbb{R}^n$, $W = \mathbb{R}^m$, $T = T_A$ (即矩阵乘法, 例 4.1) 时, 维数公式化为

$$\dim_{\mathbb{R}} \ker A + \dim_{\mathbb{R}} \text{im } A = n,$$

即 $\text{null}(A) + \text{rank } A = n$. 这正是我们在上一节 (定理 3.8) 中已经证明的秩-零度定理. 换言之, 矩阵版本的秩-零度定理是一般线性映射维数公式的特例.

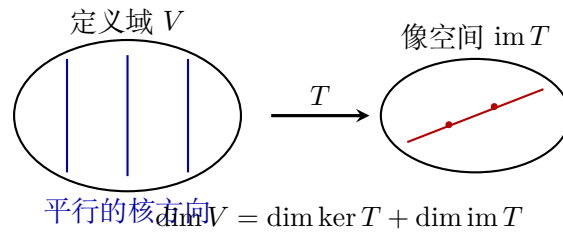


图 13: 线性映射把核方向压成零; 剩下的有效方向形成像空间.

维数公式有许多重要的推论.

推论 4.2. 对于 $A \in M_{m \times n}(\mathbb{R})$, 线性方程组 $A\mathbf{x} = \mathbf{0}$ 的解空间维数为 $n - \text{rank } A$.

推论 4.3. 设 V, W 是有限维 \mathbb{R} -线性空间且 $\dim V = \dim W$, $T: V \rightarrow W$ 是 \mathbb{R} -线性映射. 则以下条件等价:

- (1) T 是单射.
- (2) T 是满射.
- (3) T 是线性同构.

证明. 设 $\dim V = \dim W = n$. 由维数公式, $\dim \ker T + \dim \text{im } T = n$.

T 是单射 $\Leftrightarrow \dim \ker T = 0 \Leftrightarrow \dim \text{im } T = n \Leftrightarrow \text{im } T = W$ (因为 $\text{im } T \subseteq W$ 且 $\dim W = n$) $\Leftrightarrow T$ 是满射. \square

推论 4.4. 对于 $A \in M_n(\mathbb{R})$ (方阵), 以下条件等价:

- (1) A 可逆.
- (2) $A\mathbf{x} = \mathbf{0}$ 只有零解 (即 $\ker A = \{\mathbf{0}\}$).
- (3) $A\mathbf{x} = \mathbf{b}$ 对任意 $\mathbf{b} \in \mathbb{R}^n$ 有解 (即 $\text{im } A = \mathbb{R}^n$).
- (4) $\text{rank } A = n$.

证明. (1) \Rightarrow (2): 若 A 可逆且 $A\mathbf{x} = \mathbf{0}$, 则 $\mathbf{x} = A^{-1}\mathbf{0} = \mathbf{0}$. (2) \Leftrightarrow (3) 是推论4.3的矩阵版本. (2) \Leftrightarrow (4): $\ker A = \{\mathbf{0}\}$ 当且仅当 $\text{null}(A) = 0$, 即 $\text{rank } A = n$. (2) \Rightarrow (1): 若 $A\mathbf{x} = \mathbf{0}$ 只有零解, 则 T_A 是双射, 其逆映射也是线性的 (对应 A^{-1}). \square

我们以第一同构定理和一个优美的应用来结束本节.

定理 4.3 (第一同构定理). 设 $T: V \rightarrow W$ 是 \mathbb{R} -线性映射, 则 T 诱导了一个 \mathbb{R} -线性同构

$$\bar{T}: V/\ker T \xrightarrow{\sim} \text{im } T, \quad v + \ker T \mapsto Tv.$$

证明. **良定义性:** 若 $v_1 + \ker T = v_2 + \ker T$, 则 $v_1 - v_2 \in \ker T$, 从而 $Tv_1 = Tv_2$, 因此 \bar{T} 不依赖于陪集代表元的选取.

线性性: $\bar{T}((v_1 + \ker T) + (v_2 + \ker T)) = \bar{T}((v_1 + v_2) + \ker T) = T(v_1 + v_2) = Tv_1 + Tv_2 = \bar{T}(v_1 + \ker T) + \bar{T}(v_2 + \ker T)$. 数乘类似.

单射: 若 $\bar{T}(v + \ker T) = Tv = \mathbf{0}$, 则 $v \in \ker T$, 即 $v + \ker T = \ker T$ (商空间的零向量).

满射: 对任意 $w \in \text{im } T$, 存在 $v \in V$ 使得 $Tv = w$, 从而 $\bar{T}(v + \ker T) = w$. \square

注 4.11. 第一同构定理可以看作维数公式的“结构增强版”: 维数公式告诉我们 $\dim V/\ker T = \dim \text{im } T$, 而第一同构定理进一步说明 $V/\ker T$ 与 $\text{im } T$ 不仅维数相同, 而且作为线性空间是同构的, 这个同构还是典范的 (不依赖于基的选取).

维数公式有许多应用, 我们再次以线性映射的观点来证明 Lagrange 插值定理的存在性和唯一性.

定理 4.4 (Lagrange 插值). 给定 $n+1$ 个互不相同的实数 x_0, \dots, x_n 以及任意 $n+1$ 个数 y_0, \dots, y_n , 则存在唯一的次数 $\leq n$ 的多项式 $f(x)$ 使得 $f(x_i) = y_i, i = 0, 1, \dots, n$.

证明. 考虑 \mathbb{R} -线性映射 (“在给定点处求值”)

$$T: \mathbb{R}[x]_{\leq n} \rightarrow \mathbb{R}^{n+1}$$

$$f \mapsto \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix}.$$

若 $f \in \ker T$, 则 f 是次数 $\leq n$ 的多项式且有 $n+1$ 个不同的零点 x_0, \dots, x_n , 这只能 $f = 0$. 因此 $\ker T = \{0\}$. 由维数公式, $\dim \text{im } T = \dim \mathbb{R}[x]_{\leq n} - \dim \ker T = (n+1) - 0 = n+1 = \dim \mathbb{R}^{n+1}$, 从而 T 是满射 (由推论 4.3, T 也是同构). 这意味着对任意 $(y_0, \dots, y_n)^T \in \mathbb{R}^{n+1}$, 存在唯一的 $f \in \mathbb{R}[x]_{\leq n}$ 使得 $Tf = (y_0, \dots, y_n)^T$. \square

4.5 线性映射下的子空间和商空间

在上一节中, 我们引入了线性映射的核和像, 并利用维数公式和第一同构定理揭示了它们之间的深刻联系. 核和像本身就是特定的子空间, 而在第一章中, 我们已经系统地研究了子空间的直和与商空间. 现在, 我们把这两方面的知识联系起来: 当一个线性映射 T 与空间中原有的子空间结构“相容”时, 它的表示矩阵会呈现出特定的分块形式, 并且 T 可以自然地诱导出商空间之间的映射. 这一观点不仅在理论上非常优美, 也为后续对角化理论的讨论奠定了基础.

设 V, W 是有限维 \mathbb{R} -线性空间, $T: V \rightarrow W$ 是线性映射. 假设 $V_1 \subset V, W_1 \subset W$ 是子空间, 且 T 将 V_1 映入 W_1 , 即 $T(V_1) \subset W_1$.

命题 4.10 (分块上三角表示). 设 $T: V \rightarrow W$ 是线性映射, $V_1 \subset V$, $W_1 \subset W$ 满足 $T(V_1) \subset W_1$. 选取 V_1 的一组基 e_1, \dots, e_r 并扩充为 V 的基 $e_1, \dots, e_r, e_{r+1}, \dots, e_n$; 选取 W_1 的一组基 f_1, \dots, f_s 并扩充为 W 的基 $f_1, \dots, f_s, f_{s+1}, \dots, f_m$. 则 T 在这两组基下的矩阵具有分块上三角形式:

$$[T] = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix},$$

其中 $A_{11} \in M_{s \times r}(\mathbb{R})$ 是限制映射 $T|_{V_1}: V_1 \rightarrow W_1$ 在基 e_1, \dots, e_r 和 f_1, \dots, f_s 下的矩阵.

证明. 对于 $1 \leq j \leq r$, 由 $e_j \in V_1$ 和条件 $T(V_1) \subset W_1$ 知 $T(e_j) \in W_1$. 因此 $T(e_j)$ 可以表示为 W_1 的基 f_1, \dots, f_s 的线性组合, 即 $T(e_j)$ 在 f_{s+1}, \dots, f_m 方向上的坐标全部为零. 这正说明矩阵的左下角 (即第 $s+1$ 行到第 m 行、第 1 列到第 r 列组成的块) 为零矩阵. 而 A_{11} 记录的恰是 $T(e_1), \dots, T(e_r)$ 在 f_1, \dots, f_s 下的坐标, 这正是 $T|_{V_1}$ 的矩阵. \square

例 4.11. 设 $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 由矩阵

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$$

给出 (即 $T(v) = Av$). 取子空间 $V_1 = W_1 = \text{span}\{e_1, e_2\}$ (标准基的前两个向量). 由于

$$T(e_1) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in W_1, \quad T(e_2) = \begin{pmatrix} 2 \\ 4 \\ 0 \end{pmatrix} \in W_1,$$

条件 $T(V_1) \subset W_1$ 成立. 在标准基 e_1, e_2, e_3 下, 矩阵 A 天然具有分块上三角结构:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix}, \quad A_{11} = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}, \quad A_{12} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \quad A_{22} = (6).$$

其中 A_{11} 是限制映射 $T|_{V_1}: V_1 \rightarrow W_1$ 在基 e_1, e_2 下的矩阵, 而 $A_{22} = (6)$ 的意义我们将在下面的命题中解释.

命题 4.11 (商空间上的诱导映射). 设 $T: V \rightarrow W$ 是线性映射, $V_1 \subset V$, $W_1 \subset W$ 满足 $T(V_1) \subset W_1$. 则映射

$$\begin{aligned} \bar{T}: V/V_1 &\rightarrow W/W_1 \\ v + V_1 &\mapsto T(v) + W_1 \end{aligned}$$

是一个良定义的线性映射, 称为 T 在商空间上的**诱导映射** (*induced map*).

证明. **良定义性:** 若 $v + V_1 = v' + V_1$, 即 $v - v' \in V_1$, 则 $T(v - v') = T(v) - T(v') \in T(V_1) \subset W_1$, 从而 $T(v) + W_1 = T(v') + W_1$.

线性性: $\bar{T}((v_1 + V_1) + (v_2 + V_1)) = \bar{T}((v_1 + v_2) + V_1) = T(v_1 + v_2) + W_1 = (T(v_1) + W_1) + (T(v_2) + W_1) = \bar{T}(v_1 + V_1) + \bar{T}(v_2 + V_1)$. 数乘的验证类似. \square

推论 4.5 (诱导映射的矩阵表示). 在命题 4.10 的记号下, 诱导映射 $\bar{T}: V/V_1 \rightarrow W/W_1$ 在商空间的基 $\bar{e}_{r+1}, \dots, \bar{e}_n$ (其中 $\bar{e}_j = e_j + V_1$) 和 $\bar{f}_{s+1}, \dots, \bar{f}_m$ (其中 $\bar{f}_k = f_k + W_1$) 下的矩阵恰好是分块上三角矩阵中的右下角 A_{22} .

证明. 根据命题 3.18, $\bar{e}_{r+1}, \dots, \bar{e}_n$ 构成 V/V_1 的一组基, $\bar{f}_{s+1}, \dots, \bar{f}_m$ 构成 W/W_1 的一组基. 对于 $j > r$, 设

$$T(e_j) = \sum_{i=1}^s a_{ij} f_i + \sum_{k=s+1}^m a_{kj} f_k,$$

则在商空间 W/W_1 中, 由于 $f_1, \dots, f_s \in W_1$ 代表零元素, 有

$$\bar{T}(\bar{e}_j) = T(e_j) + W_1 = \sum_{k=s+1}^m a_{kj} \bar{f}_k.$$

因此 \bar{T} 在上述基下的矩阵恰好由系数 a_{kj} ($k > s, j > r$) 组成, 这正是 A_{22} . □

例 4.12. 我们用求导映射来演示上述结构. 设 $V = \mathbb{R}[x]_{\leq 3}$ (次数 ≤ 3 的多项式), 考虑求导映射 $T: V \rightarrow V, f(x) \mapsto f'(x)$. 取子空间 $V_1 = \mathbb{R}[x]_{\leq 1} = \text{span}\{1, x\}$ (次数 ≤ 1 的多项式). 由于对次数 ≤ 1 的多项式求导得到常数 (次数 $\leq 0 \leq 1$ 的多项式), 我们有 $T(V_1) \subset V_1$.

选取 V_1 的基 $e_1 = 1, e_2 = x$, 扩充为 V 的基 $e_1 = 1, e_2 = x, e_3 = x^2, e_4 = x^3$. 取 $W_1 = V_1$, 则

$$T(1) = 0, \quad T(x) = 1, \quad T(x^2) = 2x, \quad T(x^3) = 3x^2.$$

T 在此基下的矩阵为

$$[T] = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ 0 & A_{22} \end{pmatrix},$$

其中

$$A_{11} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_{12} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}, \quad A_{22} = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}.$$

这里 A_{11} 正是限制映射 $T|_{V_1}$ (对次数 ≤ 1 的多项式求导) 在基 $1, x$ 下的矩阵.

商空间 V/V_1 以 $\bar{e}_3 = x^2 + V_1, \bar{e}_4 = x^3 + V_1$ 为基, 其元素可以理解为“只关注 x^2, x^3 系数”(忽略低次项, 参见例 3.38). 诱导映射 $\bar{T}: V/V_1 \rightarrow V/V_1$ 的作用为:

$$\bar{T}(x^2 + V_1) = 2x + V_1 = V_1 \quad (\text{零元}), \quad \bar{T}(x^3 + V_1) = 3x^2 + V_1.$$

其矩阵正好是 $A_{22} = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$, 验证了推论 4.5.

注 4.12. 继续上面的例子, 在商空间中 $\bar{T}(x^2 + V_1) = V_1$ (零元), 这对应于 $T(x^2) = 2x \in V_1$ 这一事实. 换言之, 虽然 x^2 本身不在 $\ker T$ 中, 但在“模掉 V_1 之后”它被映到了零. 这种现象提示我们: 诱导映射 \bar{T} 的核和像可能与原映射 T 的核和像有所不同. 一般地, 有

$$\ker \bar{T} = \{v + V_1 \mid T(v) \in W_1\} = T^{-1}(W_1)/V_1, \quad \text{im } \bar{T} = (T(V) + W_1)/W_1,$$

这些关系在后续研究不变子空间和对角化时将非常有用.

作为本节的核心应用, 我们利用第一同构定理 (定理 4.3) 来证明矩阵的相抵标准型, 即任何线性映射都可以通过适当选取两端的基使其矩阵化为最简形式.

定理 4.5 (相抵标准型). 设 V, W 是有限维 \mathbb{R} -线性空间, $\dim V = n$, $\dim W = m$, $T: V \rightarrow W$ 是线性映射, $\text{rank } T = r$. 则存在 V 的一组基和 W 的一组基, 使得 T 在这两组基下的矩阵为

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_{m \times n}(\mathbb{R}).$$

证明. 由维数公式 (定理 4.2), $\dim \ker T = n - r$. 取 $\ker T$ 在 V 中的一个直和补空间 U , 即 $V = U \oplus \ker T$, 则 $\dim U = r$.

我们证明 T 限制在 U 上给出了 U 到 $\text{im } T$ 的同构. 一方面, 自然投射 $\pi: V \rightarrow V/\ker T$ 限制在 U 上给出同构 $\pi|_U: U \xrightarrow{\sim} V/\ker T$ (因为 $V = U \oplus \ker T$). 另一方面, 第一同构定理给出同构 $\bar{T}: V/\ker T \xrightarrow{\sim} \text{im } T$. 将二者复合即得

$$T|_U = \bar{T} \circ \pi|_U: U \xrightarrow{\sim} \text{im } T.$$

现在构造所需的基. 选取 U 的一组基 u_1, \dots, u_r , 令 $w_i = T(u_i)$, $i = 1, \dots, r$. 由于 $T|_U$ 是同构, w_1, \dots, w_r 构成 $\text{im } T$ 的一组基. 再选取 $\ker T$ 的一组基 v_1, \dots, v_{n-r} , 并将 w_1, \dots, w_r 扩充为 W 的一组基 $w_1, \dots, w_r, w_{r+1}, \dots, w_m$. 这样:

- (1) V 的基: $u_1, \dots, u_r, v_1, \dots, v_{n-r}$ (先排补空间的基, 再排核的基).
- (2) W 的基: $w_1, \dots, w_r, w_{r+1}, \dots, w_m$ (先排像空间的基, 再扩充).

在这两组基下, T 的作用为

$$T(u_i) = w_i \quad (i = 1, \dots, r), \quad T(v_j) = \mathbf{0} \quad (j = 1, \dots, n - r).$$

因此 T 的矩阵为 $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. □

注 4.13. 相抵标准型的几何含义非常鲜明. 在上述基的选取下, 线性映射 T 被彻底“解耦”为若干独立的一维空间上的行为: 对于 $i = 1, \dots, r$, 一维子空间 $\text{span}\{u_i\} \subset V$ 被同构地映到 $\text{span}\{w_i\} \subset W$, 这对应矩阵对角线上的“1”; 而一维子空间 $\text{span}\{v_j\} \subset \ker T$ 则全部被

映为零, 对应矩阵中的“0”行列. 换句话说, 任何线性映射在适当的基下都可以分解为若干一维同构映射的直和加上一个零映射.

从矩阵的角度看, 相抵标准型意味着: 对任意 $A \in M_{m \times n}(\mathbb{R})$, 存在可逆矩阵 $P \in M_n(\mathbb{R})$ 和 $Q \in M_m(\mathbb{R})$ 使得 $QAP = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$, 这里 $r = \text{rank } A$. 这就是说, **秩是矩阵在相抵变换(即左乘和右乘可逆矩阵)下的完全不变量.**

例 4.13. 设 $T: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ 定义为 $T(x_1, x_2, x_3)^T = (x_1 + x_2, x_1 - x_2)^T$. 我们按照定理 4.5 的证明来具体构造使得矩阵化为标准型的基.

第一步: 求核和秩. $T(x_1, x_2, x_3)^T = \mathbf{0}$ 即 $x_1 + x_2 = 0, x_1 - x_2 = 0$, 解得 $x_1 = x_2 = 0, x_3$ 自由. 因此 $\ker T = \text{span}\{(0, 0, 1)^T\}$, $\dim \ker T = 1, r = \text{rank } T = 3 - 1 = 2$.

第二步: 选取核的补空间. 取 $U = \text{span}\{(1, 0, 0)^T, (0, 1, 0)^T\}$, 则 $\mathbb{R}^3 = U \oplus \ker T$.

第三步: 构造两端的基. 令 $u_1 = (1, 0, 0)^T, u_2 = (0, 1, 0)^T, v_1 = (0, 0, 1)^T$, 则 u_1, u_2, v_1 是 \mathbb{R}^3 的一组基. 计算像:

$$w_1 = T(u_1) = (1, 1)^T, \quad w_2 = T(u_2) = (1, -1)^T.$$

由于 $r = 2 = \dim \mathbb{R}^2$, w_1, w_2 已经构成 \mathbb{R}^2 的一组基 (无需扩充).

验证: 在 \mathbb{R}^3 的基 u_1, u_2, v_1 和 \mathbb{R}^2 的基 w_1, w_2 下, T 的矩阵为

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \end{pmatrix},$$

恰好是秩为 2 的相抵标准型.

4.6 习题

4.6.1 练习题

习题 4.2 (投影映射). 定义线性映射 $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 为

$$T(x, y, z) = (x, y, 0).$$

1. 求 T 的矩阵.
2. 求 $\ker T$ 与 $\text{im } T$ 的一组基.
3. 验证秩-零化度公式.
4. 从几何上解释这个映射把三维空间“压”到了哪里.

习题 4.3 (换基后的表示矩阵). 设 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 在标准基下的矩阵为

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

令 $B = (b_1, b_2)$, 其中 $b_1 = (1, 1)^T$, $b_2 = (1, -1)^T$.

1. 求 $T(b_1)$ 和 $T(b_2)$.
2. 将 $T(b_1), T(b_2)$ 写成基 B 下的坐标.
3. 写出 T 在基 B 下的表示矩阵, 并说明它为什么比 A 更简单.

习题 4.4. 考虑线性映射 $F: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ 使得 $(x_1, x_2, x_3)^T \mapsto (x_1 + 2x_2, x_1 - x_2)^T$. 计算 T 关于以下 \mathbb{R}^3 的基 $\{\alpha_1, \alpha_2, \alpha_3\}$ 以及 \mathbb{R}^2 的基 $\{\beta_1, \beta_2\}$ 对应的矩阵:

1. $\alpha_1 = (1, 0, 0)^T, \alpha_2 = (0, 1, 0)^T, \alpha_3 = (0, 0, 1)^T, \beta_1 = (1, 0)^T, \beta_2 = (0, 1)^T$
2. $\alpha_1 = (1, 1, 1)^T, \alpha_2 = (0, 1, 1)^T, \alpha_3 = (0, 0, 1)^T, \beta_1 = (1, 1)^T, \beta_2 = (1, 0)^T$
3. $\alpha_1 = (1, 2, 3)^T, \alpha_2 = (0, 1, -1)^T, \alpha_3 = (-1, -2, 3)^T, \beta_1 = (1, 2)^T, \beta_2 = (2, 1)^T$

习题 4.5. 令 $B = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \in M_{2 \times 2}(\mathbb{R})$

1. 证明和 B 交换的矩阵 A 的集合 $W = \{A \in M_{2 \times 2}(\mathbb{R}) | AB = BA\}$ 是 \mathbb{R} -线性空间 $M_{2 \times 2}(\mathbb{R})$ 的子空间.
2. 找到 W 的一组基.

习题 4.6. 对于 $A \in M_n(\mathbb{R})$, 证明 $A \cdot A^T$ 的列空间和 A 的列空间相同.

习题 4.7. 令 V 是形如 $AB - BA$ 的矩阵生成的 $M_n(\mathbb{C})$ 的子空间. 证明 $V = \{A | \text{tr}(A) = 0\}$.

习题 4.8. 设 $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 3 \end{bmatrix}$. 考虑线性映射 $f: M_3(\mathbb{R}) \rightarrow M_3(\mathbb{R})$ 满足对 $B \in M_3(\mathbb{R})$ 有 $f(B) = A \cdot B$.

1. 求 A 的 (行) 最简阶梯型.
2. 求 $\text{Ker}(f)$ 作为 \mathbb{R} -线性空间的一组基.
3. 求 $\text{Im}(f)$ 作为 \mathbb{R} -线性空间的一组基.

习题 4.9. 假设 V 是 \mathbb{R} -线性空间 $\mathbb{R}[x]$, 考虑两个线性映射 $T_1, T_2: V \rightarrow V$, 使得 $T_1(f) = f'$ 和 $T_2(f) = xf$. 证明 $T_1 \circ T_2 - T_2 \circ T_1 = I$. 请问在有限维线性空间 V 中是否存在这样的线性映射?

习题 4.10. 假设 l 是二维平面上过原点的直线, 且 l 与横轴的夹角为 θ . 记 T 为以 l 为对称轴的反射. 求线性变换 T 在标准基下的矩阵. 假设另一条二维平面上过原点的直线 l' 与横轴的夹角为 α , 记 T' 为以 l' 为对称轴的反射. 利用线性变化与矩阵乘法的关系, 证明 $T \circ T'$ 是绕原点旋转的线性变换.

习题 4.11. 设 T_i 是 $\mathbb{R}^3 = \{(x_1, x_2, x_3)^T \mid x_i \in \mathbb{R}\}$ 上的线性变换, 定义为绕 x_i 轴旋转角度 π . 请写下这三个变换在标准基下的矩阵并证明 $T_1 \circ T_2$ 仍然是某个旋转变换.

习题 4.12. 证明复数在通常的加法和实数的乘法下做成 \mathbb{R} 线性空间, 且有基 $B: 1, \sqrt{-1}$. 对某一固定的复数 $u + v\sqrt{-1}$, 定义 $T: \mathbb{C} \rightarrow \mathbb{C}$ 为 $T(z) = (u + v\sqrt{-1})z$. 证明 T 是 \mathbb{C} 上的 \mathbb{R} 线性变换并写出 T 在基 B 下的矩阵.

习题 4.13. 找到一个 \mathbb{R}^2 上的线性变换将曲线 C

$$\{(x, y)^T \mid x^2 + 4xy + 10y^2 = 1\}$$

映射为半径为 1 的圆. 再找到一个线性伸缩变换 (必要时可复合旋转) 将这个圆映射为长轴在 x 轴上的椭圆.

习题 4.14. 对于 \mathbb{R}^2 上的线性变换 T , 请找出 $\text{tr}(T^3)$ 和 $\text{tr}(T^2), \text{tr}(T)$ 之间的关系.

习题 4.15. 设 V 是有限维线性空间, $T: V \rightarrow V$ 是线性变换. 证明 T 是可逆的当且仅当 T 的核是 $\{0\}$. 当 V 是无限维线性空间时, 这个结论是否成立?

证明. 假设 V 是有限维线性空间, 则根据维数公式有

$$\dim V = \dim \ker T + \dim \text{im } T.$$

若 $\ker T = \{0\}$, 则 $\dim \text{im } T = \dim V$, 故 $\text{im } T = V$, 即 T 是满射, 从而可逆. 反之若 T 可逆, 则 T 是单射, 故 $\ker T = \{0\}$ 从而 $\ker T = \{0\}$ 当且仅当 $\text{im } T = V$, 这也当且仅当 T 是线性同构.

当 V 是无限维线性空间时, 这个结论不成立: 考虑 $\ell^2 = \{(x_1, x_2, \dots) \mid x_i \in \mathbb{R}\}$ 以及其上的右移位算子 $T: \ell^2 \rightarrow \ell^2$, 定义为:

$$T(x_1, x_2, x_3, \dots) = (0, x_1, x_2, \dots),$$

其核为 $\{0\}$, 但非满射, 故不可逆. □

习题 4.16. 定义 P_n 为关于未定元 x 次数小于或等于 n 的复系数多项式组成的复线性空间. 定义 P_n 上的线性变换 $T: P_n \rightarrow P_n$ 为 $T(f) = f' + f$. 请问这个线性变换是否可逆, 并写下其逆变换.

证明. 任取 $g \in P_n$, 则 $T(f) = f' + f = g$ 等价于

$$\frac{d}{dx}(e^x f(x)) = e^x g.$$

两侧积分有

$$f(x) = e^{-x} \int e^x g + C e^{-x}.$$

由于 $f(x)$ 是多项式, 从而 $C = 0$. 因此当 $g = 0$ 时 $f = 0$, 即 T 是单射.

由于 $g \in P_n$, 从而 g 的 $n+1$ 阶导数为零, 从而分部积分若干次有

$$\int e^x g = e^x \sum_{i=0}^n (-1)^i g^{(i)}(x),$$

从而有逆变换

$$T^{-1}(g) = \sum_{i=0}^n (-1)^i g^{(i)}(x).$$

□

习题 4.17. 假设 A, B 都是 n 阶实矩阵, 且 A 可逆, $B^n = 0$. 证明以下映射 F 是双射

$$\begin{aligned} F: M_n(\mathbb{R}) &\rightarrow M_n(\mathbb{R}) \\ X &\mapsto AX + XB. \end{aligned}$$

证明. 由于 $M_n(\mathbb{R})$ 是有限维线性空间, 所以只需证明 F 是单射即可. 设 $F(X) = 0$, 即 $AX = -XB$. 左乘 A^{-1} 得:

$$X = -A^{-1}XB.$$

重复上述操作 k 次则得到

$$X = (-1)^k A^{-k} X B^k$$

由于 $B^n = 0$, 取 $k = n$, 由 $B^n = 0$ 得 $X = 0$, 这证明了单射性. □

习题 4.18. 假设 V 是 $M_n(\mathbb{R})$ 中的对称矩阵组成的子空间, W 是反对称矩阵组成的子空间. 证明 $V \oplus W = M_n(\mathbb{R})$.

证明. 任意实矩阵 A 可唯一分解为:

$$A = \underbrace{\frac{A + A^T}{2}}_{\text{对称}} + \underbrace{\frac{A - A^T}{2}}_{\text{反对称}}.$$

若 A 既对称又反对称, 则 $A = 0$, 故 $V \cap W = \{0\}$, 且 $V + W = M_n(\mathbb{R})$. □

习题 4.19. 假设 V 是实轴上的全体实值函数组成的线性空间, 其中又子空间 W_1 是全体奇函数组成的线性空间, W_2 是全体偶函数组成的线性空间. 证明 $V = W_1 \oplus W_2$.

证明. 对任意 $f \in V$, 唯一分解:

$$f(x) = \underbrace{\frac{f(x) - f(-x)}{2}}_{\in W_1} + \underbrace{\frac{f(x) + f(-x)}{2}}_{\in W_2}.$$

若 $f \in W_1 \cap W_2$, 则 $f(x) = -f(-x) = f(-x)$, 故 $f(x) = 0$. □

习题 4.20. 假设 T 是实线性空间 V 上的线性变换且满足 $T^2 = I$. 证明 $V = \ker(T - I) \oplus \ker(T + I)$. 这里 I 是恒等变换. 你能用这个事实来解释前两题的结论吗?

证明. 对任意 $v \in V$, 存在分解:

$$v = \underbrace{\frac{v + T(v)}{2}}_{v_1} + \underbrace{\frac{v - T(v)}{2}}_{v_2}.$$

我们断言 $v_1 \in \ker(T - I)$, $v_2 \in \ker(T + I)$. 直接验证如下:

$$(T - I)(v_1) = \frac{T(v) + T^2(v)}{2} - \frac{v + T(v)}{2} = \frac{T(v) + v}{2} - \frac{v + T(v)}{2} = 0.$$

同理 $(T + I)(v_2) = 0$. 若 $v \in \ker(T - I) \cap \ker(T + I)$, 则 $T(v) = v = -v$, 故 $v = 0$. 前两题中:

(1) 取 $T(A) = A^T$, 则 $\ker(T - I)$ 为对称矩阵空间, $\ker(T + I)$ 为反对称矩阵空间;

(2) 取 $T(f)(x) = f(-x)$, 则 $\ker(T - I)$ 为偶函数空间, $\ker(T + I)$ 为奇函数空间;

□

习题 4.21. 假设 T 是有限维线性空间 V 上的线性变换且满足 $T^2 = T$. 证明 $V = \ker T \oplus \operatorname{im} T$.

证明. 分解 $v = (v - T(v)) + T(v)$, 其中:

- $T(v - T(v)) = T(v) - T^2(v) = 0$, 故 $v - T(v) \in \ker T$;
- $T(v) \in \operatorname{im} T$.

若 $u \in \ker T \cap \operatorname{im} T$, 则存在 w 使得 $u = T(w)$ 且 $T(u) = 0$, 于是 $u = T(w) = T^2(w) = T(u) = 0$. □

习题 4.22. 以下假设线性空间的维数均有限. 对于子空间 $W \subset V$, 定义余维数 $\operatorname{codim}(W) = \dim V - \dim W$. 设

$$V_0 \xrightarrow{T_1} V_1 \xrightarrow{T_2} \dots \xrightarrow{T_m} V_m$$

是一串线性映射, 证明

$$\sum_{i=1}^m \dim \ker T_i - \sum_{i=1}^m \operatorname{codim} \operatorname{Im} T_i = \dim V_0 - \dim V_m.$$

证明. 对每个线性映射 $T_i: V_{i-1} \rightarrow V_i$, 根据维数公式有:

$$\dim V_{i-1} = \dim \ker T_i + \dim \operatorname{im} T_i,$$

改写为:

$$\dim \ker T_i - (\dim V_i - \dim \operatorname{im} T_i) = \dim V_{i-1} - \dim V_i.$$

对 $i = 1$ 到 m 累加得:

$$\sum_{i=1}^m \dim \ker T_i - \sum_{i=1}^m \operatorname{codim} \operatorname{im} T_i = \sum_{i=1}^m (\dim V_{i-1} - \dim V_i) = \dim V_0 - \dim V_m.$$

□

习题 4.23. 判断映射 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 是否为线性映射。

$$T(x, y) = (x + y, 2x - y), \quad S(x, y) = (x + 1, y).$$

习题 4.24. 设 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ 满足

$$T(x, y) = (x + y, x - y, 2y).$$

写出 T 在标准基下的矩阵。

习题 4.25. 设

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

把矩阵 A 看成从 \mathbb{R}^3 到 \mathbb{R}^2 的线性映射。求它的核与像空间。

习题 4.26. 设 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 是逆时针旋转 90° 的线性映射。写出 T 的矩阵, 并计算 $T(2, -1)$ 。

习题 4.27. 设

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

分别计算 AB 与 BA , 并解释它们代表的复合映射顺序有何不同。

习题 4.28. 设 $T: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 满足

$$T(x, y, z) = (x + y, y + z, 0).$$

求 $\dim \ker T$, $\dim \operatorname{im} T$, 并验证秩-零化度公式。

习题 4.29. 设 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 在标准基下的矩阵为

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

若换用基 $B = \{(1, 1), (1, -1)\}$, 求 T 在基 B 下的矩阵。

4.6.2 思考题

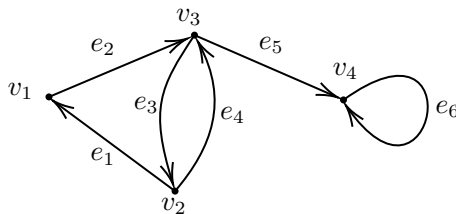
习题 4.30. 设 $G = (V, E)$ 是一个有向图, 带有映射 $s, t: E \rightarrow V$, 其中 $s(e), t(e)$ 分别表示有向边 e 的起点和终点. 记 $\mathbb{R}\{V\}$ 为形如 $\sum_{v \in V} x_v \cdot v$ ($x_v \in \mathbb{R}$) 的表达式构成的线性空间; 类似地有 $\mathbb{R}\{E\}$.

定义线性映射

$$d: \mathbb{R}\{E\} \rightarrow \mathbb{R}\{V\}$$

$$e \mapsto t(e) - s(e),$$

那么 $\dim \ker d, \operatorname{codim} \operatorname{im} d$ 给出了有向图中的什么信息? 尝试对如下例子计算 $\dim \ker d$.



习题 4.31 (幂零扰动下可逆性的传递). 设 V 是复数域 \mathbb{C} 上的 n 维向量空间, $A: V \rightarrow V$ 和 $B: V \rightarrow V$ 是两个线性变换. 已知

$$AB = BA, \quad A \text{ 是幂零算子}, \quad A + B \text{ 可逆}.$$

请问 B 是否也是可逆线性变换? 如果是, 请证明; 如果不是, 请举反例.

习题 4.32 (有限矩阵群的不变向量维数). 设 G 是 $\operatorname{GL}_n(\mathbb{C})$ 的有限子群. 定义不变向量集合

$$V = \{v \in \mathbb{C}^n \mid gv = v, \forall g \in G\}.$$

证明:

$$\dim V = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(g).$$

提示: 考虑线性算子 $P = \frac{1}{|G|} \sum_{g \in G} g$, 并证明 P 是到 V 上的投影算子.

习题 4.33 (特征标理论改编题). 设 G 是 $\operatorname{GL}_n(\mathbb{C})$ 的一个有限子群. 假设对任意 $A \in G$, 若 $A \neq I_n$, 则 $\operatorname{tr}(A) = 0$. 定义

$$T = \sum_{A \in G} A, \quad W = \{x \in \mathbb{C}^n \mid Ax = x, \forall A \in G\}.$$

证明:

1. $T^2 = |G|T$, 且 $\operatorname{im}(T) = W$.
2. 利用上问证明 $|G| \mid n$.

习题 4.34 (交换子与幂零矩阵). 对矩阵 $A, B \in M_n(\mathbb{C})$, 定义交换子 $[A, B] = AB - BA$.

1. 若 $AB - BA = A$, 证明 A 是幂零矩阵。

2. 若 $[A, [A, B]] = 0$, 证明 $[A, B]$ 是幂零矩阵。

习题 4.35 (二维交换子). 对复矩阵 $A, B \in M_n(\mathbb{C})$, 定义 $[A, B] = AB - BA$. 设 $n = 2$. 对任意满足 $\text{tr}(C) = 0$ 的 $C \in M_2(\mathbb{C})$, 是否一定存在 $X, Y \in M_2(\mathbb{C})$ 使得 $[X, Y] = C$? 证明你的结论。

习题 4.36 (Sylvester 方程). 已知 $A \in M_m(\mathbb{C})$ 和 $B \in M_n(\mathbb{C})$ 没有公共特征值. 证明: 对于任意 $C \in M_{m \times n}(\mathbb{C})$, 矩阵方程

$$AX - XB = C$$

有唯一解 $X \in M_{m \times n}(\mathbb{C})$.

习题 4.37 (矩阵空间上的线性方程). 设 V 是二阶实矩阵构成的实线性空间, A 可逆, 且 $\text{tr} A \neq 0$. 考虑线性变换

$$T(X) = AX + XA.$$

判断: 对于每个 $B \in V$, 是否存在唯一的 X 使得 $T(X) = B$? 请证明或给出反例。

5 行列式

在前几章中, 我们建立了线性空间与线性映射的基本理论. 线性映射的一个核心问题是: 给定 $T: V \rightarrow V$, 如何判断 T 是否可逆? 当 $V = \mathbb{R}^n$ 时, 这等价于矩阵 A 是否可逆. 在第一节中我们已经知道 A 可逆当且仅当 $\text{rank } A = n$, 但秩的计算需要行化简, 有时并不方便. 行列式提供了另一个判据: A 可逆当且仅当 $\det A \neq 0$, 而且 $\det A$ 本身携带了丰富的几何信息——它度量了线性映射对“体积”的缩放倍率和定向的改变.

本节我们先从 2×2 有向面积和 3×3 有向体积的几何直观出发, 再把这些直观共同满足的性质抽象为交错多重线性函数的公理. 证明这类函数构成的线性空间恰好是一维后, 我们便得到一般 n 阶行列式的定义. 之后介绍几种常用的计算方法: 按行(列)展开、行变换化三角, 以及伴随矩阵与 Cramer 法则.

在平面几何中, 鞋带公式本质上就是把多边形面积拆成若干个 2×2 行列式. 因而行列式并不是凭空造出来的符号, 而是面积计算中自然出现的量. 在高维中, 它继续扮演统一刻画面积、体积与可逆性的角色.

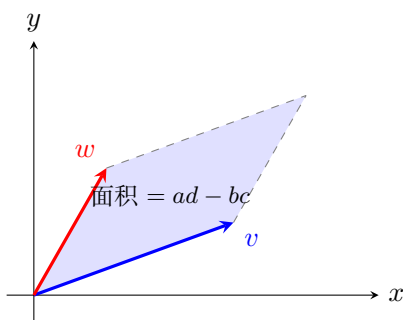
另一方面, 行列式之所以带有正负号, 是因为它还记录定向是否被翻转. 镜像变换保持面积的绝对值, 却会改变左右手系, 因而行列式应为负. 多元积分中的 Jacobian 正是这一思想的局部版本, 它衡量小体积元在局部线性近似下被放大了多少倍.

5.1 定义与基本性质

我们从 2×2 矩阵的情形开始建立直觉. 回忆在注2.4中, 我们有

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

因此 2×2 矩阵可逆当且仅当 $ad - bc \neq 0$. 实际上, $ad - bc$ 有清晰的几何含义. 考虑 \mathbb{R}^2 中由列向量 $v = \begin{pmatrix} a \\ c \end{pmatrix}$ 和 $w = \begin{pmatrix} b \\ d \end{pmatrix}$ 围成的平行四边形. 利用向量外积的计算可以验证, 这个平行四边形的有向面积恰好等于 $ad - bc$: 当 v 到 w 的旋转为逆时针方向时面积为正, 顺时针方向时为负.



在三维空间中, 同样的思想给出由三个列向量 v_1, v_2, v_3 张成的平行六面体的**有向体积**. 如果把这三个向量作为 3×3 矩阵的列, 其有向体积由六项组成: 三项取正号、三项取负号. 这正是后面例5.3中的三阶行列式公式.

我们将要定义的行列式, 就是这种有向面积和有向体积的高维推广: n 阶方阵的行列式等于其 n 个列向量张成的平行体的有向体积.

为了严格地定义行列式, 我们将有向面积所满足的核心代数性质——关于每个变元的线性性以及交换两个变元变号——抽象为公理化定义. 注意下面的定义对任意有限维线性空间 V 给出, 而不仅限于 \mathbb{R}^n .

定义 5.1. 设 V 是 n 维 \mathbb{R} -线性空间. V 上的 n 次**交错多重线性函数** (*alternating multilinear function*)是函数

$$f: \underbrace{V \times \cdots \times V}_{n \uparrow} \rightarrow \mathbb{R}$$

满足如下条件:

(1) (**多重线性**) 对每个 i , 固定其余变元后, f 关于第 i 个变元是 \mathbb{R} -线性的, 即

$$f(v_1, \dots, cv_i + c'v'_i, \dots, v_n) = cf(v_1, \dots, v_i, \dots, v_n) + c'f(v_1, \dots, v'_i, \dots, v_n).$$

(2) (**交错性**) 交换任意两个变元, 函数值变号:

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j, \dots, v_i, \dots, v_n).$$

所有 V 上的 n 次交错多重线性函数在逐点加法和数乘下构成 \mathbb{R} -线性空间, 记为 $\text{Alt}^n(V)$.

注 5.1. 交错性有如下直接推论: 如果 $v_i = v_j (i \neq j)$, 则 $f(v_1, \dots, v_n) = 0$. 事实上, 交换第 i 和第 j 个变元后函数值变号, 但变元不变, 因此 $f = -f$, 即 $f = 0$. 进而, 如果 v_1, \dots, v_n 线性相关, 则 $f(v_1, \dots, v_n) = 0$ (用多重线性将某个 v_i 展开为其他向量的线性组合, 化为有两列相同的情形).

下面的定理说明, 交错多重线性函数在本质上是唯一的——空间 $\text{Alt}^n(V)$ 恰好是一维的.

定理 5.1. 设 V 是 n 维 \mathbb{R} -线性空间, 则 $\dim_{\mathbb{R}} \text{Alt}^n(V) = 1$.

证明. 对维数 n 进行归纳.

$n = 1$ 时. 根据定义, $\text{Alt}^1(V)$ 即为所有的 $V \rightarrow \mathbb{R}$ 的线性函数组成的空间, 即对偶空间 V^* . 由 $\dim V = 1$ 可知 $\dim \text{Alt}^1(V) = \dim V^* = 1$, 结论成立.

归纳步骤. 设 $n \geq 2$, 并假设对任何 $(n-1)$ 维的线性空间结论均成立.

给定 n 维线性空间 V , 任取非零向量 $v \in V$, 并考虑商空间 $W = V / \text{span}_{\mathbb{R}}\{v\}$. 因商空间的维数为 $\dim V - \dim \text{span}_{\mathbb{R}}\{v\}$, 故 $\dim W = n - 1$. 对任意 $x \in V$, 我们将其在商空间中的等价类记作 $[x] := x + \text{span}_{\mathbb{R}}\{v\}$.

定义映射

$$\Phi: \text{Alt}^n(V) \rightarrow \text{Alt}^{n-1}(W)$$

如下: 对于任意 $f \in \text{Alt}^n(V)$, 我们定义它在 W 上的函数 $\Phi(f)$ 为给第一变元填充 v 后得到的下降一阶的函数: 即对任意 $n-1$ 个代表元 $x_2, \dots, x_n \in V$, 定义

$$\Phi(f)([x_2], \dots, [x_n]) := f(v, x_2, \dots, x_n).$$

首先, Φ 是良好定义的线性映射. 我们需要验证 $\Phi(f)$ 的取值不依赖于代表元 x_i 的选取. 对于某个 x_i , 如果将其替换为同一个等价类中的另一个代表元 $x_i + cv$, 由多重线性可知:

$$f(v, \dots, x_i + cv, \dots, x_n) = f(v, \dots, x_i, \dots, x_n) + cf(v, \dots, v, \dots, x_n).$$

由于后者的参数中有两个 v (分别位于第 1 个变元和原先 x_i 的位置), 由 f 的交错性 (注5.1) 可知其值为 0. 故而代表元的选取不改变函数值. 此外, 容易验证 $\Phi(f)$ 继承了 f 的多重线性和交错性, 从而确实有 $\Phi(f) \in \text{Alt}^{n-1}(W)$; Φ 自身的线性性也极显然.

其次, Φ 是单射. 设 $f \in \ker \Phi$, 意即对所有 $x_2, \dots, x_n \in V$ 均有 $f(v, x_2, \dots, x_n) = 0$. 我们想证明 $f = 0$.

任意取定 V 上满足 $\lambda(v) = 1$ 的线性函数 $\lambda \in V^*$. 则 V 可分解为 $V = \text{span}_{\mathbb{R}}\{v\} \oplus U$, 其中 $U = \ker \lambda$ 是一个 $(n-1)$ 维子空间. 对任意一组变元 $y_1, \dots, y_n \in V$, 我们可将其分解为 $y_i = c_i v + u_i$, 其中 $u_i \in U$. 将它们代入 $f(y_1, \dots, y_n)$ 中展开, 根据多重线性可以得到 2^n 项的和, 每一项都会是从 $\{c_i v, u_i\}$ 中各选一个变元求 f .

- 若在这 n 个选择中至少选出一个位于 v 方向上的分量 $c_i v$, 则可利用交错性将含有 v 的那一变元挪到第一位. 由于 $f(v, \dots) \equiv 0$, 该项必定为 0.
- 若在此 n 个选择中全为 U 中的分量 (即 $f(u_1, \dots, u_n)$), 由于此时所有 u_i 皆属于 $(n-1)$ 维的 U , 根据维数这 n 个向量必线性相关. 再次利用注5.1, f 此时的值亦为 0.

综上可得对于所有的 y_1, \dots, y_n , 都有 $f(y_1, \dots, y_n) = 0$, 即 $f = 0$, Φ 即是单射.

最后, Φ 是满射. 我们通过构造 Φ 的右逆证明其为满射. 仍利用刚才满足 $\lambda(v) = 1$ 的线性函数 $\lambda \in V^*$. 定义

$$\Psi: \text{Alt}^{n-1}(W) \rightarrow \text{Alt}^n(V)$$

如下: 对于 $g \in \text{Alt}^{n-1}(W)$ 及任意向量 $x_1, \dots, x_n \in V$,

$$\Psi(g)(x_1, \dots, x_n) := \sum_{i=1}^n (-1)^{i-1} \lambda(x_i) g([x_1], \dots, \widehat{[x_i]}, \dots, [x_n]),$$

其中 $\widehat{[x_i]}$ 表示将其从函数变元中删去. 可以验证 $\Psi(g)$ 是多重线性的, 且如果相邻变元 $x_k = x_{k+1}$, 求和式中有可能非零的唯有第 k 项与第 $k+1$ 项. 由于该两项所含带的 g 变元序

列完全相同, 而前面的常数 $\pm\lambda(x_k)$ 正好互为相反数, 它们求和恰好抵消为 0, 故而 $\Psi(g)$ 保留了交错性.

我们把 $\Psi(g)$ 代入 Φ 的定义中, 并计算 $\Psi(g)(v, x_2, \dots, x_n)$. 由于 $[v] = [0]$, 那些变元序列中包含 $[v]$ 的项都会因多重线性化为 0. 在求和式的 n 项中, 唯一不包含 $[x_1] = [v]$ 的只有 $i = 1$ 的一项. 故而:

$$\Phi(\Psi(g))([x_2], \dots, [x_n]) = \Psi(g)(v, x_2, \dots, x_n) = (-1)^0 \lambda(v) g([x_2], \dots, [x_n]) = g([x_2], \dots, [x_n]).$$

这意味着 $\Phi \circ \Psi = I_{\text{Alt}^{n-1}(W)}$, 因此 Φ 确是满射.

因 Φ 是双射, 从而构成线性空间同构. 进而可得

$$\dim \text{Alt}^n(V) = \dim \text{Alt}^{n-1}(W).$$

由归纳假设, $(n-1)$ 维商空间满足 $\dim \text{Alt}^{n-1}(W) = 1$, 由此推得 $\dim \text{Alt}^n(V) = 1$. \square

注 5.2. 上述定理表明, 交错多重线性函数本质上是唯一的: 一旦取定基, 它完全由其在该基上的值唯一确定.

利用 $\dim \text{Alt}^n(\mathbb{R}^n) = 1$, 我们可以自然地定义行列式.

定义 5.2. \mathbb{R}^n 上的行列式 (determinant) 是 $\text{Alt}^n(\mathbb{R}^n)$ 中唯一满足归一化条件

$$f(e_1, \dots, e_n) = 1$$

的交错多重线性函数. 对于 $A \in M_n(\mathbb{R})$, 记 $A = (v_1, \dots, v_n)$, 则 A 的行列式定义为

$$\det A = |A| := f(v_1, \dots, v_n).$$

注 5.3. 行列式的存在唯一性直接由定理 5.1 保证: 因为 $\dim \text{Alt}^n(\mathbb{R}^n) = 1$ 且该空间非零, 取任意非零元素 $g \in \text{Alt}^n(\mathbb{R}^n)$, 则 $g(e_1, \dots, e_n) \neq 0$ (否则对所有向量 $g = 0$, 与 $g \neq 0$ 矛盾), 从而 $f := g/g(e_1, \dots, e_n)$ 是唯一满足归一化的元素.

注 5.4. 利用多重线性和交错性, 将各列向量按标准基 $v_i = \sum_{j=1}^n a_{ji} e_j$ 展开, 也不难推导出行列式的置换求和公式:

$$\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(i), i},$$

其中 S_n 是 n 元置换群, $\text{sgn}(\sigma)$ 是置换 σ 的符号 (+1 或 -1). 此公式亦可作为行列式的直接定义.

补充: 排列与逆序数

上述置换求和公式中用到了排列的符号 $\text{sgn}(\sigma)$, 我们在此给出其严格定义.

设 $\sigma = (\sigma(1), \sigma(2), \dots, \sigma(n))$ 是集合 $\{1, 2, \dots, n\}$ 的一个排列, 即 σ 是该集合的一个双射到自身的映射. 我们关心排列中元素的“顺序混乱程度”, 这通过逆序数来量化.

定义 5.3 (逆序与逆序数). 对于排列 σ , 若存在一对指标 (i, j) 满足

$$1 \leq i < j \leq n \quad \text{且} \quad \sigma(i) > \sigma(j),$$

则称 $(\sigma(i), \sigma(j))$ 构成一个**逆序** (*inversion*). 排列 σ 的**逆序数**定义为其中逆序的总数, 记作:

$$\tau(\sigma) = \#\{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}.$$

例如, 排列 $(3, 1, 4, 2)$ 中的逆序对为 $(3, 1), (3, 2), (4, 2)$, 故 $\tau = 3$.

逆序数反映了排列相对于自然顺序 $(1, 2, \dots, n)$ 的“偏离程度”。特别地, 恒等排列 $(1, 2, \dots, n)$ 的逆序数为 0, 而完全倒序排列 $(n, n-1, \dots, 1)$ 的逆序数达到最大值 $\frac{n(n-1)}{2}$ 。

定义 5.4 (排列的奇偶性与符号). 若 $\tau(\sigma)$ 为偶数, 则称排列 σ 为**偶排列**; 若为奇数, 则称为**奇排列**。排列的**符号** (*sign*) 定义为

$$\text{sgn}(\sigma) = (-1)^{\tau(\sigma)}.$$

排列的奇偶性在行列式理论中具有核心作用, 因为行列式的置换求和公式中每一项的符号由对应排列的奇偶性决定。

定理 5.2 (对换改变奇偶性). 对任意排列 σ , 若对其施行一次**对换** (即交换两个位置上的元素, 其余不变), 得到新排列 σ' , 则

$$\tau(\sigma') \equiv \tau(\sigma) + 1 \pmod{2},$$

即对换总是改变排列的奇偶性。

证明. 任意对换可分解为奇数个相邻对换, 而每次相邻对换恰好改变逆序数 ± 1 , 因此总奇偶性改变。 \square

推论 5.1. 任意排列均可由恒等排列经有限次对换得到, 且所需对换次数的奇偶性唯一确定, 即等于 $\tau(\sigma) \pmod{2}$ 。因此 $\text{sgn}(\sigma)$ 是良好定义的。

例 5.1. 当 $n = 1$ 时, $\det(a) = a$. 当 $n = 2$ 时,

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc,$$

这正是我们在开头从几何直觉得到的有向面积公式。

例 5.2 (二阶行列式的计算). 例如

$$\det \begin{pmatrix} 3 & 1 \\ 2 & 5 \end{pmatrix} = 3 \cdot 5 - 1 \cdot 2 = 13.$$

它表示由向量 $(3, 2)^T$ 和 $(1, 5)^T$ 张成的平行四边形的有向面积. 若交换两列,

$$\det \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} = 1 \cdot 2 - 3 \cdot 5 = -13,$$

面积大小不变, 但定向反过来了.

例 5.3. 当 $n = 3$ 时, 利用置换求和公式 (S_3 有 6 个元素) 可得

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

注 5.5. 上述 3×3 行列式公式又被称为 **Sarrus 法则**(对角线法则): 三条”主对角线方向”的乘积取正号, 三条”副对角线方向”的乘积取负号. 需要注意的是, 这个法则**仅对** $n \leq 3$ **成立**, 对 $n \geq 4$ 没有类似的简单模式.

例 5.4 (三阶行列式的计算). 利用上面的公式,

$$\begin{aligned} \det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ 2 & 0 & 1 \end{pmatrix} &= 1 \cdot 3 \cdot 1 + 2 \cdot 1 \cdot 2 + 0 \cdot 0 \cdot 0 \\ &\quad - 0 \cdot 3 \cdot 2 - 2 \cdot 0 \cdot 1 - 1 \cdot 1 \cdot 0 \\ &= 7. \end{aligned}$$

习题 5.1. 计算下列行列式:

$$\det \begin{pmatrix} 4 & -1 \\ 2 & 3 \end{pmatrix}, \quad \det \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}.$$

例 5.5. 对于三种初等矩阵⁵, 其行列式分别为

$$(E1) \det E[i, j] = -1.$$

$$(E2) \det E[i, c] = c.$$

$$(E3) \det E[i, j, c] = 1.$$

特别地, 对于矩阵 A 以及初等矩阵 E , 有 $|AE| = |A||E|$.

命题 5.1. 行列式有如下性质:

⁵见定义2.6

- (1) 如果 A 的某一列为零, 则 $|A| = 0$.
- (2) $|A| \neq 0$ 当且仅当 $\text{rank } A = n$.
- (3) $|\mathbf{I}_n| = 1$.
- (4) $|AB| = |A||B|$.
- (5) $|A^{-1}| = |A|^{-1}, |PAP^{-1}| = |A|$.
- (6) $|A| = |A^T|$.
- (7) 假设 A 是分块上三角矩阵, 并且对角线分块矩阵为 A_1, \dots, A_n , 则 $|A| = |A_1| \dots |A_n|$.
特别地, 如果 A 是上三角矩阵, 并且对角线元素为 a_1, \dots, a_n , 则 $|A| = a_1 \dots a_n$.

证明. (1). 由行列式的多重线性 (定义5.1(1)) 即可.

(2). 设 A 的列向量为 v_1, \dots, v_n . 若 $\text{rank } A < n$, 则 v_1, \dots, v_n 线性相关, 由注5.1可知 $|A| = 0$. 反过来, 若 $\text{rank } A = n$, 则 v_1, \dots, v_n 是一组基. 由于 $\text{Alt}^n(\mathbb{R}^n)$ 是一维空间, 归一化后的行列式在任何一组基上的取值都不能为 0, 否则它在该基展开的所有 n 重输入上都为 0, 与 $\det(e_1, \dots, e_n) = 1$ 矛盾. 因此 $|A| \neq 0$.

(3). 由行列式的归一化条件 (定义5.2) 即可.

(4). 固定 A , 定义

$$g(x_1, \dots, x_n) = \det(Ax_1, \dots, Ax_n).$$

则 g 仍是 \mathbb{R}^n 上的交错多重线性函数. 由 $\dim \text{Alt}^n(\mathbb{R}^n) = 1$ 可知

$$g(x_1, \dots, x_n) = g(e_1, \dots, e_n) \det(x_1, \dots, x_n) = |A| \det(x_1, \dots, x_n).$$

取 x_1, \dots, x_n 为 B 的列向量, 即得 $|AB| = |A||B|$.

(5). 由 $AA^{-1} = \mathbf{I}_n$ 和 (4) 可得 $|A||A^{-1}| = 1$. 相似不变性由

$$|PAP^{-1}| = |P||A||P^{-1}| = |A|$$

直接推出.

(6). 由置换求和公式,

$$|A^T| = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{i, \sigma(i)}.$$

令 $\tau = \sigma^{-1}$, 则 $\text{sgn}(\tau) = \text{sgn}(\sigma)$, 且上式化为

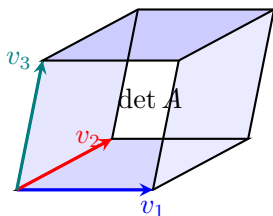
$$\sum_{\tau \in S_n} \text{sgn}(\tau) \prod_{j=1}^n a_{\tau(j), j} = |A|.$$

(7). 只需对两个对角分块证明, 多个分块由归纳得到. 设

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix},$$

其中 B 为 $r \times r$ 矩阵, D 为 $s \times s$ 矩阵. 在置换求和公式中, 若某个 $i > r$ 被送到 $\sigma(i) \leq r$, 则对应元素位于左下零块, 该项为 0. 因此非零项只能来自同时保持前 r 个指标集合和后 s 个指标集合的置换, 它们分别给出 B 和 D 的行列式. 故 $|A| = |B||D|$. 特别地, 上三角矩阵是所有对角分块均为 1×1 的情形. \square

注 5.6 (行列式的几何意义). 行列式的绝对值 $|\det A|$ 等于 A 的 n 个列向量 v_1, \dots, v_n 在 \mathbb{R}^n 中张成的平行体 (parallelepiped) 的 n 维体积, 而 $\det A$ 的符号反映了 (v_1, \dots, v_n) 相对于标准基 (e_1, \dots, e_n) 的定向 (orientation): 正号表示同向, 负号表示反向. 换言之, 线性映射 T 将标准单位体积缩放为 $|\det T|$ 倍, 并且当 $\det T < 0$ 时翻转定向.



定义 5.5. 给定 \mathbb{R} -线性空间 V 以及 \mathbb{R} -线性映射 $T: V \rightarrow V$, 则 T 的行列式 (determinant) 定义为 $\det A$, 其中 A 是 T 在任意一组基下的矩阵.

注 5.7. 线性映射的行列式是良好定义的, 因为同一个线性映射在不同基下的矩阵之间是相似的, 而根据命题 5.1 中的 (5) 可知相似的矩阵有着相同的行列式.

补充: 秩的子式刻画

利用行列式, 我们可以给出矩阵秩的另一种等价定义. 回忆矩阵 $A \in M_{m \times n}(\mathbb{R})$ 的秩 $\text{rank}(A)$ 在前面是通过最简行阶梯型的主元个数来定义的. 现在利用行列式的工具, 我们有如下等价刻画:

命题 5.2. 矩阵 $A \in M_{m \times n}(\mathbb{R})$ 的秩 $\text{rank}(A)$ 等于其非零子式的最高阶数. 即,

$$\text{rank}(A) = \max\{k \mid A \text{ 存在 } k \text{ 阶子式不为零}\}.$$

若 $A = 0$, 则 $\text{rank}(A) = 0$.

证明. 设 $\text{rank}(A) = r$. 先证明存在 r 阶非零子式. 由于列秩为 r , 可在 A 的列中取出 r 个线性无关列, 组成 $m \times r$ 矩阵 B . 矩阵 B 的列秩为 r , 因而它的行空间维数也为 r ; 于是可在

B 的行中取出 r 个线性无关行. 这些行和原先选出的 r 列交叉得到一个 $r \times r$ 子矩阵, 其行(或列)线性无关, 故行列式非零.

另一方面, 若取 A 的任意 $(r+1)$ 阶子矩阵, 其行向量仍来自 A 的行向量. 因为 A 的行空间维数为 r , 这 $r+1$ 个行向量必线性相关, 所以该子矩阵行列式为零. 因此非零子式的最高阶数恰为 r . \square

5.2 行列式的计算方法

接下来我们介绍计算矩阵行列式的常用方法.

按列展开

最基本的方法是**按列展开** (cofactor expansion along a column). 我们先推导按第一列展开的公式, 再推广到任意列和任意行.

给定 $A = (a_{ij})_{n \times n} \in M_n(\mathbb{R})$, 我们记 $A = (v_1, \dots, v_n)$ 为 A 的列向量分解. 对第一列 v_1 利用多重线性性展开:

$$\begin{aligned} \det A &= f(v_1, v_2, \dots, v_n) \\ &= f(a_{11}e_1 + \dots + a_{n1}e_n, v_2, \dots, v_n) \\ &= \sum_{i=1}^n a_{i1} f(e_i, v_2, \dots, v_n). \end{aligned}$$

现在我们来计算 $f(e_i, v_2, \dots, v_n)$. 对于 $k = 2, \dots, n$, 将 v_k 中 e_i 方向上的分量减去, 记 $v'_k = v_k - a_{ik}e_i$. 则 v'_k 属于 $W := \text{span}_{\mathbb{R}}\{e_1, \dots, \widehat{e}_i, \dots, e_n\} \cong \mathbb{R}^{n-1}$. 由交错性, $f(e_i, v_2, \dots, v_n) = f(e_i, v'_2, \dots, v'_n)$. 考虑函数

$$\begin{aligned} g: \underbrace{W \times \dots \times W}_{n-1 \text{ 个}} &\rightarrow \mathbb{R}, \\ (w_1, \dots, w_{n-1}) &\mapsto f(e_i, w_1, \dots, w_{n-1}). \end{aligned}$$

可以直接验证 g 是 $W \cong \mathbb{R}^{n-1}$ 上的交错多重线性函数. 取 W 的标准有序基 $(e_1, \dots, \widehat{e}_i, \dots, e_n)$, 我们有

$$g(e_1, \dots, \widehat{e}_i, \dots, e_n) = f(e_i, e_1, \dots, \widehat{e}_i, \dots, e_n) = (-1)^{i-1} \det I_n = (-1)^{i-1},$$

其中最后一步将 e_i 从第 1 个位置移到第 i 个位置, 需要 $i-1$ 次对换. 由 $\dim \text{Alt}^{n-1}(W) = 1$ (定理 5.1), g 由其在基上的值唯一确定, 即 $g = (-1)^{i-1} \det_{n-1}$, 因此

$$f(e_i, v'_2, \dots, v'_n) = (-1)^{i-1} \det(M_{i1}) = (-1)^{i+1} |M_{i1}|,$$

其中 M_{i1} 是由矩阵 A 去掉第 i 行和第 1 列得到的 $(n-1) \times (n-1)$ 矩阵. 于是得到**按第一列展开公式**:

$$|A| = \sum_{i=1}^n (-1)^{i+1} a_{i1} |M_{i1}|.$$

注 5.8. 回顾在证明 $\dim \text{Alt}^n(V) = 1$ (定理 5.1) 时, 当我们建立自 $\text{Alt}^n(V)$ 到 $\text{Alt}^{n-1}(W)$ 的满射时所构造的右逆映射 Ψ , 其实质正是行列式的行(列)展开公式在一般线性空间上的抽象表达: 选取一个分量并按其次维度的交错多重线性函数“展开”. 这种降维度的计算技巧是交错多重线性函数的内禀属性.

完全类似地, 对第 j 列展开可得 $|A| = \sum_{i=1}^n (-1)^{i+j} a_{ij} |M_{ij}|$, 其中 M_{ij} 是 A 去掉第 i 行和第 j 列后的矩阵. 另一方面, 利用 $|A| = |A^T|$, 对 A^T 按列展开即得 A 的**按行展开公式**: 对任意 $i = 1, \dots, n$, $|A| = \sum_{j=1}^n (-1)^{i+j} a_{ij} |M_{ij}|$.

我们将上述展开中反复出现的量定义如下.

定义 5.6. 给定 $A = (a_{ij})_{n \times n} \in M_n(\mathbb{R})$.

1. 矩阵 A 去掉第 i 行和第 j 列得到的 $(n-1) \times (n-1)$ 矩阵记为 M_{ij} , 其行列式 $|M_{ij}|$ 被称为 A 的 (i, j) **余子式 (minor)**.
2. A 的 (i, j) **代数余子式 (cofactor)** 定义为 $C_{ij} := (-1)^{i+j} |M_{ij}|$.

利用上述记号, 余子式展开公式可以简洁地表述为:

命题 5.3 (余子式展开). 给定 $A = (a_{ij})_{n \times n} \in M_n(\mathbb{R})$, 则对任意 $j = 1, \dots, n$ (按第 j 列展开) 有

$$|A| = \sum_{i=1}^n a_{ij} C_{ij} = \sum_{i=1}^n (-1)^{i+j} a_{ij} |M_{ij}|;$$

对任意 $i = 1, \dots, n$ (按第 i 行展开) 有

$$|A| = \sum_{j=1}^n a_{ij} C_{ij} = \sum_{j=1}^n (-1)^{i+j} a_{ij} |M_{ij}|.$$

注 5.9. 余子式展开将 n 阶行列式的计算递归地归结为 n 个 $(n-1)$ 阶行列式的计算. 实际计算时, 通常选取含最多零元素的行或列进行展开以减少计算量.

例 5.6. 计算行列式

$$A = \begin{pmatrix} 2 & 1 & 0 & 3 \\ 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -2 \\ 4 & 0 & -1 & 1 \end{pmatrix}.$$

选取第三行 (含一个零元素) 按行展开:

$$|A| = 0 \cdot C_{31} + 3 \cdot C_{32} + 1 \cdot C_{33} + (-2) \cdot C_{34}.$$

逐个计算三阶余子式:

$$C_{32} = (-1)^{3+2} \begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 0 \\ 4 & -1 & 1 \end{vmatrix} = -(2 \cdot 2 \cdot 1 + 0 \cdot 0 \cdot 4 + 3 \cdot 1 \cdot (-1) - 4 \cdot 2 \cdot 3 - (-1) \cdot 0 \cdot 2 - 1 \cdot 1 \cdot 0)$$

$$= -(4 + 0 - 3 - 24 - 0 - 0) = -(-23) = 23,$$

$$C_{33} = (-1)^{3+3} \begin{vmatrix} 2 & 1 & 3 \\ 1 & -1 & 0 \\ 4 & 0 & 1 \end{vmatrix} = 2(-1 - 0) - 1(1 - 0) + 3(0 + 4) = -2 - 1 + 12 = 9,$$

$$C_{34} = (-1)^{3+4} \begin{vmatrix} 2 & 1 & 0 \\ 1 & -1 & 2 \\ 4 & 0 & -1 \end{vmatrix} = -(2(1 - 0) - 1(-1 - 8) + 0) = -(2 + 9) = -11.$$

因此 $|A| = 3 \times 23 + 1 \times 9 + (-2) \times (-11) = 69 + 9 + 22 = 100$.

行化简法

另一种常用的计算方法利用行列式在初等行变换下的行为. 由行列式的性质 (命题5.1), 行列式的计算可以通过以下策略进行:

1. 交换两行: 行列式变号;
2. 某行乘以常数 c : 行列式变为 c 倍;
3. 某行加上另一行的 c 倍: 行列式不变.

利用 Gauss 消元法将矩阵化为上三角, 此时行列式等于对角线元素之积 (乘以交换行带来的符号因子).

例 5.7. 用行化简法重新计算上例中的行列式:

$$\begin{vmatrix} 2 & 1 & 0 & 3 \\ 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -2 \\ 4 & 0 & -1 & 1 \end{vmatrix} \xrightarrow{r_1 \leftrightarrow r_2} - \begin{vmatrix} 1 & -1 & 2 & 0 \\ 2 & 1 & 0 & 3 \\ 0 & 3 & 1 & -2 \\ 4 & 0 & -1 & 1 \end{vmatrix}$$

$$\begin{aligned}
& \xrightarrow{\substack{r_2-2r_1 \\ r_4-4r_1}} - \begin{vmatrix} 1 & -1 & 2 & 0 \\ 0 & 3 & -4 & 3 \\ 0 & 3 & 1 & -2 \\ 0 & 4 & -9 & 1 \end{vmatrix} \xrightarrow{r_3-r_2} - \begin{vmatrix} 1 & -1 & 2 & 0 \\ 0 & 3 & -4 & 3 \\ 0 & 0 & 5 & -5 \\ 0 & 4 & -9 & 1 \end{vmatrix} \\
& \xrightarrow{r_4-\frac{4}{3}r_2} - \begin{vmatrix} 1 & -1 & 2 & 0 \\ 0 & 3 & -4 & 3 \\ 0 & 0 & 5 & -5 \\ 0 & 0 & -\frac{11}{3} & -3 \end{vmatrix} \xrightarrow{r_4+\frac{11}{15}r_3} - \begin{vmatrix} 1 & -1 & 2 & 0 \\ 0 & 3 & -4 & 3 \\ 0 & 0 & 5 & -5 \\ 0 & 0 & 0 & -\frac{20}{3} \end{vmatrix} \\
& = -1 \times 3 \times 5 \times \left(-\frac{20}{3}\right) = 100.
\end{aligned}$$

例 5.8 (Vandermonde 行列式). 对于 $x_1, \dots, x_n \in \mathbb{R}$, **Vandermonde 行列式** 定义为

$$V_n = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

证明. 对 n 进行归纳. $n = 1$ 时 $V_1 = 1$, 结论成立. $n = 2$ 时 $V_2 = x_2 - x_1$, 结论成立. 设 $n \geq 3$, 假设 $n - 1$ 时结论成立. 对 V_n 从最后一行开始, 依次用第 k 行减去 x_1 乘以第 $k - 1$ 行 ($k = n, n - 1, \dots, 2$), 得到

$$V_n = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & x_2 - x_1 & \cdots & x_n - x_1 \\ 0 & x_2(x_2 - x_1) & \cdots & x_n(x_n - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & x_2^{n-2}(x_2 - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{vmatrix}.$$

按第一列展开, 并从第 j 列提取公因子 $(x_j - x_1)$ ($j = 2, \dots, n$), 得

$$V_n = \prod_{j=2}^n (x_j - x_1) \cdot V_{n-1}(x_2, \dots, x_n) = \prod_{j=2}^n (x_j - x_1) \cdot \prod_{2 \leq i < j \leq n} (x_j - x_i) = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

□

注 5.10. Vandermonde 行列式的一个直接推论是: $V_n \neq 0$ 当且仅当 x_1, \dots, x_n 两两不同. 这一结论在多项式插值理论中有重要应用.

分块矩阵的行列式

对于分块矩阵, 行列式的计算有以下有用的结果.

命题 5.4. 设 $2n \times 2n$ 阶矩阵

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

其中 A, B, C, D 均为 $n \times n$ 阶矩阵. 若 $AC = CA$, 则 $|M| = |AD - CB|$.

证明. 首先我们假设 A 可逆, 则

$$\begin{aligned} |M| &= \left| \begin{pmatrix} A & B \\ 0 & D - CA^{-1}B \end{pmatrix} \right| \\ &= |A| |D - CA^{-1}B| \\ &= |A(D - CA^{-1}B)| \\ &= |AD - CB| \end{aligned}$$

而当 A 不可逆时, 我们不妨考虑 $A_\lambda = A + \lambda I$. 由于 $|A_\lambda|$ 是 λ 的 n 次多项式, 从而对有限多个 λ 之外 A_λ 总可逆, 因此我们不妨取足够小的 λ 使得 A_λ 总可逆, 根据可逆时的情形我们有

$$\left| \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix} \right| = |A_\lambda D - CB|.$$

从而我们令 $\lambda \rightarrow 0$ 即有我们期待的结果⁶. □

5.3 伴随矩阵

利用代数余子式, 我们可以构造一个与逆矩阵密切相关的矩阵.

定义 5.7. 对于 $A = (a_{ij})_{n \times n} \in M_n(\mathbb{R})$, A 的**伴随矩阵** (*adjugate matrix*) A^* 定义为以代数余子式为元素的矩阵的转置:

$$(A^*)_{ij} := C_{ji} = (-1)^{i+j} |M_{ji}|.$$

换言之, A^* 的第 i 行第 j 列元素是 A 的 (j, i) 代数余子式.

注 5.11. 注意伴随矩阵定义中的转置: $(A^*)_{ij} = C_{ji}$, 而不是 C_{ij} . 这个转置是使得 $AA^* = (\det A)I_n$ 成立的关键.

⁶这个操作称为微扰法, 是矩阵中一个非常经典的技巧. 在 §6.7 中, 我们将用有理函数域的方法将微扰法“代数化”, 使其对任意域 (包括有限域) 都成立.

例 5.9. 设 $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{pmatrix}$, 则 $\det A = 1(0 - 24) - 2(0 - 20) + 3(0 - 5) = 1$. 计算各代数

余子式:

$$C_{11} = -24, \quad C_{12} = 20, \quad C_{13} = -5,$$

$$C_{21} = 18, \quad C_{22} = -15, \quad C_{23} = 4,$$

$$C_{31} = 5, \quad C_{32} = -4, \quad C_{33} = 1.$$

于是伴随矩阵为 (取代数余子式矩阵的转置):

$$A^* = \begin{pmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{pmatrix} = \begin{pmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{pmatrix}.$$

可以验证 $AA^* = I_3 = (\det A)I_3$.

命题 5.5. 对于 $A \in M_n(\mathbb{R})$, 有

$$AA^* = A^*A = (\det A)I_n.$$

证明. 计算 $(AA^*)_{ij}$:

$$(AA^*)_{ij} = \sum_{k=1}^n a_{ik}(A^*)_{kj} = \sum_{k=1}^n a_{ik}C_{jk}.$$

当 $i = j$ 时, 这恰好是 $\det A$ 按第 i 行的展开; 当 $i \neq j$ 时, 这相当于将 A 的第 i 行替换第 j 行后按第 j 行展开, 由于该矩阵有两行相同, 行列式为 0. 因此 $(AA^*)_{ij} = \delta_{ij} \det A$, 即 $AA^* = (\det A)I_n$. 类似可证 $A^*A = (\det A)I_n$. \square

推论 5.2. 如果 $A \in M_n(\mathbb{R})$ 可逆, 则

$$A^{-1} = \frac{1}{\det A} A^*.$$

推论 5.3 (克拉姆法则 (Cramer's rule)). 设 $A \in M_n(\mathbb{R})$ 可逆, 则线性方程组 $Ax = b$ 的唯一解为

$$x = A^{-1}b = \frac{1}{\det A} A^*b.$$

写成分量形式: 对 $j = 1, \dots, n$,

$$x_j = \frac{\det A_j}{\det A},$$

其中 A_j 是将 A 的第 j 列替换为 b 后得到的矩阵.

证明. 由 $x = \frac{1}{\det A} A^* b$, 其第 j 个分量为

$$x_j = \frac{1}{\det A} \sum_{k=1}^n (A^*)_{jk} b_k = \frac{1}{\det A} \sum_{k=1}^n C_{kj} b_k.$$

右端恰好是将 A 的第 j 列替换为 b 后按第 j 列展开所得的行列式 $\det A_j$, 因此 $x_j = \det A_j / \det A$. \square

5.4 Laplace 公式与 Cauchy-Binet 公式

余子式展开是按某一行 (或列) 将行列式展为若干 $(n-1)$ 阶行列式之和. Laplace 公式将此思想推广到同时选取多行进行展开.

为了陈述公式, 我们先引入记号. 对于 $A \in M_n(\mathbb{R})$ 及指标集 $M, L \subset \{1, 2, \dots, n\}$, 记 $A_{M,L}$ 为以 M 为行指标集、 L 为列指标集组成的 A 的子矩阵, A_{M^c, L^c} 为对应的余子矩阵, 其中 $M^c = \{1, 2, \dots, n\} \setminus M$.

定理 5.3 (Laplace 公式). 设 $A \in M_n(\mathbb{R})$, 固定行指标集 $M \subset \{1, \dots, n\}$, $|M| = r$, 则

$$\det A = \sum_{\substack{L \subset \{1, \dots, n\} \\ |L|=r}} (-1)^{\sigma(M)+\sigma(L)} \det(A_{M,L}) \det(A_{M^c, L^c}),$$

其中 $\sigma(S) = \sum_{i \in S} i$.

证明. 我们可以利用行列式作为交错多重线性函数的性质来证明本公式. 设 $V = \mathbb{R}^n$, $\varepsilon_1, \dots, \varepsilon_n$ 为 V 的标准基, 行列式函数记为 $\det(v_1, \dots, v_n)$.

固定行指标集 $M = \{i_1 < \dots < i_r\}$, 其补集为 $M^c = \{i'_1 < \dots < i'_{n-r}\}$. 定义两个子空间 $W_1 = \text{span}(\varepsilon_i)_{i \in M}$ 和 $W_2 = \text{span}(\varepsilon_i)_{i \in M^c}$. 显然 $V = W_1 \oplus W_2$, 且 $\dim W_1 = r$, $\dim W_2 = n - r$.

将矩阵 A 的第 j 个列向量记作 v_j , 它可以唯一分解为 $v_j = x_j + y_j$, 其中 $x_j \in W_1, y_j \in W_2$. 注意 x_j 的非零分量仅在行指标 M 中, 构成了属于行集合 M 的子列; y_j 构成了属于行集合 M^c 的子列.

利用多重线性将行列式展开:

$$\det A = \det(x_1 + y_1, \dots, x_n + y_n) = \sum \det(z_1, \dots, z_n),$$

其中每个 z_j 要么是 x_j 要么是 y_j . 由于 \det 是交错的, 如果在 (z_1, \dots, z_n) 中选了超过 r 个 W_1 中的向量, 由于 $\dim W_1 = r$, 它们必然线性相关, 从而由交错性质知该项行列式为零. 同理, 如果选了超过 $n-r$ 个 W_2 中的向量, 包含它们的行列式项也为零. 因此, 非零项只能是恰好有 r 个向量选自 W_1 , 剩下的 $n-r$ 个选自 W_2 . 这对应于选择列指标的一个大小为 r 的子集 $L = \{l_1 < \dots < l_r\} \subset \{1, \dots, n\}$, 当 $j \in L$ 时 $z_j = x_j$, 当 $j \notin L$ 时 $z_j = y_j$. 记其余列

指标为 $L^c = \{l'_1 < \cdots < l'_{n-r}\}$. 于是

$$\det A = \sum_{|L|=r} \det(Z_L),$$

其中 Z_L 表示按照原本列顺序排列的包含 x_{l_k} (对应列 L) 和 $y_{l'_k}$ (对应列 L^c) 的向量组.

我们将 Z_L 中的 r 个 x_{l_k} 依次通过相邻交换移到最前面的 r 个位置, 剩下的 $y_{l'_k}$ 保持相对顺序排在后面. 这一重排需要将列指标 l_k 所在的列与其前面的不属于 L 的列进行交换. l_1 前面有 $l_1 - 1$ 个 L^c 中的列, l_2 前面有 $l_2 - 2$ 个, 依此类推, 总跨越次数对应的符号为 $(-1)^{\sum_{k=1}^r (l_k - k)} = (-1)^{\sigma(L) - r(r+1)/2}$. 即

$$\det(Z_L) = (-1)^{\sigma(L) - r(r+1)/2} \det(x_{l_1}, \dots, x_{l_r}, y_{l'_1}, \dots, y_{l'_{n-r}}).$$

观察后面的行列式 $\det(x_{l_1}, \dots, x_{l_r}, y_{l'_1}, \dots, y_{l'_{n-r}})$. 将这些列向量拼成矩阵, 其前 r 列仅在行 M 上非零, 后 $n-r$ 列仅在行 M^c 上非零. 将该矩阵的行作置换, 把行集合 M 的 r 行依次换到最上面的 r 行, 把 M^c 的行换到下面. 与前面列置换同理, 这次行交换跨越次数的符号为 $(-1)^{\sigma(M) - r(r+1)/2}$. 经过行置换后, 该矩阵变成了分块对角矩阵 $\begin{pmatrix} A_{M,L} & 0 \\ 0 & A_{M^c,L^c} \end{pmatrix}$, 其行列式恰好等于对角两个块的行列式的乘积 $\det(A_{M,L}) \det(A_{M^c,L^c})$. 于是

$$\det(x_{l_1}, \dots, x_{l_r}, y_{l'_1}, \dots, y_{l'_{n-r}}) = (-1)^{\sigma(M) - r(r+1)/2} \det(A_{M,L}) \det(A_{M^c,L^c}).$$

将这两步合并, $\det(Z_L)$ 的总符号为

$$(-1)^{\sigma(L) - \frac{r(r+1)}{2}} \cdot (-1)^{\sigma(M) - \frac{r(r+1)}{2}} = (-1)^{\sigma(M) + \sigma(L) - r(r+1)}.$$

因为 $r(r+1)$ 必为偶数, $(-1)^{-r(r+1)} = 1$, 负号可以忽略. 我们即证明了 Laplace 展开公式:

$$\det A = \sum_{|L|=r} (-1)^{\sigma(M) + \sigma(L)} \det(A_{M,L}) \det(A_{M^c,L^c}).$$

□

注 5.12. 当 $|M| = 1$, 即 $M = \{i\}$ 时, Laplace 公式退化为按第 i 行展开的余子式展开公式 (命题 5.3).

例 5.10. 利用 Laplace 公式计算 4×4 行列式. 设

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

选取 $M = \{3, 4\}$ (第 3、4 行), 则 $\sigma(M) = 3 + 4 = 7$. 第 3、4 行的各 $\binom{4}{2} = 6$ 个 2×2 子矩阵中, 仅有列指标 $L = \{1, 2\}$ 时 $\det(A_{M,L}) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$ 非零. 此时 $\sigma(L) = 1 + 2 = 3$, 且

$$A_{M^c, L^c} = A_{\{1,2\}, \{3,4\}} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \quad \det(A_{M^c, L^c}) = 6.$$

因此 $\det A = (-1)^{7+3} \cdot 1 \cdot 6 = 6$.

Laplace 公式的一个重要推广是 Cauchy-Binet 公式, 它将行列式乘积公式 $|AB| = |A||B|$ 推广到非方阵的情形.

定理 5.4 (Cauchy-Binet 公式). 设 $A \in M_{m \times n}(\mathbb{R})$, $B \in M_{n \times m}(\mathbb{R})$, 则

$$\det(AB) = \begin{cases} \sum_{\substack{S \subset \{1, \dots, n\} \\ |S|=m}} \det(A_{[m], S}) \det(B_{S, [m]}), & m \leq n, \\ 0, & m > n, \end{cases}$$

其中 $[m] = \{1, \dots, m\}$, $A_{[m], S}$ 是 A 取列指标在 S 中的 $m \times m$ 子矩阵, $B_{S, [m]}$ 是 B 取行指标在 S 中的 $m \times m$ 子矩阵.

证明. 记 A 的列向量为 $\alpha_1, \dots, \alpha_n \in \mathbb{R}^m$, 则 $A = (\alpha_1, \dots, \alpha_n)$. 记 $B = (b_{ij})_{n \times m}$, 则矩阵 AB 的第 j 列 c_j 是 A 的各列的线性组合:

$$c_j = A \begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix} = \sum_{k=1}^n b_{kj} \alpha_k.$$

根据行列式作为交错多重线性函数的多重线性性, 我们有

$$\begin{aligned} \det(AB) &= \det(c_1, c_2, \dots, c_m) \\ &= \det \left(\sum_{k_1=1}^n b_{k_1 1} \alpha_{k_1}, \dots, \sum_{k_m=1}^n b_{k_m m} \alpha_{k_m} \right) \\ &= \sum_{k_1=1}^n \cdots \sum_{k_m=1}^n b_{k_1 1} \cdots b_{k_m m} \det(\alpha_{k_1}, \dots, \alpha_{k_m}). \end{aligned}$$

由于交错性, 如果 k_1, \dots, k_m 中有重复的指标, 则 $\det(\alpha_{k_1}, \dots, \alpha_{k_m}) = 0$.

如果 $m > n$, 那么在任一组指标选取 $k_1, \dots, k_m \in \{1, \dots, n\}$ 中, 必然至少有两个指标相同 (抽屉原理). 因此求和式中的每一项皆为 0, 此时 $\det(AB) = 0$.

如果 $m \leq n$, 求和式中仅剩那些由选取 m 个不同指标构成的非零项. 这样的指标列 k_1, \dots, k_m 必定对应于一个严格递增的 m 元子集 $S = \{s_1 < s_2 < \cdots < s_m\} \subset \{1, \dots, n\}$ 以

及某一个置换 $\sigma \in S_m$, 使得 $k_j = s_{\sigma(j)}$. 于是我们可以将上式组织为按子集 S 分组求和的形式:

$$\det(AB) = \sum_{\substack{S \subset \{1, \dots, n\} \\ |S|=m}} \sum_{\sigma \in S_m} b_{s_{\sigma(1)}, 1} \cdots b_{s_{\sigma(m)}, m} \det(\alpha_{s_{\sigma(1)}}, \dots, \alpha_{s_{\sigma(m)}}).$$

再利用行列式的交错性, 把变元排至自然顺序, 得 $\det(\alpha_{s_{\sigma(1)}}, \dots, \alpha_{s_{\sigma(m)}}) = \operatorname{sgn}(\sigma) \det(\alpha_{s_1}, \dots, \alpha_{s_m})$. 注意到 $\det(\alpha_{s_1}, \dots, \alpha_{s_m})$ 恰好等于行列式 $\det(A_{[m], S})$. 从而

$$\begin{aligned} \det(AB) &= \sum_{\substack{S \subset \{1, \dots, n\} \\ |S|=m}} \det(A_{[m], S}) \left(\sum_{\sigma \in S_m} \operatorname{sgn}(\sigma) b_{s_{\sigma(1)}, 1} \cdots b_{s_{\sigma(m)}, m} \right) \\ &= \sum_{\substack{S \subset \{1, \dots, n\} \\ |S|=m}} \det(A_{[m], S}) \det(B_{S, [m]}). \end{aligned}$$

最后一步等号使用了 $B_{S, [m]}$ 的置换求和公式. 命题得证. \square

注 5.13. 当 $m = n$ 时, 只有一个子集 $S = \{1, \dots, n\}$, 公式退化为 $\det(AB) = \det A \cdot \det B$, 这正是行列式的乘法性质 (命题 5.1(4)).

例 5.11. 设 $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2 \times 3}(\mathbb{R})$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_{3 \times 2}(\mathbb{R})$. 直接计算 $AB =$

$\begin{pmatrix} 4 & 5 \\ 10 & 11 \end{pmatrix}$, 故 $\det(AB) = 44 - 50 = -6$.

用 *Cauchy-Binet* 公式验证: S 遍历 $\{1, 2, 3\}$ 的三个二元子集:

$$S = \{1, 2\}: \det \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (-3)(1) = -3,$$

$$S = \{1, 3\}: \det \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix} \det \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (-6)(1) = -6,$$

$$S = \{2, 3\}: \det \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix} \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = (-3)(-1) = 3.$$

求和得 $-3 + (-6) + 3 = -6$, 与直接计算一致.

5.5 习题

5.5.1 练习题

习题 5.2 (多边形面积与行列式). 设平面多边形顶点按逆时针方向依次为

$$P_i = (x_i, y_i), \quad i = 1, \dots, n,$$

并约定 $P_{n+1} = P_1$. 把多边形分解成若干个以原点为公共顶点的有向三角形, 证明其有向面积为

$$\frac{1}{2} \sum_{i=1}^n \det \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix}.$$

用该公式计算顶点 $(0, 0), (3, 0), (2, 2), (0, 1)$ 围成的四边形面积.

习题 5.3. 计算下列行列式:

1.

$$\begin{vmatrix} 4 & -2 & 0 & 5 \\ 3 & 2 & -2 & 1 \\ -2 & 1 & 3 & -1 \\ 2 & 3 & -6 & -3 \end{vmatrix}$$

2.

$$\begin{vmatrix} x & y & z & 1 \\ y & z & x & 1 \\ z & x & y & 1 \\ \frac{z+x}{2} & \frac{x+y}{2} & \frac{y+z}{2} & 1 \end{vmatrix}$$

3.

$$\begin{vmatrix} 3 & 2 & 0 & \cdots & 0 \\ 1 & 3 & 2 & \cdots & 0 \\ 0 & 1 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 3 \end{vmatrix}_{n \times n}$$

4. 因式分解

$$\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix}$$

5. Vandermonde 行列式

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{vmatrix}$$

6.

$$\begin{vmatrix} s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ s_2 & s_3 & s_4 & \cdots & s_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & s_{n+1} & \cdots & s_{2n-2} \end{vmatrix}$$

其中 $s_k = X_1^k + X_2^k + \cdots + X_n^k$.

7. 在复数域 \mathbb{C} 上, 将关于 n 个变量 a_1, a_2, \cdots, a_n 的多项式

$$\begin{vmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{vmatrix}$$

分解为不可约因子乘积.

8. $\det(A^*)$, 其中 A^* 是方阵 A 的伴随.

9. $(n+1) \times (n+2)$ 的矩阵

$$A = (a_{ij}) = \left(\binom{j-1}{i-1} \right), 1 \leq i \leq n+1, 1 \leq j \leq n+2,$$

A_k 为 A 去掉第 k 列得到的矩阵, 计算 $\det(A_k)$.

参考解. 1. -21(计算过程略).

2. 第一行加第三行等于第四行的 2 倍, 故行列式为 0.

3. 我们记这个行列式为 A_n , 这是一个依赖于 n 的函数. 若 $n \geq 3$, 对第一行展开有 $A_n = 3A_{n-1} - 2A_{n-2}$. 方程 $x^2 = 3x - 2$ 有两个单根 $x = 1, 2$, 故上述递归表达式有一般解 $A_n = a + b2^n$. 容易验证 $A_1 = 3, A_2 = 7$, 代入一般表达式解得 $a = -1, b = 2$, 故 $A_n = 2^{n+1} - 1$.

4. 我们可以假设 $a \neq 0$, 用第一列的 a 消去其他非零元, 再对称地用第一行的 a 消去其他

非零元. 然后用第二列的 a 和第二行的 a 消去其他非零元. 结果如下:

$$\begin{aligned} & \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix} \xrightarrow{\text{1st column}} \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ 0 & -d & -bd/a & f - eb/a \\ 0 & -e & -f - cd/a & -ec/a \end{pmatrix} \\ & \xrightarrow{\text{1st row}} \begin{pmatrix} 0 & a & 0 & 0 \\ -a & 0 & d & e \\ 0 & -d & 0 & f - eb/a + cd/a \\ 0 & -e & -f - cd/a + eb/a & 0 \end{pmatrix} \\ & \xrightarrow{\text{2nd column \& row}} \begin{pmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & f - eb/a + cd/a \\ 0 & 0 & -f - cd/a + eb/a & 0 \end{pmatrix} \end{aligned}$$

由于以上行列变换不改变行列式, 故

$$\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = a^2(f + cd/a - eb/a)^2 = (af - be + cd)^2.$$

注: 严格来讲, 我们以上的运算是在环 $\mathbb{Z}[a, b, c, d, e, f][1/a]$ 中进行的. 但是环 $\mathbb{Z}[a, b, c, d, e, f]$ 是 $\mathbb{Z}[a, b, c, d, e, f][1/a]$ 的一个子环, 故等式

$$\begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = (af - be + cd)^2$$

在 $\mathbb{Z}[a, b, c, d, e, f][1/a]$ 上成立, 且等式两边的元素都落入 $\mathbb{Z}[a, b, c, d, e, f]$ 中, 则等式在 $\mathbb{Z}[a, b, c, d, e, f]$ 上成立. 也可以考虑摄动法或直接计算.

5. 我们消去第一行有

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & X_2 - X_1 & \cdots & X_n - X_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & X_2^{n-1} - X_1^{n-1} & \cdots & X_n^{n-1} - X_1^{n-1} \end{vmatrix}$$

对 $2 \leq i \leq n-1$, 我们把第 i 行乘以 $-X_1$ 加到第一行, 行列式不变, 为

$$\begin{aligned}
 & \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & X_2 - X_1 & \cdots & X_n - X_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & X_2^{n-2}(X_2 - X_1) & \cdots & X_n^{n-2}(X_n - X_1) \end{vmatrix} \\
 &= (X_2 - X_1) \cdots (X_n - X_1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & X_2^{n-2} & \cdots & X_n^{n-2} \end{vmatrix} \\
 &= (X_2 - X_1) \cdots (X_n - X_1) \begin{vmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ X_2^{n-2} & \cdots & X_n^{n-2} \end{vmatrix}
 \end{aligned}$$

注意到式子后一部分是一个 $n-1$ 阶的 Vandermonde 行列式, 故可用归纳法得到 n 阶 Vandermonde 行列式为

$$\prod_{1 \leq i < j \leq n} (X_j - X_i).$$

6.

$$\begin{aligned}
 & \begin{vmatrix} s_0 & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ s_2 & s_3 & s_4 & \cdots & s_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & s_{n+1} & \cdots & s_{2n-2} \end{vmatrix} \\
 &= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{vmatrix} \begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ 1 & X_2 & \cdots & X_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix} \\
 &= \prod_{1 \leq i < j \leq n} (X_j - X_i)^2.
 \end{aligned}$$

7. 令 $J = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & I_{n-1} \\ 1 & 0 \end{pmatrix}$, 则可以验证对任意 $1 \leq i \leq n-1$, $J^i =$

$\begin{pmatrix} 0 & I_{n-i} \\ I_i & 0 \end{pmatrix}$. 由于 $|\lambda I_n - J| = \lambda^n - 1$ (请自行验证), 故该多项式有 n 个单根, 即所有的 n 次单位根. 记 $\omega = e^{\frac{2\pi i}{n}}$, 则 J 的所有特征值为 $\omega^i, 0 \leq i \leq n-1$. 由于 J 的特征多项式只有单根, J 可以对角化, 于是存在可逆阵 P 使得 $P^{-1}JP = \text{diag}(1, \omega, \dots, \omega^{n-1})$. 令 $f(x) = a_1 + a_2x + \dots + a_nx^{n-1}$, 注意到题目中的矩阵恰为 $a_1I + a_2J + \dots + a_nJ^{n-1} = f(J)$, 于是

$$P^{-1}f(J)P = \text{diag}(f(1), f(\omega), \dots, f(\omega^{n-1})).$$

因此

$$\det(f(J)) = \prod_{i=0}^{n-1} f(\omega^i) = \prod_{i=0}^{n-1} (a_1 + a_2\omega^i + \dots + a_n\omega^{i(n-1)}).$$

我们得到了一个该行列式的因式分解, 而每个因子都是一次的, 故不可约.

8. 若 $n = 1$, 设 $A = (a)$, 则 $A^* = (1)$, 所以 $\det(A^*) = 1 = \det(A)^0$. 下设 $n \geq 2$. 若 $A = 0$, 则 $A^* = 0$, 从而 $\det(A^*) = 0 = \det(A)^{n-1}$. 若 $A \neq 0$ 且不可逆, 则 $AA^* = \det(A)I_n = 0$. 于是得到 A^* 也不可逆, 否则等式两边乘以 $(A^*)^{-1}$ 得到 $A = 0$, 矛盾! 故 $\det(A^*) = 0 = \det(A)^{n-1}$. 若 A 可逆, 则由 $AA^* = \det(A)I_n$ 知 $\det(A)\det(A^*) = \det(\det(A)I_n) = \det(A)^n$, 而 $\det(A) \neq 0$, 故 $\det(A^*) = \det(A)^{n-1}$.
9. 我们先说明: 对于固定的 i , 函数 $j \rightarrow \binom{j}{i}$ 是一个首项系数为 $1/i!$ 的 i 次多项式. 这是因为 $\binom{j}{i} = \frac{j(j-1)\cdots j-i+1}{i!}$ (注意此式对 $0 \leq j \leq i-1$ 仍然成立, 此时等式两边为 0.) 我们记 $P_i(x) = \frac{x(x-1)\cdots x-i+1}{i!}$. 由归纳法我们可以证明存在系数 $c_{ij}, 0 \leq j \leq i-1$ 使得 $\frac{1}{i!}x^i = P_i(x) + c_{i,i-1}P_{i-1}(x) + \dots + c_{i,0}P_0(x)$. 所求行列式为

$$\begin{vmatrix} P_0(0) & P_0(1) & \cdots & P_0(k-2) & P_0(k) & \cdots & P_0(n+1) \\ P_1(0) & P_1(1) & \cdots & P_1(k-2) & P_1(k) & \cdots & P_1(n+1) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ P_n(0) & P_n(1) & \cdots & P_n(k-2) & P_n(k) & \cdots & P_n(n+1) \end{vmatrix}$$

我们从下到上把第 j 行乘以系数 c_{ij} 加到第 i 行上去, 得到行列式

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & k-2 & k & \cdots & n+1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1/n! & \cdots & (k-2)^n/n! & k^n/n! & \cdots & (n+1)^n/n! \end{vmatrix}$$

由第 5 问知它等于

$$\frac{\prod_{0 \leq i < j \leq n+1, i, j \neq k-1} (j-i)}{\prod_{1 \leq i \leq n} i!}$$

由于

$$\frac{\prod_{1 \leq i \leq n+1} i!}{\prod_{0 \leq i < j \leq n+1} (j-i)} = 1$$

故可将它乘到上一式中并消去相同的项, 得到

$$\frac{(n+1)!}{\prod_{0 \leq i < j \leq n+1, i=k-1} (j-i) \prod_{0 \leq i < j \leq n+1, j=k-1} (j-i)} = \frac{(n+1)!}{(n+1-(k-1)!(k-1)!} = \binom{n+1}{k-1}.$$

□

习题 5.4. 设 A 是 $m \times n$ 矩阵, B 是 $n \times m$ 矩阵, 证明

$$\det(I_m + AB) = \det(I_n + BA).$$

证明. 我们考虑矩阵 $\begin{pmatrix} I_m & A \\ -B & I_n \end{pmatrix}$. 用 I_m 消去左下角的 $-B$ 知其行列式为 $\det(I_n + BA)$, 用 I_n 消去右上角的 A 知其行列式为 $\det(I_m + AB)$, 故二者相等.

□

习题 5.5. 计算下列行列式。

$$\begin{vmatrix} 2 & 3 \\ 1 & 4 \end{vmatrix}, \quad \begin{vmatrix} -1 & 5 \\ 2 & 0 \end{vmatrix}.$$

习题 5.6. 计算

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{vmatrix}.$$

习题 5.7. 设

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}.$$

用行列式判断 A 是否可逆, 并说明对应的线性方程组可能出现什么情况。

习题 5.8. 求由向量 $u = (2, 1)$ 与 $v = (1, 3)$ 张成的平行四边形面积。

习题 5.9. 用克拉默法则解方程组

$$\begin{cases} 2x + y = 5, \\ x - y = 1. \end{cases}$$

习题 5.10. 如果 A 是 3×3 矩阵, 且 $\det A = 4$, 求 $\det(2A)$ 与 $\det(A^{-1})$ 。

习题 5.11. 设 A 是 $n \times n$ 矩阵. 若 A 的两行相同, 说明为什么 $\det A = 0$ 。

5.5.2 思考题

习题 5.12. $M_n(\mathbb{R})$ 是实数域上的 n 阶方阵的集合. $\Phi: M_n(\mathbb{R}) \rightarrow \mathbb{R}$ 是一个映射, 满足以下条件

- (1) $\Phi(AB) = \Phi(A)\Phi(B), \forall A, B \in M_n(\mathbb{R});$
- (2) 对任意上三角矩阵 $A \in M_n(\mathbb{R}), \Phi(A)$ 等于 A 的主对角线元素之积;
- (3) 对任意下三角矩阵 $A \in M_n(\mathbb{R}), \Phi(A)$ 等于 A 的主对角线元素之积.

1. 证明: $\Phi(A) = |A|, \forall A \in M_n(\mathbb{R}).$

2. 如果 Φ 只满足条件 (a) 和 (b), 结论是否成立? 请证明.

习题 5.13 (Hopf 迹公式). 考虑一串线性映射

$$\cdots \xrightarrow{d_{n+1}} V_n \xrightarrow{d_n} V_{n-1} \xrightarrow{d_{n-1}} V_{n-2} \xrightarrow{d_{n-2}} \cdots$$

其中 V_k 都是有限维 \mathbb{R} -向量空间, 并且对任何 $k \in \mathbb{Z}, d_{k-1} \circ d_k = 0.$

- 记 $Z_k = \ker d_k, B_k = \text{im } d_{k+1},$ 证明 B_k 是 Z_k 的子空间, 由此定义商空间 $H_k = Z_k/B_k.$
- 设 $\{f_n: V_n \rightarrow V_n\}_{n \in \mathbb{Z}}$ 是一串线性映射, 满足对任何 $n, d_n \circ f_n = f_{n-1} \circ d_n,$ 则 $f_n(Z_n) \subset Z_n, f_n(B_n) \subset B_n.$
- 利用商空间的性质说明, f_n 诱导了线性映射 $f_{n*}: H_n \rightarrow H_n,$ 使得如下图表交换:

$$\begin{array}{ccc} Z_n & \xrightarrow{f_n} & Z_n \\ \downarrow \pi_n & & \downarrow \pi_n \\ H_n & \xrightarrow{f_{n*}} & H_n \end{array}$$

其中 $\pi_n: Z_n \rightarrow H_n = Z_n/B_n$ 是商空间的投影映射.

- (Hopf 迹公式) 设对某个 $N \in \mathbb{Z}_+,$ 当 $|n| > N$ 时, $V_n = 0.$ 证明

$$\sum_{n \in \mathbb{Z}} (-1)^n \text{tr}(f_n: V_n \rightarrow V_n) = \sum_{n \in \mathbb{Z}} (-1)^n \text{tr}(f_{n*}: H_n \rightarrow H_n).$$

注意这里操作的实际上是有限和, 不涉及级数收敛问题.

- 假设所有的 f_n 都可逆, 且对某个 $N \in \mathbb{Z}_+,$ 当 $|n| > N$ 时, $V_n = 0.$ 请证明

$$\prod_{n \in \mathbb{Z}} (\det(f_n: V_n \rightarrow V_n))^{(-1)^n} = \prod_{n \in \mathbb{Z}} (\det(f_{n*}: H_n \rightarrow H_n))^{(-1)^n}.$$

注意这里零维向量空间的线性变换的 \det 定义为 1, 以上操作的实际上是有限乘积, 不涉及级数收敛问题.

证明. 若 $x \in B_k$ 则 $x = d_{k+1}(y)$, 又因为 $d_k \circ d_{k+1} = 0$ 我们有 $d_k(x) = d_k \circ d_{k+1}(y) = 0$, 因此 $B_k \subset Z_k$. 先证明 $f_n(Z_n) \subset Z_n$, 若 $d_n(x) = 0$ 则 $d_n(f_n(x)) = f_n(d_n(x)) = 0$; 再证明 $f_n(B_n) \subset B_n$, 若 $x = d_{n+1}(y)$ 则 $f_n(x) = d_{n+1}(f_n(y))$. 利用商的万有性质可得映射 $f_n: H_n \rightarrow H_n$ 以及交换性.

由于 $B_n \subset Z_n \subset V_n$ 都是 f_n 不变线性空间, 因此 $tr(f_n; V_n) = tr(f_n; B_n) + tr(f_n; H_n) + tr(f_n; V_n/Z_n)$. 我们断言 $tr(f_{n-1}; B_{n-1}) = tr(f_n; V_n/Z_n)$, 而这个式子不难推出 Hopf 迹公式. 事实上根据第一同构定理 $\tilde{d}_n: V_n/Z_n \rightarrow B_{n-1}$ 是线性空间的同构, 且 $\tilde{d} \circ f = f \circ \tilde{d}$ 从而得到断言. \square

习题 5.14. 记 $w = e^{-\frac{2\pi i}{N}}$. 证明矩阵

$$W = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

可逆, 并求 W^{-1} .

证明. 由 Van der monde 行列式的计算得矩阵可逆. $W(w)W(w^{-1}) = I$ \square

习题 5.15 (伴随矩阵的特征值). 设 A 是 n 阶复矩阵, $\lambda_1, \dots, \lambda_n$ 是 A 的全部特征值 (含重数). 令 A^* 表示 A 的伴随矩阵, 满足 $AA^* = A^*A = (\det A)I_n$. 求 A^* 的全部特征值, 并证明结论.

习题 5.16 (伴随矩阵的秩). 假设 n 阶方阵 A 的秩为 r , A^* 表示 A 的伴随矩阵. 求 A^* 的秩, 并证明:

1. 若 $\text{rank}(A) = n$, 则 $\text{rank}(A^*) = n$;
2. 若 $\text{rank}(A) = n - 1$, 则 $\text{rank}(A^*) = 1$;
3. 若 $\text{rank}(A) \leq n - 2$, 则 $A^* = O$.

习题 5.17 (幂和行列式与 Vandermonde 变体). 设 $s_k = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k$, $k = 1, 2, \dots$. 求证:

$$\begin{vmatrix} n & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & s_{n+1} & \cdots & s_{2n-2} \end{vmatrix} = \prod_{1 \leq j < i \leq n} (\lambda_i - \lambda_j)^2.$$

习题 5.18 (Cauchy 行列式与 Hilbert 矩阵). 设 x_1, \dots, x_n 与 y_1, \dots, y_n 为实数, 且 $x_i + y_j \neq 0$. 令 $M_{ij} = \frac{1}{x_i + y_j}$.

1. 证明 Cauchy 行列式公式:

$$\det M = \frac{\prod_{1 \leq i < j \leq n} (x_j - x_i)(y_j - y_i)}{\prod_{i,j=1}^n (x_i + y_j)}.$$

2. n 阶 Hilbert 矩阵 H_n 定义为 $(H_n)_{ij} = \frac{1}{i+j-1}$. 利用第 (1) 问求 $\det H_n$.

习题 5.19 (Sylvester 恒等式与矩阵行列式引理). 设 $A \in \mathbb{R}^{n \times n}$ 可逆, $u, v \in \mathbb{R}^n$ 为列向量.

1. 对 $U \in \mathbb{R}^{m \times n}$ 、 $V \in \mathbb{R}^{n \times m}$, 证明 $\det(I_m + UV) = \det(I_n + VU)$.

2. 证明矩阵行列式引理:

$$\det(A + uv^T) = \det(A)(1 + v^T A^{-1}u).$$

3. 给出 $A + uv^T$ 可逆的充要条件, 并说明如何快速计算 $(A + uv^T)^{-1}$.

习题 5.20 (三对角 Toeplitz 行列式). 设

$$D_n(a, b) = \det \begin{pmatrix} a & b & 0 & \cdots & 0 \\ b & a & b & \ddots & \vdots \\ 0 & b & a & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & b \\ 0 & \cdots & 0 & b & a \end{pmatrix}.$$

求 $D_n(a, b)$ 关于 a 和 b 的表达式.

习题 5.21 (严格对角占优矩阵的行列式). 假设实方阵 $A = (a_{ij})$ 满足对每个 $1 \leq i \leq n$ 都有

$$a_{ii} > \sum_{j \neq i} |a_{ij}|.$$

证明: $\det A > 0$.

习题 5.22 (矩阵行列式的微积分). 设 $X(t)$ 是 $n \times n$ 矩阵值函数, 每个元素都关于 t 可微.

1. 证明:

$$\left. \frac{d}{dt} \det(I_n + tA) \right|_{t=0} = \operatorname{tr}(A).$$

2. 若 $X(t_0)$ 可逆, 证明 Jacobi 公式:

$$\left. \frac{d}{dt} \det X(t) \right|_{t=t_0} = \det X(t_0) \operatorname{tr}(X(t_0)^{-1} X'(t_0)).$$

6 选读: 域上的线性空间

选学说明

本章把前面在 \mathbb{R} 上建立的线性代数推广到一般域. 教材主线仍然以实数域 \mathbb{R} 和复数域 \mathbb{C} 上的线性空间为主; 有限域、域扩张和有理函数域可以作为拓展阅读, 初学时可先掌握例子和结论的直观意义.

回顾前面几章的内容, 我们发展了线性方程组、线性空间、线性映射和行列式的理论. 这些理论的基础工具——高斯消元、基与维数定理、秩-零化度定理、行列式的多线性性——都只用到了系数之间的**加、减、乘、除**四则运算.

更准确地说, 考虑线性方程组 $Ax = b$. 如果系数矩阵 A 和右端 b 的元素都是有理数, 那么高斯消元的每一步——用一行减去另一行的倍数, 或用主元的倒数来归一化——都只产生有理数. 因此行最简形 $\text{rref}(A, b)$ 的元素仍然是有理数, 解 (如果存在的话) 也可以取有理数. 换言之, 高斯消元不需要开根号、取极限等超出四则运算的操作.

这个观察给我们的启示是: 只要有一个集合 \mathbb{F} , 其中的元素可以做加减乘除, 并且这些运算满足我们习以为常的基本法则 (交换律、结合律、分配律), 那么**前面关于线性方程组、线性空间、线性映射和行列式的主要理论都可以搬到 \mathbb{F} 上来**. 这样的集合 \mathbb{F} 称为**域** (field).

为什么要关心 \mathbb{R} 以外的域? 至少有以下两个原因:

- **复数域 \mathbb{C}** : 在之后我们研究矩阵的特征值时, 实系数矩阵的特征多项式可能没有实数根, 例如旋转矩阵 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 的特征值 $\pm\sqrt{-1}$ 不在 \mathbb{R} 中. 为了使每个矩阵都有特征值, 我们常常需要在 \mathbb{C} 上工作——这将是第8章中特征值理论的核心主题之一.
- **有限域 \mathbb{F}_q** : 在编码理论和密码学中, 核心对象是只有有限个元素的域 (如 $\mathbb{F}_2 = \{0, 1\}$) 上的线性空间. 有限域不仅有直接的应用价值, 还提供了令人意外的计数工具: 在 §6.6 中, 我们将用有限域上的线性代数对第 1 章选读内容中的庞加莱多项式 (定理 1.10) 给出一个全新的、更加自然的证明.

6.1 域

定义 6.1. 一个集合 \mathbb{F} 被称为一个**域** (field), 如果其上拥有如下两种运算:

(1) 加法: $+: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}, (a, b) \mapsto a + b$;

(2) 乘法: $\times: \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F}, (a, b) \mapsto ab$.

并且满足:

- 存在 $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{F}$ ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), 使得任取 $m \in \mathbb{F}$ 有 $0_{\mathbb{F}} + m = m, 1_{\mathbb{F}} \cdot m = m$;

- 任取 $m \in \mathbb{F}$, 存在 $-m \in \mathbb{F}$ 使得 $m + (-m) = 0_{\mathbb{F}}$;
- 任取 $0_{\mathbb{F}} \neq m \in \mathbb{F}$, 存在 $m^{-1} \in \mathbb{F}$ 使得 $mm^{-1} = 1_{\mathbb{F}}$;
- 任取 $a, b, c \in \mathbb{F}$, 有如下结合律, 交换律和分配律:

$$(i) \quad a + b = b + a, (a + b) + c = a + (b + c);$$

$$(ii) \quad ab = ba, (ab)c = a(bc);$$

$$(iii) \quad (a + b)c = ac + bc, c(a + b) = ca + cb.$$

读者会发现, 域的公理恰好是我们在前面章节中对系数做四则运算时所使用的全部性质. 前面关于线性空间和线性映射的每一个证明, 都可以逐字搬到以任意域 \mathbb{F} 为系数的情形.

例 6.1. 实数 \mathbb{R} , 有理数 \mathbb{Q} , 复数 \mathbb{C} 都是域. 整数 \mathbb{Z} 不是域, 因为非零整数 (除 ± 1 外) 没有整数乘法逆元, 例如 2 在 \mathbb{Z} 中没有逆元.

例 6.2 (用 \mathbb{R}^2 构造复数). 在 \mathbb{R}^2 上定义

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \times (c, d) = (ac - bd, ad + bc).$$

直接验证可知上述运算满足域的全部公理. 其中 $0_{\mathbb{F}} = (0, 0)$, $1_{\mathbb{F}} = (1, 0)$. 任取 $(a, b) \in \mathbb{R}^2$, 有 $-(a, b) = (-a, -b)$. 对于 $(a, b) \neq (0, 0)$, 有

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

这实际上用 \mathbb{R}^2 构造了复数域 \mathbb{C} : (a, b) 对应于 $a + \sqrt{-1}b$, 乘法规则正是 $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

例 6.3 (有限域 \mathbb{F}_p). 有限域是只含有限多个元素的域. 最基本的有限域是素数阶有限域 \mathbb{F}_p . 对于素数 p , 考虑集合 $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ (即整数模 p 的剩余类), 加法和乘法定义为模 p 的运算. 例如:

当 $p = 2$ 时, $\mathbb{F}_2 = \{0, 1\}$, 其运算表为:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

这里 $1 + 1 = 0$ (因为 $2 \equiv 0 \pmod{2}$). \mathbb{F}_2 是最小的域, 在编码理论中有着核心地位.

当 $p = 3$ 时, $\mathbb{F}_3 = \{0, 1, 2\}$, 注意 $2 + 1 = 0$ (即 $3 \equiv 0 \pmod{3}$), $2 \cdot 2 = 1$ (即 $4 \equiv 1 \pmod{3}$), 所以 $2^{-1} = 2$.

一般地, \mathbb{F}_p 之所以是域, 关键在于 p 是素数: 对于 $0 \neq a \in \mathbb{F}_p$, 由 $\gcd(a, p) = 1$ 知存在整数 s, t 使得 $sa + tp = 1$, 从而 $sa \equiv 1 \pmod{p}$, 即 a 在 \mathbb{F}_p 中有乘法逆元 $s \pmod{p}$. 如果 p 不是素数, 例如 $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$, 则 2 没有乘法逆元 (因为 $2 \cdot 0 = 0, 2 \cdot 1 = 2, 2 \cdot 2 = 0, 2 \cdot 3 = 2$, 没有一个等于 1), 所以 $\mathbb{Z}/4\mathbb{Z}$ 不是域.

注 6.1 (有限域与纠错码). 有限域最直接的应用之一来自数字通信. 一串 0-1 比特天然可以看成 \mathbb{F}_2^n 中的一个向量, 而“奇偶校验”这样的条件本质上就是 \mathbb{F}_2 上的线性方程组. *Hamming* 码以及更一般的线性码都可以表述为某个校验矩阵 H 的零空间. 更进一步, 条形码、二维码和深空通信中常用的 *Reed-Solomon* 码则建立在更大有限域上的多项式插值理论之上. 因而有限域上的线性代数并不是数学家的游戏, 而是现代信息传输与存储技术的核心语言之一.

命题 6.1 (域中没有零因子). 在域 \mathbb{F} 中, 若 $ab = 0$, 则 $a = 0$ 或 $b = 0$.

证明. 若 $a \neq 0$, 则 a 有乘法逆元 a^{-1} , 两边乘以 a^{-1} 得 $b = a^{-1} \cdot 0 = 0$. 此处用到了 $a^{-1} \cdot 0 = 0$, 这由分配律推出: $a^{-1} \cdot 0 = a^{-1}(0 + 0) = a^{-1} \cdot 0 + a^{-1} \cdot 0$, 两边消去即得. \square

注 6.2. 域中没有零因子这一性质, 正是前面章节中许多论证得以成立的关键. 例如, 在证明线性无关性时, 我们经常需要从 $c \cdot v = 0$ (c 是域中非零元素) 推出 $v = 0$, 这在有零因子的集合 (如 $\mathbb{Z}/4\mathbb{Z}$) 中是不成立的.

定义 6.2 (子域). 设 \mathbb{F} 是域, $K \subset \mathbb{F}$ 是一个子集. 如果 K 在 \mathbb{F} 的加法和乘法运算下自身也构成域 (即包含 $0, 1$, 且对加减乘除封闭), 则称 K 是 \mathbb{F} 的**子域** (*subfield*), 也称 \mathbb{F} 是 K 的**扩域** (*extension field*), 记做 $K \subset \mathbb{F}$.

例 6.4. 我们有自然的子域链 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. 此外, $\mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ 也是 \mathbb{C} 的子域 (读者可在习题中验证).

例 6.5 (四元有限域 \mathbb{F}_4 的构造). 在例 6.2 中, 我们在 \mathbb{R}^2 上定义了一种乘法使其成为域 \mathbb{C} , 关键的一步是找到一个“虚数单位” i 满足 $i^2 = -1$, 即 i 是多项式 $x^2 + 1$ 的根. 我们可以对 \mathbb{F}_2 做完全类似的事情, 但需要注意: 在 \mathbb{F}_2 中 $-1 = 1$ (因为 $1 + 1 = 0$), 所以 $x^2 + 1 = x^2 + x + x + 1 = (x + 1)^2$ 已经有根 $x = 1$, 不能用来构造扩域. 正确的选择是不可约多项式 $x^2 + x + 1$: 代入 $x = 0$ 得 $1 \neq 0$, 代入 $x = 1$ 得 $1 + 1 + 1 = 1 \neq 0$, 所以 $x^2 + x + 1$ 在 \mathbb{F}_2 中确实没有根.

现在模仿 \mathbb{C} 的构造: 在集合 $\mathbb{F}_2^2 = \{(a, b) \mid a, b \in \mathbb{F}_2\}$ 上, 加法按分量进行 (即 \mathbb{F}_2^2 的标准加法), 乘法定义为

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc + bd),$$

其中运算均在 \mathbb{F}_2 中进行. 记 $\omega = (0, 1)$, 则

$$\omega^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 + 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0 + 1 \cdot 1) = (1, 1),$$

而 $(1, 1)$ 对应于 $1 + \omega$. 于是 $\omega^2 = \omega + 1$, 即 $\omega^2 + \omega + 1 = 0$, 正如所期望的.

由此得到的域 $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ (其中 $\omega^2 = 1 + \omega$) 包含 $2^2 = 4$ 个元素. 其完整的加法表和乘法表为:

$+$	0	1	ω	ω^2	\times	0	1	ω	ω^2
0	0	1	ω	ω^2	0	0	0	0	0
1	1	0	ω^2	ω	1	0	1	ω	ω^2
ω	ω	ω^2	0	1	ω	0	ω	ω^2	1
ω^2	ω^2	ω	1	0	ω^2	0	ω^2	1	ω

注意加法表的特点: 在 \mathbb{F}_2 中 $1 + 1 = 0$, 所以每个元素都是自身的加法逆元 (即 $-a = a$). 乘法表中的关键等式 $\omega \cdot \omega^2 = 1$ 说明 $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$.

\mathbb{F}_2 通过 $a \mapsto (a, 0)$ 自然嵌入 \mathbb{F}_4 , 构成 \mathbb{F}_4 的子域. 从线性空间的角度看, \mathbb{F}_4 是 \mathbb{F}_2 上的 2 维线性空间, $\{1, \omega\}$ 为一组基.

注 6.3. 上述构造的思想可以推广: 只要域 \mathbb{F} 上存在一个 n 次不可约多项式 $f(x)$, 就可以构造一个包含 $|\mathbb{F}|^n$ 个元素的有限域. 这一构造与后文关于不可约多项式的讨论 (§7.5) 密切相关. 有限域理论中的一个基本定理是: 对于每个素数幂 $q = p^n$, 恰好存在一个 (同构意义下的) q 元域 \mathbb{F}_q ; 反之, 有限域的元素个数必为素数幂.

6.2 域上的线性空间

在第3章中, 我们定义了 \mathbb{R} -线性空间的概念, 并由此发展了子空间、基、维数和线性映射的完整理论. 现在我们将“ \mathbb{R} ”替换为一般域“ \mathbb{F} ”:

定义 6.3 (\mathbb{F} -线性空间). 设 \mathbb{F} 是一个域. 一个集合 V 连同两种运算——加法 $+: V \times V \rightarrow V$ 和数乘 $\cdot: \mathbb{F} \times V \rightarrow V$ ——被称为 \mathbb{F} 上的**线性空间** (vector space), 如果满足以下八条公理:

加法公理:

- (11) (交换律) 对任意 $u, v \in V$, $u + v = v + u$;
- (22) (结合律) 对任意 $u, v, w \in V$, $(u + v) + w = u + (v + w)$;
- (33) (零向量) 存在 $\mathbf{0} \in V$, 使得对任意 $v \in V$, $v + \mathbf{0} = v$;
- (44) (逆元) 对任意 $v \in V$, 存在 $-v \in V$ 使得 $v + (-v) = \mathbf{0}$.

数乘公理:

- (M1) (单位元) 对任意 $v \in V$, $1 \cdot v = v$;
- (M2) (结合律) 对任意 $a, b \in \mathbb{F}, v \in V$, $(ab) \cdot v = a \cdot (b \cdot v)$;

(M3) (分配律 I) 对任意 $a \in \mathbb{F}, u, v \in V, a \cdot (u + v) = a \cdot u + a \cdot v$;

(M4) (分配律 II) 对任意 $a, b \in \mathbb{F}, v \in V, (a + b) \cdot v = a \cdot v + b \cdot v$.

注 6.4. 读者可以对比第 3 章中 \mathbb{R} -线性空间的定义: 八条公理完全相同, 唯一的变化是将“实数”替换为“域 \mathbb{F} 中的元素”. 因此, 前面关于线性空间、线性映射和行列式的定理, 只要证明中仅使用四则运算和域公理, 就可搬到 \mathbb{F} -线性空间上. 我们在此列出关键概念以固定符号:

- **\mathbb{F} -子空间:** $W \subseteq V$ 对 V 的加法和 \mathbb{F} -数乘封闭 (参见第 3 章);
- **\mathbb{F} -线性无关:** $v_1, \dots, v_n \in V$, 若 $c_1 v_1 + \dots + c_n v_n = \mathbf{0} (c_i \in \mathbb{F})$ 蕴含 $c_1 = \dots = c_n = 0$ (参见第 3 章);
- **\mathbb{F} -基与 \mathbb{F} -维数:** \mathbb{F} -极大线性无关组为 \mathbb{F} -基, 基中元素个数为 $\dim_{\mathbb{F}} V$ (参见第 3 章).

例 6.6. $\mathbb{F}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}\}$ 连同逐分量的加法和数乘构成 \mathbb{F} -线性空间, $\dim_{\mathbb{F}} \mathbb{F}^n = n$. 当 $\mathbb{F} = \mathbb{R}$ 时即为我们熟悉的 \mathbb{R}^n ; 当 $\mathbb{F} = \mathbb{F}_2$ 时, \mathbb{F}_2^n 恰好包含 2^n 个向量. 在编码理论中, \mathbb{F}_2^n 中的子空间被称为**线性码 (linear code)**: 例如 \mathbb{F}_2^7 中的一个 4 维子空间 C 包含 $2^4 = 16$ 个码字, 称为 $[7, 4]$ 汉明码 (Hamming code).

例 6.7 (系数限制——同一集合上的不同线性空间结构). 设 $\mathbb{F} \subset K$ 是域的扩张. 任何 K -线性空间 V 自然地也是 \mathbb{F} -线性空间, 只需将数乘限制在 $\mathbb{F} \subset K$ 上. 但 \mathbb{F} -维数通常大于 K -维数. 例如:

- (1) \mathbb{C} 是 \mathbb{C} -线性空间, $\dim_{\mathbb{C}} \mathbb{C} = 1$ (基为 $\{1\}$). 但 \mathbb{C} 也是 \mathbb{R} -线性空间, $\dim_{\mathbb{R}} \mathbb{C} = 2$ (基为 $\{1, i\}$).
- (2) \mathbb{C}^n 作为 \mathbb{C} -空间的维数是 n , 但作为 \mathbb{R} -空间的维数是 $2n$.
- (3) $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ 作为 \mathbb{F}_2 -线性空间的维数是 2 (基为 $\{1, \omega\}$), 但 $\dim_{\mathbb{F}_4} \mathbb{F}_4 = 1$.

这种“同一集合, 不同域, 不同维数”的现象, 是推广到一般域之后才出现的新特征, 也正是域扩张理论的出发点.

例 6.8 (多项式空间). 设 \mathbb{F} 为域, $\mathbb{F}[x]$ 为 \mathbb{F} 上的多项式全体. 与 $\mathbb{R}[x]$ 完全类似, $\mathbb{F}[x]$ 是无穷维 \mathbb{F} -线性空间, 基为 $\{1, x, x^2, \dots\}$. 其中次数不超过 n 的多项式构成 $\mathbb{F}[x]$ 的 $(n + 1)$ 维子空间 $\mathbb{F}_{\leq n}[x]$.

6.3 域扩张与维数的乘法公式

本小节讨论当域发生扩张时, 线性空间的维数如何变化. 这是理解例如 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ 这类包含链的关键工具.

定义 6.4. 设 $K \subseteq \mathbb{E}$ 是域扩张 (field extension), 即 K 是 \mathbb{E} 的子域. 若 V 是一个 \mathbb{E} -线性空间, 则称 V 同时为约化到 K 的 K -线性空间, 操作由 $K \subset \mathbb{E}$ 中的元素天然作用定义. 这个过程叫做系数的限制 (restriction of scalars).

下面是维数乘法公式的基本形式.

定理 6.1 (维数的乘法公式). 设 $K \subseteq \mathbb{E}$ 为域扩张. 令 V 为有限维的 \mathbb{E} -线性空间. 则视为 K -线性空间时有

$$\dim_K V = (\dim_K \mathbb{E}) \cdot (\dim_{\mathbb{E}} V).$$

证明. 选取 $\{e_1, \dots, e_m\}$ 为 V 作为 \mathbb{E} -线性空间的一组基, 选取 $\{\alpha_1, \dots, \alpha_n\}$ 为 \mathbb{E} 作为 K -线性空间的一组基 (即 $\dim_K \mathbb{E} = n$). 我们断言集合

$$\{\alpha_p e_q \mid 1 \leq p \leq n, 1 \leq q \leq m\}$$

是 V 作为 K -线性空间的基. 首先任取 $v \in V$, 由 $\{e_q\}$ 为 \mathbb{E} -基, 存在 $\beta_q \in \mathbb{E}$ 使得 $v = \sum_{q=1}^m \beta_q e_q$. 每个 β_q 又可以写成 $\beta_q = \sum_{p=1}^n c_{pq} \alpha_p$ ($c_{pq} \in K$), 因此

$$v = \sum_{q=1}^m \sum_{p=1}^n c_{pq} (\alpha_p e_q),$$

即任意向量都由 $\{\alpha_p e_q\}$ 生成. 其次若有线性关系

$$\sum_{p,q} d_{pq} (\alpha_p e_q) = 0 \quad (d_{pq} \in K),$$

我们可以将其重写为

$$\sum_q \left(\sum_p d_{pq} \alpha_p \right) e_q = 0.$$

因为 $\{e_q\}$ 在 \mathbb{E} 上线性无关, 故对每个 q 有 $\sum_p d_{pq} \alpha_p = 0$ 在 \mathbb{E} 中成立. 又 $\{\alpha_p\}$ 在 K 上线性无关, 从而每个 $d_{pq} = 0$. 因此 $\{\alpha_p e_q\}$ 线性无关, 从而是基, 基数即为 nm . 证毕. \square

注 6.5. 上述证明完全代数化: 唯一需要的是 \mathbb{E} 作为 K -向量空间是有限维的. 在常见例子中 (例如 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$), 我们经常只在有限扩张 (如 $\mathbb{Q}(\sqrt{2})$) 情形下应用此定理.

6.4 复数结构与实线性变换

当域扩张 $\mathbb{R} \subset \mathbb{E}$ 满足 $\dim_{\mathbb{R}} \mathbb{E} = 2$ 时, 可以从中提取出“复数结构”——即一个平方为 -1 的线性变换. 这一观点将复数乘法与旋转矩阵联系起来.

命题 6.2. 设 $\mathbb{E} \supset \mathbb{R}$ 为域扩张且 $\dim_{\mathbb{R}} \mathbb{E} = 2$. 则存在 $\alpha \in \mathbb{E}$ 使得 $\{1, \alpha\}$ 为 \mathbb{E} 的 \mathbb{R} -基, 并且 $\alpha^2 = -1$. 从而 $\mathbb{E} \cong \mathbb{C}$.

证明. 取任意 $\beta \in \mathbb{E} \setminus \mathbb{R}$, 则 $\{1, \beta\}$ 为 \mathbb{R} -基. 因为 $1, \beta, \beta^2$ 三个元素在 2 维实线性空间中必线性相关, 故存在实数 s, t 使得

$$\beta^2 + s\beta + t = 0.$$

这个二次多项式在 \mathbb{R} 上没有根; 否则 β 会等于某个实数, 与 $\beta \notin \mathbb{R}$ 矛盾. 因此它的判别式 $\Delta = s^2 - 4t < 0$, 即 $4t - s^2 > 0$. 令

$$\alpha = \frac{2\beta + s}{\sqrt{4t - s^2}}.$$

由 $\beta^2 + s\beta + t = 0$ 可得 $(2\beta + s)^2 = s^2 - 4t$, 从而 $\alpha^2 = -1$. 于是 $\{1, \alpha\}$ 仍为 \mathbb{E} 的一组 \mathbb{R} -基, 并且映射

$$\mathbb{C} \rightarrow \mathbb{E}, \quad a + bi \mapsto a + b\alpha$$

保持加法和乘法, 因而是域同构. □

有了这一命题, 设 V 为 \mathbb{E} -向量空间 (其中 $\mathbb{E} \cong \mathbb{C}$). 将 V 视为 \mathbb{R} -向量空间, 则“乘以 α ”定义了一个 \mathbb{R} -线性变换 $T_\alpha(v) = \alpha \cdot v$, 满足 $T_\alpha^2 = -\text{Id}$. 我们称 T_α 为 V 上的**复数结构**.

例 6.9 (复数乘法的矩阵表示). 取 $V = \mathbb{C}$, $\alpha = i$, \mathbb{R} -基 $\{1, i\}$. 对 $z = a + bi \in \mathbb{C}$, “乘以 z ”的映射 $M_z: \mathbb{C} \rightarrow \mathbb{C}$ 在此基下的矩阵为

$$[M_z] = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

特别地, $[M_i] = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 满足 $[M_i]^2 = -I_2$, 这正是平面上逆时针旋转 90° 的矩阵.

注 6.6. 反过来, 若 $T: V \rightarrow V$ 是有限维 \mathbb{R} -向量空间上的线性变换满足 $T^2 = -\text{Id}$, 则可以定义 \mathbb{C} -数乘 $(a + bi) \cdot v = av + bT(v)$ 使 V 成为 \mathbb{C} -向量空间. 因此复数结构等价于满足 $T^2 = -\text{Id}$ 的实线性算子. 特别地, 这要求 $\dim_{\mathbb{R}} V$ 为偶数 (习题 6.10).

6.5 选读: 代数数与多项式商空间 *

选学背景

本小节解释如何用多项式商空间构造新的数系, 是“域扩张”的第一眼图像. 高中友好主线只需要熟悉 \mathbb{R}, \mathbb{C} 上的向量空间; 若还不熟悉多项式整除和不可约多项式, 可以先跳到下一节主线内容.

本小节是选学内容, 将域扩张与多项式的商空间联系起来.

定义 6.5. 设 K 为域, $\mathbb{E} \supset K$ 为扩域. 元素 $\alpha \in \mathbb{E}$ 称为 K 上的**代数元** (algebraic over K), 若存在非零多项式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$. 否则称 α 为 K 上的**超越元** (transcendental over K).

例 6.10. $\sqrt{2}$ 是 \mathbb{Q} 上的代数元 ($x^2 - 2$ 的根); i 是 \mathbb{R} 上的代数元 ($x^2 + 1$ 的根); π 和 e 是 \mathbb{Q} 上的超越元.

若 α 是 K 上的代数元, 则在所有满足 $f(\alpha) = 0$ 的首一多项式中, 次数最小者称为**最小多项式** (minimal polynomial), 记为 $m_{\alpha, K}(x)$. 它必定不可约⁷(否则可以分解为次数更低的因子, 由域中无零因子可推出矛盾). 设 $n = \deg m_{\alpha, K}$, 则:

- $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ 是 $K(\alpha)$ 作为 K -向量空间的基, $\dim_K K(\alpha) = n$.
- $K(\alpha) \cong K[x]/(m_{\alpha, K}(x))$ (通过赋值映射 $g(x) \mapsto g(\alpha)$ 和第一同构定理).

在基 $\{1, \alpha, \dots, \alpha^{n-1}\}$ 下, “乘以 α ” 的矩阵称为**友阵** (companion matrix):

$$C(m) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix},$$

其中 $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. 友阵的特征多项式恰为 $m(x)$.

例 6.11. $\alpha = \sqrt{2}$, $m(x) = x^2 - 2$, 友阵 $C = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, 特征多项式 $x^2 - 2$.

注 6.7. 这一理论统一了前面的构造:

- 例 6.2 中用 \mathbb{R}^2 构造 \mathbb{C} : 这是 $\mathbb{R}[x]/(x^2 + 1)$, 其中 i 对应 \bar{x} .
- 例 6.5 中 \mathbb{F}_4 的构造: 这是 $\mathbb{F}_2[x]/(x^2 + x + 1)$, 其中 ω 对应 \bar{x} .

6.6 选读: 有限域上的 Grassmannian 计数*

选学背景

这里把有限域和子空间计数结合起来, 是组合数学和代数几何的拓展入口. 它可以帮助理解为什么高斯二项式系数自然出现, 但不影响本章关于“域上线性空间”的主线.

在第 1 章的选学内容中, 我们通过最简行阶梯型将格拉斯曼流形 $G(k, n)$ 分解为舒伯特胞腔, 并证明了其庞加莱多项式为 q -二项式系数 (定理 1.10):

$$P_{k,n}(t) = \binom{n}{k}_t.$$

⁷关于不可约多项式的严格定义参见定义 7.5.

现在有了有限域的工具, 我们可以给出这一公式的另一种理解: 将 t 替换为素数幂 p , $P_{k,n}(p)$ 恰好等于 \mathbb{F}_p^n 中 k 维子空间的个数. 这种“有限域计数”方法在代数几何中被称为 Weil 的“动机”(motives) 思想的雏形.

设 p 为素数, \mathbb{F}_p 为 p 元有限域. 记 $G(k, n; \mathbb{F}_p)$ 为 \mathbb{F}_p^n 中所有 k 维子空间的集合 (有限域上的格拉斯曼流形). 我们来计算 $\#G(k, n; \mathbb{F}_p)$.

引理 6.1. \mathbb{F}_p^n 中 m 个线性无关向量组成的有序组 (v_1, \dots, v_m) 的个数为

$$\prod_{k=0}^{m-1} (p^n - p^k).$$

证明. 逐步选取:

- v_1 : 任意非零向量, 有 $p^n - 1$ 种选择.
- v_2 : 不能落在 $\text{span}(v_1)$ 中. 由于 $\text{span}(v_1)$ 是 1 维子空间, 含 p 个向量, 故有 $p^n - p$ 种选择.
- v_j : 不能落在 $\text{span}(v_1, \dots, v_{j-1})$ 中. 这是一个 $(j-1)$ 维子空间, 含 p^{j-1} 个向量, 故有 $p^n - p^{j-1}$ 种选择.

各步的选择互不影响, 相乘即得. □

推论 6.1. 一般线性群 $\text{GL}(m, \mathbb{F}_p)$ 的阶为

$$\#\text{GL}(m, \mathbb{F}_p) = \prod_{k=0}^{m-1} (p^m - p^k).$$

证明. 可逆矩阵 $A \in \text{GL}(m, \mathbb{F}_p)$ 的列向量 (v_1, \dots, v_m) 恰好构成 \mathbb{F}_p^m 中 m 个线性无关向量的有序组, 由引理 6.1 (取 $n = m$) 即得. □

定理 6.2 (有限域上的 Grassmannian 计数).

$$\#G(k, n; \mathbb{F}_p) = \frac{\prod_{j=0}^{k-1} (p^n - p^j)}{\prod_{j=0}^{k-1} (p^k - p^j)} = \binom{n}{k}_p.$$

证明. 考虑将 k 维子空间 W 表示为某个秩为 k 的 $k \times n$ 矩阵 B 的行空间. W 的所有有序基 (w_1, \dots, w_k) 的个数等于 $\#\text{GL}(k, \mathbb{F}_p)$, 因为基之间通过可逆矩阵相互转化.

由引理6.1, \mathbb{F}_p^n 中 k 个线性无关向量的有序组共有 $\prod_{j=0}^{k-1} (p^n - p^j)$ 个. 每 $\# \text{GL}(k, \mathbb{F}_p)$ 个有序组对应同一个 k 维子空间, 因此

$$\#G(k, n; \mathbb{F}_p) = \frac{\prod_{j=0}^{k-1} (p^n - p^j)}{\prod_{j=0}^{k-1} (p^k - p^j)}.$$

最后验证这等于 q -二项式系数在 $q = p$ 处的值:

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q! [n-k]_q!} = \frac{\prod_{i=1}^n (q^i - 1)}{\prod_{i=1}^k (q^i - 1) \cdot \prod_{i=1}^{n-k} (q^i - 1)}.$$

而

$$\frac{\prod_{j=0}^{k-1} (p^n - p^j)}{\prod_{j=0}^{k-1} (p^k - p^j)} = \prod_{j=0}^{k-1} \frac{p^n - p^j}{p^k - p^j} = \prod_{j=0}^{k-1} \frac{p^j (p^{n-j} - 1)}{p^j (p^{k-j} - 1)} = \prod_{j=0}^{k-1} \frac{p^{n-j} - 1}{p^{k-j} - 1} = \frac{\prod_{i=n-k+1}^n (p^i - 1)}{\prod_{i=1}^k (p^i - 1)} = \binom{n}{k}_p.$$

□

例 6.12. 取 $p = 2$, 计算 \mathbb{F}_2^3 中 1 维子空间的个数 (即 \mathbb{F}_2 上的射影平面):

$$\#G(1, 3; \mathbb{F}_2) = \frac{2^3 - 1}{2^1 - 1} = 7.$$

这 7 条“直线”(每条含 $2^1 = 2$ 个点: 零向量和一个非零向量)恰好对应 \mathbb{F}_2^3 中的 7 个非零向量.

庞加莱多项式在 $t = 2$ 处的值: $P_{1,3}(2) = 2^2 + 2 + 1 = 7$, 与计数结果一致.

注 6.8. 定理 6.2 给出了定理 1.10 中 q -二项式系数的一种新的组合解释: 格拉斯曼流形 $G(k, n)$ 的舒伯特胞腔分解和庞加莱多项式, 恰好编码了有限域上子空间的计数信息. 具体而言, 将庞加莱多项式 $P_{k,n}(t)$ 在 $t = p$ 处取值, 得到的正是 \mathbb{F}_p^n 中 k 维子空间的个数. 由于 p 可以取无穷多个素数, 而两个有理数域上的多项式在无穷多个不同的数上取值相等等价于这两个多项式相等, 所以这个观察也给出来定理 1.10 的一个新的证明.

这一现象并非巧合. 在代数几何中, 格拉斯曼流形 $G(k, n)$ 是一个光滑射影簇, 其在有限域 \mathbb{F}_q 上的有理点个数恰好由庞加莱多项式 $P_{k,n}(q)$ 给出. Weil 猜想 (已由 Dwork, Grothendieck 和 Deligne 证明) 指出, 对于一大类代数簇, 有理点个数与拓扑不变量 (如 Betti 数) 之间存在深刻的联系.

6.7 选读: 微扰法的代数化: 有理函数域方法*

选学背景

这一节用有理函数域把“取一个很小的扰动再令其趋于零”的想法改写成纯代数证明. 它适合想理解“为什么某些实数证明能推广到任意域”的读者; 初学时可先将其看作处理不可逆矩阵的一种高级技巧.

在第5章中, 我们证明分块矩阵的行列式公式 (命题5.4) 时使用了“微扰法”: 先对 A 可逆的情形进行计算, 再用 $A + \lambda I$ 替换 A , 最后令 $\lambda \rightarrow 0$. 这个极限论证依赖于实数的连续性, 但我们在本章已经看到, 行列式的定义和基本性质 (多线性性、反对称性) 对任意域 \mathbb{F} 上的矩阵都成立. 一个自然的问题是:

在 \mathbb{F}_2 或 \mathbb{F}_p 等有限域上, “ $\lambda \rightarrow 0$ ” 没有意义,
分块矩阵的行列式公式还成立吗?

答案是肯定的. 关键思想是: 用有理函数域替代极限论证. 具体而言, 我们不再把 λ 当成一个“趋于 0 的实数”, 而是把它当成一个形式变量 (indeterminate), 在更大的域——有理函数域 $\mathbb{F}(\lambda)$ ——上进行运算.

定义 6.6. 设 \mathbb{F} 为域. \mathbb{F} 上的有理函数域 (field of rational functions) 定义为

$$\mathbb{F}(\lambda) := \left\{ \frac{f(\lambda)}{g(\lambda)} \mid f, g \in \mathbb{F}[\lambda], g \neq 0 \right\},$$

其中两个分式 $\frac{f_1}{g_1}$ 与 $\frac{f_2}{g_2}$ 被视为相等当且仅当 $f_1 g_2 = f_2 g_1$ (作为 $\mathbb{F}[\lambda]$ 中的多项式). $\mathbb{F}(\lambda)$ 在通常的分式加法和乘法下构成域, 且 $\mathbb{F} \subset \mathbb{F}[\lambda] \subset \mathbb{F}(\lambda)$.

有了有理函数域, 微扰法的代数化可以表述如下.

命题 6.3 (多项式恒等式原则). 设 \mathbb{F} 为域, $p(\lambda), q(\lambda) \in \mathbb{F}[\lambda]$ 为两个多项式. 若存在无穷多个 $\lambda_0 \in \mathbb{F}$ 使得 $p(\lambda_0) = q(\lambda_0)$, 则 $p = q$ (作为 $\mathbb{F}[\lambda]$ 中的多项式).

特别地, 若 \mathbb{F} 是无穷域 (如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 或 $\mathbb{F}(\lambda)$ 本身), 则对所有 $\lambda_0 \in \mathbb{F}$ 都有 $p(\lambda_0) = q(\lambda_0)$ 蕴含 $p = q$.

证明. $h = p - q$ 是一个多项式, 且有无穷多个根, 但非零多项式的根的个数不超过其次数 (推论7.2). 因此 $h = 0$. \square

注 6.9. 对于有限域 \mathbb{F}_p , 多项式 $\lambda^p - \lambda$ 在 \mathbb{F}_p 中有 p 个根 (即 \mathbb{F}_p 的所有元素), 但它不是零多项式. 因此上述命题的“对所有 $\lambda_0 \in \mathbb{F}$ ”在有限域上并不直接适用. 但我们可以绕开这个困难: 在 $\mathbb{F}[\lambda]$ 中, 如果两个多项式作为形式多项式相等 (即各次系数都相等), 那么它们在任意域的任何点上取值都相等. 这正是下面定理所利用的关键.

现在我们给出分块矩阵行列式公式的纯代数证明.

定理 6.3 (一般域上的分块行列式公式). 设 \mathbb{F} 为任意域, $A, B, C, D \in M_n(\mathbb{F})$, 且 $AC = CA$. 则

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

证明. 引入形式变量 λ , 考虑有理函数域 $\mathbb{F}(\lambda)$ 上的矩阵 $A_\lambda := A + \lambda I_n \in M_n(\mathbb{F}(\lambda))$.

第一步: A_λ 在 $\mathbb{F}(\lambda)$ 上可逆. $\det A_\lambda = \det(A + \lambda I_n)$ 是 λ 的 n 次首一多项式 (系数在 \mathbb{F} 中), 作为 $\mathbb{F}[\lambda]$ 中的元素它不是零多项式 (因为最高次项为 λ^n), 因此 $\det A_\lambda \neq 0$, 即 A_λ 在 $\mathbb{F}(\lambda)$ 上可逆. 进一步, $A_\lambda^{-1} = \frac{1}{\det A_\lambda} A_\lambda^*$, 其元素都在 $\mathbb{F}(\lambda)$ 中.

第二步: 在 $\mathbb{F}(\lambda)$ 上做消元. 由于 A_λ 可逆, 可以进行分块消元:

$$\begin{pmatrix} I & 0 \\ -CA_\lambda^{-1} & I \end{pmatrix} \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix} = \begin{pmatrix} A_\lambda & B \\ 0 & D - CA_\lambda^{-1}B \end{pmatrix}.$$

对两边取行列式:

$$\det \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix} = \det(A_\lambda) \cdot \det(D - CA_\lambda^{-1}B).$$

由于 $AC = CA$, 而 $A_\lambda = A + \lambda I$ 显然与 C 交换 (因为 A 和 I 都与 C 交换), 从而 $A_\lambda C = CA_\lambda$, 进而 $CA_\lambda^{-1} = A_\lambda^{-1}C$ (两边左乘 A_λ^{-1} 右乘 A_λ^{-1}). 于是:

$$\det(A_\lambda) \cdot \det(D - A_\lambda^{-1}CB) = \det(A_\lambda(D - A_\lambda^{-1}CB)) = \det(A_\lambda D - CB).$$

因此

$$\det \begin{pmatrix} A_\lambda & B \\ C & D \end{pmatrix} = \det(A_\lambda D - CB). \quad (8)$$

第三步: 从 $\mathbb{F}(\lambda)$ 回到 \mathbb{F} . 将 $A_\lambda = A + \lambda I$ 代入 (8) 的两边, 展开后都是 $\mathbb{F}[\lambda]$ 中的多项式 (因为行列式是矩阵元素的多项式表达式). 因此 (8) 是 $\mathbb{F}[\lambda]$ 中的**多项式恒等式**, 各次系数完全相同. 令 $\lambda = 0$ (即在 $\mathbb{F}[\lambda]$ 中做代入, 而非取极限), 得到

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

□

注 6.10. 让我们比较一下实数域上的微扰法与代数化方法的异同:

- **经典微扰法** ($\mathbb{F} = \mathbb{R}$): 用 $A + \lambda I$ 替换 A , 在 \mathbb{R} 上对足够小的 $\lambda \neq 0$ 验证等式, 再令 $\lambda \rightarrow 0$ 取极限. 需要用到实数的**拓扑性质** (连续性), 也需要知道 $\det(A + \lambda I) \neq 0$ 至多只有有限个例外.

- **代数化方法** (任意 \mathbb{F}): 在 $\mathbb{F}(\lambda)$ 上验证等式, 再注意到两边是 $\mathbb{F}[\lambda]$ 中的多项式恒等式, 令 $\lambda = 0$ 做代入. 整个过程只用到域的代数性质, 不涉及拓扑或极限.

第二种方法的核心洞察是: $\mathbb{F}[\lambda]$ 中“各项系数相等”能推出“对所有 λ 成立”, 而关于前者的等式可以将 $\mathbb{F}[\lambda]$ 放在域 $\mathbb{F}(\lambda)$ 中验证. 此时 $\mathbb{F}(\lambda)$ 是域, 我们可以用前面章节中发展的线性代数工具来处理. 这一方法是代数学中的标准技巧, 有时也称为“泛系数方法”或“一般位置论证”.

这一方法有着广泛的适用性. 作为一个示例, 我们再用它来证明矩阵乘法的行列式公式.

例 6.13 (行列式乘法公式的另一种证明). 设 \mathbb{F} 为任意域, $A, B \in M_n(\mathbb{F})$. 我们用有理函数域方法重新证明 $\det(AB) = \det A \cdot \det B$.

在 $\mathbb{F}(\lambda)$ 上, 令 $A_\lambda = A + \lambda I$. 由第一步的论证, A_λ 可逆. 考虑恒等式

$$A_\lambda B = A_\lambda \cdot B,$$

取行列式: $\det(A_\lambda B) = \det(A_\lambda) \det(B)$. 这里左边的等式对可逆矩阵是容易证明的⁸. 两边都是 λ 的多项式, 令 $\lambda = 0$ 得到 $\det(AB) = \det(A) \det(B)$.

注 6.11. 更一般地, 代数化方法的哲学可以这样概括: 设 $f(a_1, \dots, a_N)$ 和 $g(a_1, \dots, a_N)$ 是矩阵元素 a_1, \dots, a_N 的两个多项式表达式, 它们定义了 \mathbb{F}^N 到 \mathbb{F} 的多项式映射. 如果在某个无穷域 (比如 \mathbb{R} 或 \mathbb{C}) 上已经知道 $f = g$, 那么作为多元多项式它们的系数完全相同. 由于多项式的系数只涉及整数运算 (加法和乘法), 因此 $f = g$ 在任何域上都成立. 这就是为什么 §4 中所有关于行列式的公式 (Laplace 展开、Cauchy–Binet 公式、 $\det(AB) = \det A \det B$ 等) 自动对任意域成立.

6.8 习题

6.8.1 练习题

习题 6.1 (最简单的奇偶校验码). 在 \mathbb{F}_2 上考虑集合

$$C = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}.$$

1. 证明 C 是 \mathbb{F}_2^4 的子空间.
2. 求 C 的维数和一组基.
3. 解释为什么 C 中的向量可以检测一位传输错误, 但不能总是纠正错误.

习题 6.2 (域的基本性质). 利用域 \mathbb{F} 的运算公理证明: 对任意 $a \in \mathbb{F}$, $0 \cdot a = 0$.

⁸对可逆矩阵 A , 将 A 分解为初等矩阵的乘积, 再逐步使用行列式在初等行变换下的性质即可.

习题 6.3. 证明域中不存在零因子, 即若 $ab = 0$ 则 $a = 0$ 或 $b = 0$. (提示: 若 $a \neq 0$, 两边乘 a^{-1} .)

习题 6.4. 验证 $\mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ 作为 \mathbb{C} 的子集, 在 \mathbb{C} 的乘法和加法下构成域. 求 $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{-1}]$.

习题 6.5. 验证 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 构成域, 并写出 $(1 + \sqrt{2})^{-1}$. 求 $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}]$.

习题 6.6 (构造 \mathbb{F}_4). 在 \mathbb{F}_2 上, 多项式 $x^2 + x + 1$ 没有根 (验证之). 在 \mathbb{F}_2^2 上定义加法为逐分量加法, 乘法为

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc + bd),$$

其中运算在 \mathbb{F}_2 中进行. 令 $\omega = (0, 1)$.

1. 验证上述运算使 \mathbb{F}_2^2 成为域 (记为 \mathbb{F}_4), 并写出完整的乘法表.
2. 验证 $\omega^2 = \omega + 1$ (即 $\omega^2 + \omega + 1 = 0$).
3. 证明 $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$.

习题 6.7 (\mathbb{F}_p 中 $x^2 + 1$ 何时有根). 对于素数 p , 证明 $x^2 + 1 = 0$ 在 \mathbb{F}_p 中有解当且仅当 $p = 2$ 或 $p \equiv 1 \pmod{4}$. (提示: 考虑 \mathbb{F}_p^\times 的阶和元素的阶.)

习题 6.8 (多项式商空间与友阵). 设 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$, 其中 $a_n \neq 0$, \mathbb{F} 为域. 令 $V = \mathbb{F}[x]/(f(x))$.

1. 求 V 的一组 \mathbb{F} -基, 并计算 $\dim_{\mathbb{F}} V$.
2. 定义线性变换 $T: V \rightarrow V, \overline{g(x)} \mapsto \overline{x \cdot g(x)}$. 求 T 在所选基下的矩阵表示, 并验证它是 $f(x)$ 的友阵 (经适当归一化后).

习题 6.9 (系数的限制与维数乘法). 设 $\mathbb{F} \subset K$ 为域扩张.

1. 证明 K 在 \mathbb{F} 的数乘下构成 \mathbb{F} -线性空间.
2. 设 V 为有限维 K -线性空间. 证明 V 在限制系数到 \mathbb{F} 后成为 \mathbb{F} -线性空间, 且 $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} K \cdot \dim_K V$. (参见定理 6.1.)
3. 设 $\mathbb{F} = \mathbb{R}, \dim_{\mathbb{R}} K = 2$. 证明存在 $\alpha \in K$ 使得 $\{1, \alpha\}$ 为 K 的 \mathbb{R} -基且 $\alpha^2 = -1$. (参见命题 6.2.)
4. 沿用 (3) 的记号. 证明 $T_\alpha(v) = \alpha \cdot v$ 定义了 V 上的 \mathbb{R} -线性变换. 选取一组适当的 \mathbb{R} -基写出 T_α 的矩阵, 并证明该矩阵的平方为 $-I$.

习题 6.10 ($T^2 = -I$ 与偶维数). 设 V 为有限维 \mathbb{R} -线性空间, $T: V \rightarrow V$ 为 \mathbb{R} -线性变换满足 $T^2 = -\text{Id}$.

1. 证明 $\dim_{\mathbb{R}} V$ 为偶数. (提示: 计算 $\det(T^2)$.)
2. 证明存在 V 的一组 \mathbb{R} -基使得 T 的矩阵为 n 个 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 的直和 (其中 $\dim_{\mathbb{R}} V = 2n$).
(提示: 对任意 $v \neq 0$, 证明 $\{v, Tv\}$ \mathbb{R} -线性无关, 并对 $\text{span}\{v, Tv\}$ 的补空间用归纳法.)

习题 6.11 (代数数与超越数). 设 $\alpha \in \mathbb{R}$, 将 \mathbb{R} 视为 \mathbb{Q} -线性空间.

1. 证明 α 是无理数当且仅当 $1, \alpha$ 在 \mathbb{Q} 上线性无关.
2. 定义 $\mathbb{Q}[\alpha] = \{g(\alpha) \mid g(x) \in \mathbb{Q}[x]\}$. 证明 α 是 \mathbb{Q} 上的代数数 (即存在非零 $f \in \mathbb{Q}[x]$ 使 $f(\alpha) = 0$) 当且仅当 $\mathbb{Q}[\alpha]$ 是 \mathbb{Q} 上的有限维线性空间.
3. 若 α 的最小多项式 $m(x) \in \mathbb{Q}[x]$ 的次数为 n , 求 $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha]$.

习题 6.12 (维数的传递性). 设 $\mathbb{F} \subset K \subset \mathbb{E}$ 为域的链, 且 $[K : \mathbb{F}]$ 和 $[\mathbb{E} : K]$ 均有限. 利用定理 6.1 证明

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : K] \cdot [K : \mathbb{F}].$$

并以 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ 为例验证.

习题 6.13. 把复数 $2-3i$ 看成 \mathbb{R} 上的二维向量. 写出它对应的坐标, 并计算 $(2-3i)+(1+i)$ 与 $(1+i)(2-3i)$.

习题 6.14. 在复数域 \mathbb{C} 上, 判断向量组

$$(1, i), \quad (i, -1)$$

是否线性无关.

习题 6.15. 把 \mathbb{C} 看成 \mathbb{R} 上的向量空间. 说明 $\{1, i\}$ 是一组基, 并写出 $3-2i$ 在这组基下的坐标.

习题 6.16. 在只有两个元素的域 $\mathbb{F}_2 = \{0, 1\}$ 中, 规定 $1+1=0$. 列出 \mathbb{F}_2^2 中的全部向量.

习题 6.17. 在 \mathbb{F}_2^2 中, 判断向量 $(1, 0)$ 与 $(1, 1)$ 是否线性无关.

6.8.2 思考题

习题 6.18 (有限域上的子空间计数). 1. 计算 $\#G(1, 4; \mathbb{F}_2)$ (即 \mathbb{F}_2^4 中 1 维子空间的个数).

2. 计算 $\#G(2, 4; \mathbb{F}_2)$, 并与 §1 中例 1.11 的舒伯特胞腔分解进行对比 (庞加莱多项式 $P_{2,4}(t)$ 在 $t=2$ 处取值).

3. 证明 $\# \text{GL}(n, \mathbb{F}_p) = p^{\binom{n}{2}} \prod_{k=1}^n (p^k - 1)$.

习题 6.19 (有理函数域与微扰法). 设 \mathbb{F} 为域, $A, B \in M_n(\mathbb{F})$.

1. 证明 $\mathbb{F}(\lambda)$ 是一个域. (提示: 验证分式的加法和乘法满足域的公理.)
2. 证明 $\det(A + \lambda I_n) \in \mathbb{F}[\lambda]$ 是 λ 的 n 次首一多项式, 从而 $A + \lambda I_n$ 在 $\mathbb{F}(\lambda)$ 上可逆.
3. 利用有理函数域方法证明 *Sylvester* 行列式恒等式: 对任意 $A \in M_{m \times n}(\mathbb{F})$, $B \in M_{n \times m}(\mathbb{F})$, 有

$$\det(I_m + AB) = \det(I_n + BA).$$

(提示: 先在 $\mathbb{F}(\lambda)$ 上证明 $\det(\lambda I_m + AB) = \lambda^{m-n} \det(\lambda I_n + BA)$ 当 $m \geq n$ 时成立, 利用 $\lambda I_m + AB = \lambda(I_m + \lambda^{-1}AB)$ 以及分块矩阵

$$\begin{pmatrix} \lambda I_m & A \\ B & I_n \end{pmatrix}$$

的两种消元方式.)

4. 利用有理函数域方法证明: 对任意 $A \in M_n(\mathbb{F})$, 有 $\det(\text{adj}(A)) = (\det A)^{n-1}$, 其中 $\text{adj}(A)$ 是 A 的伴随矩阵. (提示: 先对 $A + \lambda I_n$ 可逆的情形利用 $A \cdot \text{adj}(A) = (\det A)I_n$ 两边取行列式, 再利用多项式恒等式原则.)

习题 6.20 (伴随矩阵的乘法公式). 设 \mathbb{F} 为任意域, $A, B \in M_n(\mathbb{F})$. 利用有理函数域方法证明

$$(AB)^* = B^*A^*.$$

(提示: 引入形式变量 λ, μ , 令 $A_\lambda = A + \lambda I_n$, $B_\mu = B + \mu I_n$. 先对 $\mathbb{F}(\lambda, \mu)$ 上的可逆矩阵 A_λ, B_μ 利用 $A_\lambda^* = (\det A_\lambda)A_\lambda^{-1}$ 建立等式 $(A_\lambda B_\mu)^* = B_\mu^* A_\lambda^*$, 再注意到两边的矩阵元素都是 λ, μ 的多项式, 从而这是 $\mathbb{F}[\lambda, \mu]$ 中的多项式恒等式, 令 $\lambda = \mu = 0$ 即得.)

习题 6.21 (从有限域到有理数的提升). 设 $A \in M_{m \times n}(\mathbb{Z})$ 是整数系数矩阵, $b \in \mathbb{Z}^m$ 是整数向量. 假设对无穷多个素数 p , 线性方程组 $Ax \equiv b \pmod{p}$ (即视为 \mathbb{F}_p 上的方程组 $\bar{A}x = \bar{b}$) 有解. 证明方程组 $Ax = b$ 在 \mathbb{Q} 上有解.

习题 6.22 ($PSL(2, \mathbb{F}_3)$ 的阶与同构类型). 记

$$\text{SL}(2, \mathbb{F}_3) = \{A \in M_2(\mathbb{F}_3) \mid \det(A) = 1\},$$

$PSL(2, \mathbb{F}_3)$ 为商群

$$\text{SL}(2, \mathbb{F}_3) / \{\lambda I \mid \lambda \in \mathbb{F}_3^\times\}.$$

1. 计算 $PSL(2, \mathbb{F}_3)$ 的阶数.

2. 证明 $PSL(2, \mathbb{F}_3)$ 同构于交错群 A_4 。

习题 6.23 (\mathbb{F}_2 上的非退化二次型). 设 $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ 。称映射 $Q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ 为二次型, 若

$$Q(x) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j.$$

定义双线性形式

$$B(x, y) = Q(x + y) - Q(x) - Q(y).$$

若对每个 $x \neq 0$ 存在 y 使 $B(x, y) = 1$, 称 Q 非退化。证明:

1. $B(x, x) = 0$ 对所有 $x \in \mathbb{F}_2^n$ 成立。
2. \mathbb{F}_2^n 上每个非退化二次型都存在一组辛基。
3. 当 $n = 2$ 时, 非退化二次型在同构意义下恰好有两类。
4. \mathbb{F}_2^6 上的非退化二次型在同构意义下恰好有两种。

习题 6.24 (有限域计数与 q -组合恒等式). 设 V 是 \mathbb{F}_q 上的 n 维线性空间, 其中 q 为素数幂。

1. 证明 V 中所有 k 维子空间的个数为高斯二项式系数

$$\#G(k, n; \mathbb{F}_q) = \binom{n}{k}_q,$$

从而 V 中所有子空间的个数为

$$S_n(q) = \sum_{k=0}^n \binom{n}{k}_q.$$

2. 通过直接计数 $V \times V$ 中满足 $(v, w) \in W \times W$ 的有序对 $((v, w), W)$, 其中 W 遍历 V 的所有子空间, 证明

$$\sum_{k=0}^n q^{2k} \binom{n}{k}_q = S_n(q) + (q^2 - 1) \binom{n}{1}_q S_{n-1}(q) + (q^2 - 1)(q^2 - q) \binom{n}{2}_q S_{n-2}(q),$$

其中约定 $S_m(q) = 0$ 当 $m < 0$ 。提示: 按 $\dim \text{span}\{v, w\} = 0, 1, 2$ 分类; 若 $\dim \text{span}\{v, w\} = r$, 则包含 $\text{span}\{v, w\}$ 的子空间个数等于 $S_{n-r}(q)$ 。

3. 设 $n \geq 1$ 。通过计算 \mathbb{F}_q^n 中的完全旗

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = \mathbb{F}_q^n, \quad \dim V_i = i,$$

的个数, 证明

$$\#\{\text{完全旗}\} = \prod_{k=1}^n \frac{q^k - 1}{q - 1} = [n]_q!.$$

4. 对上述恒等式两边视为关于 q 的多项式或有理函数, 说明它们作为 \mathbb{Q} 上的恒等式成立, 并解释 $[n]_q! \rightarrow n!$ 在 $q \rightarrow 1$ 时的含义。

习题 6.25 (模 p 下的二元二次表示). 假设 p 是一个素数, $a, b, c \in \mathbb{Z}$, 且 $ab \not\equiv 0 \pmod{p}$. 证明: 存在 $x, y \in \mathbb{Z}$ 使得

$$ax^2 + by^2 \equiv c \pmod{p}.$$

习题 6.26 (主同余子群中的有限阶元). 记 $\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$. 设 p 为素数, 定义

$$\Gamma(p) = \{A \in \mathrm{GL}_n(\mathbb{Z}) \mid A \equiv I_n \pmod{p}\}.$$

设 $A \in \Gamma(p)$, 并且 A 是有限阶元。证明:

1. 若 $A \neq I_n$, 存在整数 $r \geq 1$ 及整数矩阵 B , 使得

$$A = I_n + p^r B, \quad B \not\equiv 0 \pmod{p}.$$

2. 若素数 ℓ 满足 $A^\ell = I_n$ 且 $\ell \neq p$, 则 $A = I_n$ 。

3. 当 $p \geq 3$ 时, $\Gamma(p)$ 中的有限阶元只有平凡元素。

4. 当 $p = 2$ 时, 给出 $\Gamma(2)$ 中一个非恒等的有限阶元素。

7 多项式

在线性代数的进阶学习中, 我们经常需要借助多项式来研究线性变换的结构. 本章我们将简要复习并总结域 \mathbb{F} 上一元多项式的基本理论, 特别是带余除法、最大公因式、不可约多项式与唯一分解定理等概念, 为下一章特征值理论与若尔当标准型的学习做好必要的代数准备.

多项式之所以在代数学中占据中心位置, 并不是偶然的. 从低次方程的经典求解到 Galois 理论的诞生, “多项式如何分解” 始终是代数学的主线之一. 因而这一章虽然是在为后文做准备, 讨论的却是代数学最核心的一批对象.

从线性代数的角度看, 多项式也会不断出现. 对 Fibonacci 型递推尝试代入 $a_n = r^n$ 就会导出多项式方程; 在线性递推、矩阵幂和常系数微分方程中, 特征多项式更是核心角色. 在编码理论中, CRC 和 Reed-Solomon 码又要依赖有限域上的带余除法与插值. 因此本章介绍的是一门之后会反复回头使用的共同语言.

7.1 多项式环

设 \mathbb{F} 是一个域. 域 \mathbb{F} 上的一个一元多项式可以表示为形式和

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

其中 $a_i \in \mathbb{F}$, 且 x 是一个形式变量. 若 $a_n \neq 0$, 我们称 n 为该多项式的**次数** (degree), 记作 $\deg f = n$. 此时 a_n 称为**首项系数** (leading coefficient). 当首项系数 $a_n = 1$ 时, 称 $f(x)$ 为**首一多项式** (monic polynomial).

对于非零常数多项式 $f(x) = c \neq 0$, 其次数为 0. 我们特别规定零多项式 $f(x) = 0$ 的次数为 $\deg 0 = -\infty$. 在这一约定下, 对于任意两个多项式 $f(x), g(x)$, 都有

$$\deg(f + g) \leq \max(\deg f, \deg g), \quad \deg(fg) = \deg f + \deg g.$$

所有系数在域 \mathbb{F} 中的多项式全体构成一个集合, 记作 $\mathbb{F}[x]$. 在定义了普通的多项式加法和乘法后, $\mathbb{F}[x]$ 构成一个环, 称为域 \mathbb{F} 上的**多项式环** (polynomial ring). 由于域 \mathbb{F} 中没有零因子, 并且乘法可交换, $\mathbb{F}[x]$ 也是一个无零因子的交换环 (即整环).

7.2 带余除法与整除

与整数环 \mathbb{Z} 类似, 多项式环中最基础的工具是带余除法.

定理 7.1 (带余除法). 设 $f(x), g(x) \in \mathbb{F}[x]$, 并且 $g(x) \neq 0$. 则存在唯一的多项式 $q(x)$ (商) 与 $r(x)$ (余数) 满足:

$$f(x) = g(x)q(x) + r(x), \quad \text{其中 } \deg r < \deg g.$$

证明. **存在性.** 对 $\deg f$ 进行数学归纳法. 若 $\deg f < \deg g$, 取 $q = 0, r = f$ 即可.

设 $\deg f = m \geq \deg g = n$, 且对所有次数小于 m 的多项式结论成立. 设 f 的首项系数为 a , g 的首项系数为 b , 令

$$f_1(x) = f(x) - \frac{a}{b} x^{m-n} g(x).$$

则 f_1 的最高次项被消去, 故 $\deg f_1 < m$. 由归纳假设, 存在 q_1, r 使得 $f_1 = g q_1 + r$, 且 $\deg r < \deg g$. 于是

$$f = \frac{a}{b} x^{m-n} g + f_1 = g \left(\frac{a}{b} x^{m-n} + q_1 \right) + r,$$

取 $q = \frac{a}{b} x^{m-n} + q_1$ 即满足要求.

唯一性. 假设 $f = g q_1 + r_1 = g q_2 + r_2$, 其中 $\deg r_1, \deg r_2 < \deg g$. 则 $g(q_1 - q_2) = r_2 - r_1$. 若 $q_1 \neq q_2$, 则左边的次数 $\geq \deg g$, 而右边的次数 $< \deg g$, 矛盾. 因此 $q_1 = q_2$, 从而 $r_1 = r_2$. \square

定义 7.1 (整除). 设 $f(x), g(x) \in \mathbb{F}[x]$. 若存在 $h(x) \in \mathbb{F}[x]$ 使得 $f(x) = g(x)h(x)$, 我们就称 $g(x)$ **整除** (*divides*) $f(x)$, 记为 $g(x) \mid f(x)$, 并称 $g(x)$ 是 $f(x)$ 的**因式** (*factor*). 若 $g(x)$ 不整除 $f(x)$, 记为 $g(x) \nmid f(x)$.

注 7.1. 按此定义, 任何多项式都整除零多项式 (取 $h = 0$), 零多项式只整除自身. 非零常数 $c \in \mathbb{F}^*$ 整除任何多项式 (因为 $f = c \cdot (c^{-1}f)$), 这类因式称为**平凡因式**.

可以验证, 整除关系具有传递性: 若 $f \mid g, g \mid h$, 则 $f \mid h$. 此外若 $f \mid g$ 且 $f \mid h$, 则对任意 $u, v \in \mathbb{F}[x]$, 有 $f \mid (ug + vh)$. 若 $f \mid g$ 且 $g \mid f$, 则 f, g 次数相同并且相差一个非零常数倍 (称它们相伴). 任何非零多项式都唯一相伴于一个首一多项式.

7.3 最大公因式与辗转相除法

辗转相除法为什么重要

整数的辗转相除法可以求最大公因数, 多项式的辗转相除法也可以求最大公因式. 它的意义不止是“算一个 gcd”: 在纠错码中, 接收端要根据校验信息推断错误位置和错误大小, 这会转化为多项式方程; 求解这些方程的核心步骤之一就是多项式欧几里得算法. 后面研究极小多项式和有理标准型时, 同样会不断用到“互素多项式可以通过裴蜀恒等式拼出 1”这一思想.

定义 7.2 (最大公因式). 设 $f(x), g(x) \in \mathbb{F}[x]$, 不同时为零. 若多项式 $d(x) \in \mathbb{F}[x]$ 满足:

- (1) $d(x)$ 既是 $f(x)$ 的因式, 也是 $g(x)$ 的因式 (即 $d \mid f, d \mid g$);
- (2) 对于任意使得 $h \mid f$ 且 $h \mid g$ 的多项式 $h(x)$, 都有 $h \mid d$;

7.4 裴蜀定理与互素

辗转相除法不仅可以用来计算最大公因式,我们将这个除法过程倒推还能得出关于最大公因式最为重要的代数性质:

定理 7.3 (裴蜀定理, Bézout's Identity). 对于不全为零的多项式 $f(x), g(x) \in \mathbb{F}[x]$, 存在多项式 $u(x), v(x) \in \mathbb{F}[x]$, 使得

$$u(x)f(x) + v(x)g(x) = \gcd(f(x), g(x)).$$

证明. 在辗转相除法 (定理7.2) 中, 第一步给出 $r_1 = f - q_1g$, 第二步给出 $r_2 = g - q_2r_1 = -q_2f + (1 + q_1q_2)g$. 如此反复代入, 每一个余数 r_i 都可以表示为 f 和 g 的 $\mathbb{F}[x]$ -线性组合. 最终, 最后一个非零余数 r_k 即为 $\gcd(f, g)$ (至多相差一个常数倍), 从而 $\gcd(f, g) = uf + vg$. \square

例 7.2 (裴蜀恒等式的计算). 续例7.1. 辗转相除法给出 $x - 1 = (x^3 - 1) - (x^2 - 1) \cdot x$, 因此取 $u = 1, v = -x$ 即有

$$1 \cdot (x^3 - 1) + (-x) \cdot (x^2 - 1) = x - 1 = \gcd(x^3 - 1, x^2 - 1).$$

这一恒等式在线性代数中有极其广泛的应用, 它能够将多项式的整除关系转化为可以直接计算的代数等式.

定义 7.3 (互素). 若 $\gcd(f, g) = 1$, 我们称 $f(x)$ 与 $g(x)$ **互素** (*coprime*). 此时存在多项式 u, v 使得 $uf + vg = 1$.

互素性质有许多深刻的代数推论, 比如:

引理 7.2. 若 $h \mid fg$, 且 $\gcd(h, f) = 1$, 则 $h \mid g$.

证明. 既然 $\gcd(h, f) = 1$, 根据定理7.3存在 u, v 使得 $uh + vf = 1$. 两边同乘 g 得到 $uhg + vfg = g$. 注意到 h 整除 uhg , 并且因为 $h \mid fg$, h 也整除 $v(fg)$. 所以 h 整除上述两者之和, 故 $h \mid (uhg + vfg) = g$. \square

引理 7.3 (互素乘积整除). 若 f, g 互素, 且 $f \mid h, g \mid h$, 则 $fg \mid h$.

证明. 由 $f \mid h$ 写 $h = fh_1$, 则 $g \mid fh_1$. 因为 $\gcd(f, g) = 1$, 由引理7.2知 $g \mid h_1$, 从而 $fg \mid h$. \square

上述结果可以推广到多个多项式的情形:

定义 7.4 (多个多项式的最大公因式). 对于 $f_1, \dots, f_s \in \mathbb{F}[x]$ (不全为零), 递归地定义

$$\gcd(f_1, \dots, f_s) = \gcd(\gcd(f_1, \dots, f_{s-1}), f_s).$$

可以验证这一定义不依赖于多项式的排列顺序.

推论 7.1 (多元裴蜀恒等式). 若 $\gcd(f_1, \dots, f_s) = 1$, 则存在 $u_1, \dots, u_s \in \mathbb{F}[x]$ 使得

$$u_1 f_1 + \dots + u_s f_s = 1.$$

证明. 对 s 进行归纳. $s = 2$ 即为裴蜀定理 (定理 7.3). 设 $s \geq 3$, 令 $d = \gcd(f_1, \dots, f_{s-1})$, 则 $\gcd(d, f_s) = 1$, 存在 a, b 使得 $ad + bf_s = 1$. 由归纳假设, 存在 v_1, \dots, v_{s-1} 使得 $v_1 f_1 + \dots + v_{s-1} f_{s-1} = d$. 代入即得 $\sum_{i=1}^{s-1} (av_i) f_i + bf_s = 1$. \square

7.5 不可约多项式与唯一分解定理

定义 7.5 (不可约多项式). 设多项式 $p(x) \in \mathbb{F}[x]$ 满足 $\deg p \geq 1$. 若 $p(x)$ 不能表示为两个次数严格小于 $\deg p$ 的多项式的乘积, 则称 $p(x)$ 为域 \mathbb{F} 上的**不可约多项式** (*irreducible polynomial*). 反之, 则称为可约多项式.

例 7.3 (不可约性依赖于底域). 多项式 $x^2 + 1$ 在不同的域上有截然不同的表现:

- (1) 在 $\mathbb{R}[x]$ 中不可约: 它没有实数根, 而 2 次多项式可约等价于有根.
- (2) 在 $\mathbb{C}[x]$ 中可约: $x^2 + 1 = (x + i)(x - i)$.
- (3) 在 $\mathbb{F}_2[x]$ 中可约: $x^2 + 1 = (x + 1)^2$ (因为 \mathbb{F}_2 中 $-1 = 1$).

不可约多项式在多项式环中扮演了整数环中素数的地位. 对于不可约多项式 $p(x)$, 唯一的因式只有非零常数和与它相伴的多项式.

命题 7.1 (不可约多项式的素性). 若 $p(x)$ 是不可约多项式, 且 $p \mid fg$, 则 $p \mid f$ 或 $p \mid g$.

证明. 若 $p \nmid f$, 由于 p 不可约, p 的因式只有非零常数和常数倍的 p 本身, 从而 $\gcd(p, f) = 1$. 由引理 7.2 即知 $p \mid g$. \square

定理 7.4 (多项式唯一分解定理). 域 \mathbb{F} 上的任一非零且次数 ≥ 1 的多项式 $f(x)$ 都可以唯一地写成

$$f(x) = c p_1(x)^{m_1} p_2(x)^{m_2} \cdots p_k(x)^{m_k},$$

其中 $c \in \mathbb{F}$ 是首项系数, $p_i(x)$ 是互不相同的首一不可约多项式, $m_i \geq 1$ 是正整数. “唯一”意味着除了因式的排列顺序不同外, 该分解方式在 $\mathbb{F}[x]$ 中是确定的.

证明. **存在性.** 对 $\deg f$ 进行归纳. 若 $\deg f = 1$, 则 f 本身 (至多相差一个常数) 即为首一不可约多项式. 设 $\deg f \geq 2$: 若 f 不可约, 则 $f = c \cdot \tilde{f}$ (\tilde{f} 为相应首一不可约多项式), 结论成立; 若 f 可约, 则 $f = g \cdot h$, 其中 $1 \leq \deg g, \deg h < \deg f$. 由归纳假设, g 和 h 各自有不可约分解, 将它们乘在一起即得 f 的不可约分解.

唯一性. 假设 f 有两种分解:

$$c p_1^{m_1} \cdots p_k^{m_k} = c' q_1^{n_1} \cdots q_l^{n_l}.$$

比较首项系数可知 $c = c'$. 因为 $p_1 \mid q_1^{n_1} \cdots q_l^{n_l}$, 根据命题7.1(反复应用), 必有某个 j 使得 $p_1 \mid q_j$. 因为 p_1 和 q_j 都是首一不可约多项式, 故 $p_1 = q_j$. 两边消去一个 p_1 (利用 $\mathbb{F}[x]$ 无零因子), 对消去后的多项式次数进行归纳, 即可证明两种分解的不可约因子完全相同 (包括重数). \square

7.6 多项式的根与形式导数

定义 7.6 (代入与根). 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$, $\lambda \in \mathbb{F}$. 将 λ 代入 $f(x)$ 得到域元素

$$f(\lambda) = a_n \lambda^n + \cdots + a_1 \lambda + a_0 \in \mathbb{F}.$$

映射 $\text{ev}_\lambda: \mathbb{F}[x] \rightarrow \mathbb{F}$, $f(x) \mapsto f(\lambda)$ 称为在 λ 处的**赋值映射** (evaluation map), 不难验证它是环同态. 若 $f(\lambda) = 0$, 则称 λ 为 $f(x)$ 的一个**根** (root).

利用带余除法 (定理7.1), 设 $f(x) = (x - \lambda)q(x) + r$, 由于 $\deg r < \deg(x - \lambda) = 1$, r 必须是一个常数. 代入 $x = \lambda$ 可得 $r = f(\lambda)$. 于是我们有:

定理 7.5 (余数定理与因式定理). 设 $f(x) \in \mathbb{F}[x]$, $\lambda \in \mathbb{F}$. 则:

- (1) (余数定理) $f(x)$ 除以 $(x - \lambda)$ 的余数为 $f(\lambda)$.
- (2) (因式定理) $(x - \lambda) \mid f(x)$ 当且仅当 λ 是 $f(x)$ 的根.

进而结合互素概念, 若 $\lambda_1, \dots, \lambda_k$ 为 f 的互不相同的根, 由于 $(x - \lambda_i)$ 两两互素, 可以归纳地利用引理7.2证明 $\prod_{i=1}^k (x - \lambda_i)$ 整除 $f(x)$. 比较次数即得:

推论 7.2. 域 \mathbb{F} 上任意一个非零的 n 次多项式 $f(x)$ 在 \mathbb{F} 中最多只有 n 个根.

注 7.2. 这一推论虽然简单, 但非常重要. 例如, 它在 §6.7中恒等式原理的证明中发挥了关键作用.

推论7.2给出了根的个数的上界. 一个自然的问题是: 根是否一定存在? 这取决于底域的性质. 例如, $x^2 + 1 \in \mathbb{R}[x]$ 没有实数根. 然而, 复数域具有一个根本性的完备性质:

定理 7.6 (代数基本定理, Fundamental Theorem of Algebra). $\mathbb{C}[x]$ 中任何一个次数 ≥ 1 的多项式至少有一个根.

代数基本定理的证明需要用到分析学 (如拓扑学或复分析) 的工具, 超出了本书的范围⁹. 但我们可以从中推出多项式分解的重要结论:

⁹代数基本定理有多种不同风格的证明: 利用复分析中的刘维尔定理, 利用拓扑学中的基本群, 或利用实分析中的介值定理配合代数论证等. 读者可参阅任何一本复分析教材中的相关章节.

推论 7.3 (复多项式环的不可约多项式). $\mathbb{C}[x]$ 中的不可约多项式恰好是一次多项式. 因此, 任何 n 次多项式 $f(x) \in \mathbb{C}[x]$ 都可以完全分解为一次因式的乘积:

$$f(x) = c(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n),$$

其中 $c \in \mathbb{C}^*$, $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ (允许重复, 即计入重数).

证明. 设 $p(x) \in \mathbb{C}[x]$ 为不可约多项式. 若 $\deg p \geq 2$, 由代数基本定理, p 有一个根 $\lambda \in \mathbb{C}$, 则由因式定理 (定理7.5(2)) $(x - \lambda) \mid p(x)$, 从而 $p(x) = (x - \lambda)q(x)$, 其中 $\deg q \geq 1$, 这与不可约矛盾. 故 $\mathbb{C}[x]$ 中的不可约多项式必为一次多项式. 再结合唯一分解定理 (定理7.4) 即得完全分解. \square

推论 7.4 (复系数多项式的根). $\mathbb{C}[x]$ 中任一 n 次多项式 ($n \geq 1$) 恰好有 n 个根 (计入重数).

代数基本定理对实系数多项式也有重要推论. 由于实系数多项式的复数根一定成对共轭出现 (即若 $\lambda \in \mathbb{C}$ 是 $f(x) \in \mathbb{R}[x]$ 的根, 则 $\bar{\lambda}$ 也是, 参见习题7.17), 这将给出 $\mathbb{R}[x]$ 中不可约多项式的完全分类 (参见习题7.19).

定义 7.7 (形式导数与重根). 对于 $f(x) = \sum_{k=0}^n a_k x^k$, 定义其**形式导数** (formal derivative) 为 $f'(x) = \sum_{k=1}^n k a_k x^{k-1}$. 我们称 λ 是 $f(x)$ 的 m **重根** (root of multiplicity m), 如果 $(x - \lambda)^m \mid f(x)$ 但 $(x - \lambda)^{m+1} \nmid f(x)$. 当 $m \geq 2$ 时称 λ 为**重根** (multiple root).

形式导数满足通常的莱布尼兹求导法则 $(fg)' = f'g + fg'$ 和线性性质 (可以直接从定义验证). 利用形式导数, 我们可以给出判断多项式是否有重因式的代数判别法:

命题 7.2 (重因式判别法). 设 \mathbb{F} 的特征为 0 (例如 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$). 多项式 $f(x) \in \mathbb{F}[x]$ ($\deg f \geq 1$) 没有重因式 (即在不可约分解中所有 $m_i = 1$) 当且仅当 $\gcd(f, f') = 1$.

证明. 先证明若 f 有重因式, 则 $\gcd(f, f') \neq 1$. 设存在不可约多项式 $p(x)$ 使得 $p^2 \mid f$, 写 $f = p^2 h$. 则 $f' = 2pp'h + p^2 h' = p(2p'h + ph')$, 所以 $p \mid f'$. 又 $p \mid f$, 故 $\gcd(f, f') \neq 1$.

反过来, 若 $\gcd(f, f') \neq 1$, 则存在不可约多项式 p 使得 $p \mid f$ 且 $p \mid f'$. 写 $f = pg$, 则 $f' = p'g + pg'$. 由 $p \mid f'$ 和 $p \mid pg'$ 知 $p \mid p'g$. 在特征 0 下, $\deg p' = \deg p - 1 \geq 0$ 且 $p' \neq 0$ (因为首项系数 $\deg p \cdot a_{\deg p} \neq 0$), 所以 $\gcd(p, p') = 1$ (因为 p 不可约且 $\deg p' < \deg p$). 由引理7.2知 $p \mid g$, 从而 $p^2 \mid f$, 即 f 有重因式. \square

7.7 习题

7.7.1 练习题

习题 7.1 (用裴蜀恒等式求多项式商空间中的逆). 在 $\mathbb{R}[x]/(x^2 + 1)$ 中, 求 $x + 1$ 的乘法逆元.

1. 用辗转相除法找到多项式 $u(x), v(x)$, 使得

$$u(x)(x+1) + v(x)(x^2+1) = 1.$$

2. 由此写出 $x+1$ 在商空间 $\mathbb{R}[x]/(x^2+1)$ 中的逆元.

3. 用直接乘法验证答案.

习题 7.2 (多项式带余除法). 在 $\mathbb{Q}[x]$ 中分别作带余除法:

1. $x^4 - 3x + 1$ 除以 $x^2 + 1$;

2. $2x^3 + x^2 - 1$ 除以 $x - 2$.

习题 7.3 (最大公因式). 用辗转相除法求 $\gcd(x^3 - x, x^2 - 1)$ 和 $\gcd(x^4 - 1, x^2 + x)$.

习题 7.4. 求在 $\mathbb{Q}[x]$ 和 $\mathbb{F}_2[x]$ 中多项式 $x^4 - 1$ 的不可约分解.

习题 7.5. 用辗转相除法求 $\gcd(x^4 + x^3 + x^2 + x + 1, x^3 + x^2 + 1)$ 在 $\mathbb{F}_2[x]$ 中的值, 并写出相应的裴蜀恒等式.

习题 7.6. 若多项式 $f(x)$ 和 $g(x)$ 的最大公因式为 1, 证明 $f(x)$ 和 $g^2(x)$ 的最大公因式也为 1.

习题 7.7. 设 f, g 互素, 且 $f | h, g | h$. 证明 $fg | h$.

习题 7.8. 设 $d = \gcd(f, g)$. 证明 $\gcd(f/d, g/d) = 1$.

习题 7.9. 设 p 为素数. 证明 $\mathbb{F}_p[x]$ 中的二次多项式 $f(x) = x^2 + bx + c$ 不可约当且仅当 f 在 \mathbb{F}_p 中没有根. 举例说明对于三次及以上的多项式, “没有根” 不等价于不可约.

习题 7.10. 假设 \mathbb{F} 为特征为 0 的域. 试证明 $\lambda \in \mathbb{F}$ 为多项式 $f(x)$ 的 m 重根当且仅当 $f(\lambda) = f'(\lambda) = \dots = f^{(m-1)}(\lambda) = 0$ 且 $f^{(m)}(\lambda) \neq 0$.

习题 7.11. 设 $f(x) \in \mathbb{F}[x]$, 定义 $\bar{f}(x) = f(x)/\gcd(f, f')$. 证明 \bar{f} 与 f 有相同的根 (不计重数), 且 \bar{f} 没有重根.

习题 7.12. 用多项式除法计算

$$x^3 - 1$$

除以 $x - 1$ 的商和余数。

习题 7.13. 求多项式 $x^2 - 5x + 6$ 的全部根, 并把它分解为一次因式的乘积。

习题 7.14. 求 $x^3 - x$ 与 $x^2 - 1$ 的最大公因式。

习题 7.15. 判断 $x = 2$ 是否为多项式 $p(x) = x^3 - 4x^2 + 5x - 2$ 的重根。

习题 7.16. 设矩阵

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

计算 $A^2 - 3A + 2I$, 并观察它与多项式 $(x-1)(x-2)$ 的关系。

7.7.2 思考题

习题 7.17 (共轭根定理). 设 $f(x) \in \mathbb{R}[x]$ 为实系数多项式, $\lambda = a + bi \in \mathbb{C} (b \neq 0)$ 为 f 的一个复数根. 证明:

(1) 其共轭 $\bar{\lambda} = a - bi$ 也是 f 的根, 且与 λ 有相同的重数.

(2) $(x - \lambda)(x - \bar{\lambda}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$, 即二次因式的系数均为实数.

(提示: 对于 (1), 利用共轭的性质 $\overline{f(\lambda)} = f(\bar{\lambda})$.)

习题 7.18 (奇数次实系数多项式必有实根). 设 $f(x) \in \mathbb{R}[x]$ 为奇数次多项式. 利用代数基本定理 (定理 7.6) 和习题 7.17 的结论, 证明 f 至少有一个实根. (也可以用实分析中的介值定理直接证明.)

习题 7.19 ($\mathbb{R}[x]$ 的不可约多项式分类). 利用代数基本定理和共轭根定理 (习题 7.17), 证明 $\mathbb{R}[x]$ 中的不可约多项式恰好是以下两类:

(1) 一次多项式 $ax + b (a \neq 0)$;

(2) 判别式为负的二次多项式 $ax^2 + bx + c (a \neq 0, b^2 - 4ac < 0)$.

由此推出: $\mathbb{R}[x]$ 中任一次数 ≥ 1 的多项式都可以分解为一次因式和判别式为负的二次因式的乘积.

习题 7.20 (实系数多项式的分解). 将以下多项式在 $\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 中分别分解为不可约因式的乘积:

(1) $x^4 + 1$;

(2) $x^4 + x^2 + 1$;

(3) $x^6 - 1$.

习题 7.21 (商空间上的乘法算子). 设 $f(x), g(x) \in \mathbb{C}[x]$ 为首一多项式, 且 $\deg f = n \geq 1, \deg g = m \geq 1$. 已知

$$f(x) = \prod_{i=1}^l (x - \lambda_i)^{n_i},$$

其中 λ_i 互不相同。定义商空间

$$V = \mathbb{C}[x]/(f)$$

上的线性变换

$$S(\bar{p}) = \overline{p(x)g(x)}.$$

1. 求 V 的维数。

2. 证明

$$\det(S) = \prod_{i=1}^l g(\lambda_i)^{n_i}.$$

3. 若 $g(x) = \prod_{i=1}^l (x - \lambda_i)^{m_i}$, 写出 S 可对角化的充要条件。

习题 7.22 (互素多项式与核分解). 设 V 是有理数域 \mathbb{Q} 上的有限维线性空间, $T \in \text{End}(V)$, $f, g \in \mathbb{Q}[x]$ 为互素多项式。若

$$f(T)g(T) = 0,$$

证明

$$V = \ker f(T) \oplus \ker g(T).$$

8 线性变换和特征值理论

在前面的章节中, 我们建立了域 \mathbb{F} 上线性空间的基本理论 (§6), 研究了行列式作为“体积”的代数度量 (§5), 并系统地发展了多项式的算术 (§7). 现在我们来到了线性代数最核心的问题之一: 给定线性空间 V 上的一个线性变换 $T: V \rightarrow V$, 能否找到一组“好的”基使得 T 在这组基下的矩阵尽可能简单?

最理想的情形是找到一组基, 使得 T 的矩阵变成对角矩阵——这就是**可对角化**问题. 对角矩阵的优点是显而易见的: 矩阵的幂次 A^k , 行列式 $\det A$, 方程 $(A - \lambda I)x = 0$ 的求解, 都变得完全平凡. 然而, 并非所有线性变换都可以对角化, 因此我们需要发展一套系统的理论来判断何时可以对角化, 以及当不能对角化时如何尽可能地简化矩阵表示.

本节的核心工具链如下: **特征值和特征向量**提供了对角化的候选基向量; **特征多项式**将寻找特征值的问题化为多项式求根的问题, 从而与 §7中建立的多项式理论衔接; **Cayley-Hamilton 定理**建立了矩阵与其特征多项式之间的深刻联系, 它断言每个矩阵都“满足”自己的特征多项式; 而**极小多项式**则精确地刻画了可对角化的充要条件. 这些工具的有效性在很大程度上依赖于 §3中发展的子空间直和分解与商空间的理论, 以及 §7中多项式整除与互素分解的结果.

特征值看长期趋势

若一个系统每一步都由同一个矩阵 A 更新, 即 $x_{k+1} = Ax_k$, 那么特征值和特征向量常常决定长期行为. 人口年龄结构模型中, 主特征值描述总人口的增长或衰减率, 主特征向量描述长期稳定的年龄比例; 耦合弹簧系统中, 特征向量给出正常振动模式, 特征值决定固有频率; 第 1 章中的 PageRank 模型本质上也是在寻找随机矩阵特征值 1 对应的稳定方向. 这些例子共同说明: 特征值理论的真正力量在于把复杂演化拆解为若干彼此独立的基本模式.

具体而言, 本节的组织结构如下:

- 在 §8.1中, 我们定义特征值、特征向量和特征多项式, 通过 2×2 矩阵和求导算子的具体例子建立直觉, 并看到并非所有线性变换都可以对角化.
- 在 §8.2中, 我们引入不变子空间的概念, 它是将线性变换“分块”研究的基本语言. 在此基础上, 我们证明复数域上的线性变换总可以上三角化, 并建立对角化的特征子空间判据.
- 在 §8.3中, 我们将上述理论翻译为矩阵语言, 重点阐明**相似分类**的观点: 对角化问题的本质是矩阵的相似等价类中是否包含对角矩阵. 我们还通过一个遗传学中的 Markov 链模型演示对角化在计算矩阵高次幂中的威力.
- 在 §8.5中, 我们引入代数重数和几何重数的概念, 将可对角化问题精确化为“每个特征值的几何重数是否等于代数重数”.

- 在 §8.6 中, 我们证明 Cayley-Hamilton 定理, 它是连接特征多项式与线性变换的代数性质的桥梁.
- 在 §8.7 中, 我们研究极小多项式, 给出可对角化的充要条件: 极小多项式在 $\mathbb{F}[\lambda]$ 中可分解为没有重根的一次因式的乘积.
- 在 §8.8 中, 我们引入友阵的概念, 建立多项式与矩阵之间的直接桥梁, 并证明矩阵相似于友阵当且仅当其极小多项式等于特征多项式. 友阵和循环向量的概念将在 §13 的若尔当标准型理论中发挥核心作用.

8.1 特征值与特征向量

我们从可对角化问题出发引入特征值和特征向量的概念. 回忆线性映射 $T: V \rightarrow V$ 在取定 V 的一组基之后可以表示为矩阵. 如果能找到一组“特别好”的基, 使得 T 在这组基下的矩阵成为对角矩阵, 那么 T 的许多性质都一目了然. 这就引出如下问题:

对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 能否找到 V 的一组基 $\{v_1, \dots, v_n\}$ 满足对任意的 $1 \leq i \leq n$ 有 $Tv_i = \lambda_i v_i$, 其中 $\lambda_i \in \mathbb{F}$, 称为线性映射的**可对角化** (diagonalizable) 问题. 用矩阵的语言来说, 给定矩阵 $A \in M_{n \times n}(\mathbb{F})$, 是否存在可逆矩阵 $P \in M_{n \times n}(\mathbb{F})$ 使得 $P^{-1}AP$ 是对角矩阵.

当 $\dim_{\mathbb{F}} V = 1$ 时是显然的, 因为任何 1×1 阶矩阵都是对角矩阵. 但是对一般的维数来说, 并不是所有的线性映射都是可对角化的. 考虑 $\dim_{\mathbb{F}} V = 2$ 的情形: 固定 V 的一组基 B 将 T 看作矩阵

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

那么 $0 \neq v \in V$ 满足 $Tv = \lambda v$, 其中 $\lambda \in \mathbb{F}$, 等价于 $(\lambda I_2 - A)v = 0$ 有非零解, 根据定理 2.1 以及命题 5.1 的 (2) 可知这等价于 λ 满足 $|\lambda I_2 - A| = 0$, 即

$$\lambda^2 - (a + d)\lambda + ad - bc = 0$$

我们考虑如下的情况:

- (1) 如果 $\lambda^2 - (a + d)\lambda + ad - bc = 0$ 不存在根, 那么一定不存在 V 的一组基 $\{v_1, v_2\}$ 使得 $Tv_i = \lambda_i v_i$, 其中 $i = 1, 2$.
- (2) 如果 $\lambda^2 - (a + d)\lambda + ad - bc = 0$ 有两个不同的根 λ_1, λ_2 , 那么对于每一个 λ_i 考虑 $(\lambda_i I_2 - A)v = 0$ 的非零解 v_i , 我们断言 $\{v_1, v_2\}$ 构成了一组基, 因此满足我们的要求: 假设 $\{v_1, v_2\}$ 线性相关, 不妨假设 $v_1 = \mu v_2$, 从而

$$\lambda_1 v_1 = Tv_1 = T(\mu v_2) = \mu \lambda_2 v_2.$$

这意味着 $\mu(\lambda_1 - \lambda_2) = 0$, 从而有 $\mu = 0$. 但 $v_1 = \mu v_2$ 会给出 $v_1 = 0$, 与 v_1 是特征向量矛盾. 因此 v_1, v_2 线性无关.

(3) 如果 $\lambda^2 - (a+d)\lambda + ad - bc = 0$ 有重根 λ , 我们要考虑 $\lambda I_2 - A$ 的秩:

(a) $\text{rank}(\lambda I_2 - A) = 0$, 此时根据推论4.2解空间的维数是 2, 因此可以找到两个线性无关的向量 $\{v_1, v_2\}$ 满足 $Tv_i = \lambda v_i$, 其中 $i = 1, 2$.

(b) $\text{rank}(\lambda I_2 - A) = 1$, 此时根据推论4.2解空间的维数是 1, 则此时找不到两个线性无关的向量.

定义 8.1. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, $\lambda \in \mathbb{F}$ 被称为 T 的**特征值** (*eigenvalue*), 如果存在 $0 \neq v \in V$ 使得

$$Tv = \lambda v.$$

此时 v 称为特征值 λ 对应的**特征向量** (*eigenvector*).

定义 8.2. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其中 $\dim_{\mathbb{F}} V = n$. 取定 V 的一组基, 将 T 表示为矩阵 $A \in M_{n \times n}(\mathbb{F})$, 定义关于 λ 的 n 次多项式 $\det(\lambda I_n - A)$ 为 T 的**特征多项式** (*characteristic polynomial*). 由于相似矩阵有相同的特征多项式, 故此定义与基的选取无关.

注 8.1. \mathbb{F} -线性映射 T 的特征值恰好是特征多项式在域 \mathbb{F} 中的根 (参见定义 7.6). 由推论 7.2, n 次多项式在 \mathbb{F} 中至多有 n 个不同的根, 因此 n 维线性空间上的线性映射至多有 n 个不同的特征值. 值得注意的是, 对于一般的域 \mathbb{F} , 特征多项式可能没有根, 此时 T 没有特征值.

例 8.1 (二阶矩阵的完整对角化). 考虑

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

其特征多项式为

$$\chi_A(\lambda) = \det \begin{pmatrix} \lambda - 2 & -1 \\ -1 & \lambda - 2 \end{pmatrix} = (\lambda - 3)(\lambda - 1).$$

对 $\lambda = 3$, 解 $(A - 3I)v = 0$ 得特征向量 $(1, 1)^T$; 对 $\lambda = 1$, 解 $(A - I)v = 0$ 得特征向量 $(1, -1)^T$. 取

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

则

$$P^{-1}AP = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

这个例子展示了对角化的基本流程: 求特征值, 求特征向量, 将特征向量作为 P 的列.

下面我们通过一个来自微积分的自然例子来说明: 即使在域 \mathbb{F} 包含特征多项式的全部根的情况下, 线性变换仍然可能不可对角化.

例 8.2 (求导算子). 设 $V = \mathbb{F}_n[x] = \{f(x) \in \mathbb{F}[x] \mid \deg f \leq n\}$ 是次数 $\leq n$ 的多项式构成的 \mathbb{F} -线性空间, 其中 \mathbb{F} 的特征为 0 (例如 $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$). 取标准基 $B = \{1, x, x^2, \dots, x^n\}$, 则 $\dim V = n + 1$. 考虑求导映射

$$D: V \rightarrow V, \quad f(x) \mapsto f'(x).$$

由于 $D(x^k) = kx^{k-1}$, D 在基 B 下的表示矩阵为

$$[D]_B^B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

这是一个严格上三角矩阵, 因此其特征多项式为 $\chi_D(\lambda) = \lambda^{n+1}$, 唯一的特征值为 $\lambda = 0$, 代数重数为 $n + 1$.

然而, 求解 $Df = 0$ (即 $f'(x) = 0$) 可知 $V_0 = \ker D = \text{span}\{1\}$, 几何重数仅为 1. 由于 $1 < n + 1$ (当 $n \geq 1$ 时), 特征子空间 V_0 远不足以张成整个 V , 因此 D **不可对角化**.

值得注意的是, D 在标准基下的矩阵已经是上三角矩阵. 这提示我们: 即使无法对角化, 线性变换也可能存在一组基使其表示矩阵为上三角形式. 上三角矩阵虽不如对角矩阵那样简洁, 但其对角线上的元素仍然是全部特征值 (计入重数), 而且矩阵的幂次、行列式、可逆性等性质都易于读出. 在下一小节中, 我们将证明: 只要底层域是代数闭域 (如 \mathbb{C}), **任何**线性变换都可以上三角化.

8.2 不变子空间和上三角化

为了证明上三角化定理, 我们需要引入**不变子空间**的概念. 它是将线性变换“分块”研究的基本语言, 也是后续若尔当标准型理论的出发点.

定义 8.3 (不变子空间). 设 $T: V \rightarrow V$ 是 \mathbb{F} -线性映射, $W \subset V$ 为子空间. 若 $T(W) \subset W$, 则称 W 为 T 的一个**不变子空间** (*invariant subspace*).

若 W 是 T -不变子空间, 则 T 限制在 W 上得到线性映射 $T|_W: W \rightarrow W$; 同时 T 在商空间上诱导出映射 $\bar{T}: V/W \rightarrow V/W$ (参见命题 4.11). 取 W 的一组基并将其扩充为 V 的基, 则 T 在此基下的矩阵具有分块上三角的形式 (参见命题 4.10):

$$[T]_B = \begin{pmatrix} [T|_W] & * \\ \mathbf{0} & [\bar{T}] \end{pmatrix}.$$

注意到特征子空间 $\ker(\lambda I - T)$ 就是一个典型的 T -不变子空间. 下面我们利用不变子空间的观点来证明: 在复数域上, 每个线性变换都可以上三角化.

命题 8.1. 假设 V 是 n 维 \mathbb{C} -线性空间, 给定 \mathbb{C} -线性映射 $T: V \rightarrow V$, 存在 V 的一组基 B 使得 $[T]_B^B$ 是上三角矩阵.

证明. 我们对维数 n 做归纳法. 当 $n = 1$ 的时候是显然的. 假设命题对维数 $< n$ 都成立. 由于 \mathbb{C} 是代数闭域, T 的特征多项式在 \mathbb{C} 中必有根 (定理 7.6), 即 T 存在特征值 λ_1 及对应的非零特征向量 v_1 .

令 $W = \text{span}\{v_1\}$, 则 W 是 T -不变子空间 (定义 8.3). 由命题 4.11, T 在商空间 V/W 上诱导出 \mathbb{C} -线性映射 $\bar{T}: V/W \rightarrow V/W$. 由于 $\dim(V/W) = n - 1 < n$, 根据归纳假设, 存在 V/W 的一组基 $\{\bar{v}_2, \dots, \bar{v}_n\}$ 使得 \bar{T} 在这组基下的矩阵为上三角矩阵.

在 V 中选取 \bar{v}_i 的代表元 $v_i \in V (2 \leq i \leq n)$, 则 $B = \{v_1, v_2, \dots, v_n\}$ 构成 V 的一组基. 由命题 4.10, T 在此基下的矩阵具有分块上三角形式:

$$[T]_B^B = \begin{pmatrix} \lambda_1 & * \\ 0 & [\bar{T}] \end{pmatrix},$$

其中 $[\bar{T}]$ 已经是上三角矩阵, 因此 $[T]_B^B$ 也是上三角矩阵. □

推论 8.1. 对于 \mathbb{C} -线性映射 $T: V \rightarrow V$, 其特征值恰为 $[T]_B^B$ 对角线上的元素, 其中 B 是使得 $[T]_B^B$ 为上三角矩阵的基.

定义 8.4. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 全体特征值 λ 对应的特征向量构成了一个 \mathbb{F} -线性空间, 称为特征值 λ 的**特征子空间** (eigenspace), 记做 V_λ .

命题 8.2. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$ 以及其特征值 λ , 有

$$V_\lambda = \ker(\lambda I - T).$$

证明. 根据定义即可. □

下面的引理是对角化理论的一个基石性结果:

引理 8.1. 设 $T: V \rightarrow V$ 是 \mathbb{F} -线性映射, $\lambda_1, \dots, \lambda_k$ 是 T 的两两不同的特征值, v_i 是 λ_i 对应的非零特征向量, 则 v_1, \dots, v_k 线性无关.

证明. 对 k 做归纳法. 当 $k = 1$ 时, $v_1 \neq 0$ 故线性无关. 假设对 $k - 1$ 个不同特征值结论成立, 现设

$$a_1 v_1 + a_2 v_2 + \dots + a_k v_k = 0.$$

对上式两端作用 $T - \lambda_k I$, 注意到 $(T - \lambda_k I)v_i = (\lambda_i - \lambda_k)v_i$, 从而

$$a_1(\lambda_1 - \lambda_k)v_1 + a_2(\lambda_2 - \lambda_k)v_2 + \dots + a_{k-1}(\lambda_{k-1} - \lambda_k)v_{k-1} = 0.$$

由归纳假设 v_1, \dots, v_{k-1} 线性无关, 因此 $a_i(\lambda_i - \lambda_k) = 0$ 对所有 $1 \leq i \leq k - 1$ 成立. 又因为 $\lambda_i \neq \lambda_k$, 所以 $a_1 = \dots = a_{k-1} = 0$, 代回原式得 $a_k v_k = 0$, 由 $v_k \neq 0$ 知 $a_k = 0$. □

定理 8.1. \mathbb{F} -线性映射 $T: V \rightarrow V$ 可对角化当且仅当 V 有特征子空间分解, 即 $V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$, 其中 $\lambda_1, \dots, \lambda_s$ 是 T 的全体不同特征值.

证明. 假设 $V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$, 则任取 $V_{\lambda_1}, \dots, V_{\lambda_s}$ 的基, 将其并起来得到 V 的一组基, 则在这组基下 T 对应的矩阵是对角矩阵; 另一方面, 假设 T 可对角化, 则可以找到 V 的一组由特征向量构成的基, 这组基给出了 V 的特征子空间分解. \square

8.3 矩阵的相似与对角化

前两小节中, 我们用线性映射的语言建立了特征值理论. 在实际计算和应用中, 我们常常直接面对矩阵. 本小节将上述结果翻译为矩阵语言, 并重点阐明**相似分类**的观点: 对角化问题的本质是矩阵的相似等价类中是否包含一个对角矩阵.

定义 8.5 (矩阵的相似). 矩阵 $A, B \in M_{n \times n}(\mathbb{F})$ 称为**相似的** (*similar*), 如果存在可逆矩阵 $P \in GL_n(\mathbb{F})$ 使得 $B = P^{-1}AP$.

相似关系是一个等价关系, 它将 $M_{n \times n}(\mathbb{F})$ 分成若干不相交的**相似等价类**. 同一个等价类中的所有矩阵不过是同一个线性映射在不同基下的表示矩阵: 若 $A = [T]_B^B$, P 是从基 B' 到基 B 的过渡矩阵, 则 $P^{-1}AP = [T]_{B'}^{B'}$. 因此, 与基的选取无关的不变量 (如行列式、秩、迹、特征多项式等) 在相似矩阵之间保持不变.

命题 8.3. 相似矩阵有相同的特征多项式, 从而有相同的特征值 (含代数重数)、相同的行列式和相同的迹.

证明. 设 $B = P^{-1}AP$, 则

$$\det(\lambda I_n - B) = \det(\lambda I_n - P^{-1}AP) = \det(P^{-1}(\lambda I_n - A)P) = \det(\lambda I_n - A).$$

行列式是特征多项式的常数项 (至差一个符号), 迹是特征多项式 λ^{n-1} 项的系数 (至差一个符号), 故它们也相同. \square

需要注意的是, 特征多项式相同**不能**保证矩阵相似. 例如 I_2 和 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 有相同的特征多项式 $(\lambda - 1)^2$, 但它们不相似. 完全的相似不变量需要用到若尔当标准型 (参见 §13).

利用相似关系, 我们可以将线性映射版的对角化判据直接翻译为矩阵语言:

定义 8.6 (矩阵的可对角化). 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 称为**可对角化的** (*diagonalizable*), 如果 A 相似于一个对角矩阵, 即存在可逆矩阵 P 使得 $P^{-1}AP$ 是对角矩阵. 等价地, A 作为 \mathbb{F}^n 上的线性变换 $x \mapsto Ax$ 是可对角化的.

定理 8.2. 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 可对角化当且仅当 \mathbb{F}^n 有特征子空间分解, 即 $\mathbb{F}^n = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$, 其中 $\lambda_1, \dots, \lambda_s$ 是 A 的全体不同特征值.

证明. 将 A 视为 \mathbb{F}^n 上的线性变换, 直接应用定理 8.1 即可. \square

注 8.2. 将 A 可对角化写成 $A = P\Lambda P^{-1}$ 的形式 (其中 Λ 是对角矩阵), 则 P 的各列恰好是 A 的特征向量, Λ 的对角元素是对应的特征值.

对角化的一个重要应用是高效计算矩阵的幂次. 若 $A = P\Lambda P^{-1}$, 其中 $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_n)$, 则

$$A^k = P\Lambda^k P^{-1} = P \text{diag}(\lambda_1^k, \dots, \lambda_n^k) P^{-1}, \quad (9)$$

对角矩阵的幂次是平凡的, 因此只需一次对角化就能将 A^k 的计算化为代数运算. 这在动态系统、概率论 (Markov 链) 和递推数列的求解中有广泛应用. 下面我们用一个遗传学中的 Markov 链模型来演示.

例 8.3 (基因型频率的演化). 考虑一个群体遗传学中的 **自体受精** (*selfing*) 模型. 某基因座有两个等位基因 A 和 a , 基因型分为 AA 、 Aa 、 aa 三种, 设第 k 代的频率向量为 $\mathbf{x}_k = (x_{AA}, x_{Aa}, x_{aa})^T$. 在自体受精中, 每个个体与自身交配产生后代, 后代基因型由 Mendel 遗传定律决定:

- 基因型 AA 的个体自交, 后代全为 AA ;
- 基因型 Aa 的个体自交, 后代按 $AA : Aa : aa = \frac{1}{4} : \frac{1}{2} : \frac{1}{4}$ 分布;
- 基因型 aa 的个体自交, 后代全为 aa .

因此, 下一代中 AA 的频率为 $x_{AA} \cdot 1 + x_{Aa} \cdot \frac{1}{4} + x_{aa} \cdot 0$, 其余类推. 将三种基因型的转移规则写成列向量, 恰好给出矩阵乘法 $\mathbf{x}_{k+1} = M\mathbf{x}_k$, 其中转移矩阵为

$$M = \begin{pmatrix} 1 & \frac{1}{4} & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{4} & 1 \end{pmatrix}.$$

经过 k 代后频率为 $\mathbf{x}_k = M^k \mathbf{x}_0$. 我们用对角化来计算 M^k .

(1) **特征多项式与特征值.** M 是分块上三角矩阵, 计算得

$$\chi_M(\lambda) = \det(\lambda I_3 - M) = (\lambda - 1)^2 \left(\lambda - \frac{1}{2} \right).$$

特征值为 $\lambda_1 = 1$ (代数重数 2) 和 $\lambda_2 = \frac{1}{2}$ (代数重数 1).

(2) **特征子空间与对角化.** 对 $\lambda_1 = 1$, 解 $(I_3 - M)\mathbf{v} = \mathbf{0}$ 得

$$V_1 = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\},$$

几何重数 = 2 = 代数重数. 对 $\lambda_2 = \frac{1}{2}$, 解 $(\frac{1}{2}\mathbf{I}_3 - M)\mathbf{v} = \mathbf{0}$ 得

$$V_{1/2} = \text{span} \left\{ \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right\}.$$

取过渡矩阵

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

则 $P^{-1}MP = \text{diag}(1, 1, \frac{1}{2})$.

(3) 计算 M^k . 根据(9),

$$M^k = P \text{diag} \left(1, 1, \frac{1}{2^k} \right) P^{-1}.$$

令 $k \rightarrow \infty$, 由于 $\frac{1}{2^k} \rightarrow 0$, 得到

$$\lim_{k \rightarrow \infty} M^k = P \text{diag}(1, 1, 0) P^{-1} = \begin{pmatrix} 1 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \\ 0 & \frac{1}{2} & 1 \end{pmatrix}.$$

从而

$$\mathbf{x}_\infty = \lim_{k \rightarrow \infty} M^k \mathbf{x}_0 = \begin{pmatrix} x_{AA} + \frac{1}{2}x_{Aa} \\ 0 \\ x_{aa} + \frac{1}{2}x_{Aa} \end{pmatrix} = \begin{pmatrix} p \\ 0 \\ q \end{pmatrix},$$

其中 $p = x_{AA} + \frac{1}{2}x_{Aa}$ 和 $q = x_{aa} + \frac{1}{2}x_{Aa}$ 正是初始群体中等位基因 A 和 a 的频率. 这意味着: 经过若干代自体受精后, 杂合子 Aa 的比例趋于零, 群体最终**完全纯合化**, 纯合子 AA 和 aa 的比例恰好等于初始等位基因频率 p 和 q .

(4) **生物学意义.** 特征值 $\lambda_1 = 1$ 对应的二维特征子空间 V_1 反映了等位基因频率 p 和 q 在自交过程中始终不变——这是守恒量; 特征值 $\lambda_2 = \frac{1}{2}$ 对应的特征向量 $(1, -2, 1)^T$ 描述了杂合子偏离 *Hardy-Weinberg* 平衡的方向, 其系数以 $(\frac{1}{2})^k$ 的速率指数衰减. 这个例子展示了对角化在理解动态系统长期行为中的威力: 不同特征值对应的成分分别刻画了系统的守恒量和衰减模式.

8.4 选读: PageRank、Markov 链与阻尼因子

选学背景

本小节把特征向量用于网页排序和随机过程. 阅读前最好先知道概率向量(所有分量非负且和为 1)、行随机矩阵(每行和为 1)与列随机矩阵(每列和为 1)的区别. 若当前目标是掌握特征值和对角化, 可以先读例子的直观叙述, 暂时跳过阻尼因子的严格讨论.

第 1 节中, 我们曾用 PageRank 引出线性方程组. 当时我们只把它看作方程

$$Px = x$$

的求解问题. 现在有了特征值、特征向量和矩阵幂的语言后, 可以重新理解这个例子: PageRank 本质上是在寻找一个 Markov 链的平稳分布.

设共有 n 个网页. 如果第 j 个网页有链接指向若干网页, 并且用户在网页 j 上等概率点击其中一个链接, 则记

p_{ij} = 从网页 j 跳转到网页 i 的概率.

令

$$P = (p_{ij}) \in M_n(\mathbb{R}).$$

由于用户从每个网页 j 出发时, 总要跳到某个网页, 每一列的概率和为 1:

$$\sum_{i=1}^n p_{ij} = 1, \quad j = 1, \dots, n.$$

这样的矩阵称为**列随机矩阵**(column-stochastic matrix). 如果 $x_k \in \mathbb{R}^n$ 表示第 k 步时用户位于各网页的概率分布, 则

$$x_{k+1} = Px_k.$$

因此

$$x_k = P^k x_0.$$

这正是个离散时间 **Markov 链**.

定义 8.7 (平稳分布). 设 P 是列随机矩阵. 若向量 $\pi \in \mathbb{R}^n$ 满足

$$\pi_i \geq 0, \quad \sum_{i=1}^n \pi_i = 1,$$

并且

$$P\pi = \pi,$$

则称 π 为该 Markov 链的**平稳分布** (stationary distribution).

从特征值角度看, 平稳分布正是特征值 1 对应的非负特征向量, 再归一化为坐标和等于 1. PageRank 向量就是网页随机游走模型的平稳分布; π_i 越大, 表示长期随机浏览过程中停留在网页 i 上的比例越高, 因而该网页越重要.

列随机矩阵一定满足

$$\mathbf{1}^T P = \mathbf{1}^T,$$

其中 $\mathbf{1} = (1, \dots, 1)^T$. 这说明若 x 是概率分布, 则

$$\mathbf{1}^T (Px) = \mathbf{1}^T x = 1,$$

所以矩阵乘法保持总概率. 同时, P 有特征值 1: 将 $\mathbf{1}^T P = \mathbf{1}^T$ 转置, 得到 $P^T \mathbf{1} = \mathbf{1}$. 因此 1 是 P^T 的特征值; 又因为 P 和 P^T 有相同的特征多项式, 所以 1 也是 P 的特征值.

接下来讨论收敛性. 理想情况下, 我们希望对任意初始分布 x_0 都有

$$P^k x_0 \rightarrow \pi.$$

如果 P 可以对角化, 且特征值可排列为

$$\lambda_1 = 1, \quad |\lambda_2|, \dots, |\lambda_n| < 1,$$

那么这件事可以直接由矩阵幂看出. 设

$$P = S \operatorname{diag}(1, \lambda_2, \dots, \lambda_n) S^{-1}.$$

则

$$P^k = S \operatorname{diag}(1, \lambda_2^k, \dots, \lambda_n^k) S^{-1}.$$

当 $k \rightarrow \infty$ 时, $\lambda_2^k, \dots, \lambda_n^k$ 都趋于 0, 只剩下特征值 1 对应的方向. 这就是 Markov 链长期稳定的线性代数本质.

然而, 真实网页图可能并不满足这些理想条件. 例如, 某些网页没有任何出链, 或网页图被分成互不连通的部分, 或随机游走在几个网页之间周期性跳动. 这些情况会导致平稳分布不唯一或迭代不收敛. PageRank 的一个关键修正是加入**阻尼因子**(damping factor).

设 S 是根据网页链接得到的列随机矩阵. 取 $0 < \alpha < 1$, 定义

$$G = \alpha S + (1 - \alpha) \frac{1}{n} \mathbf{1} \mathbf{1}^T.$$

矩阵 G 称为带阻尼的 Google 矩阵. 它对应如下随机浏览模型:

- 以概率 α 按照当前网页的链接继续点击;
- 以概率 $1 - \alpha$ 随机跳转到任意一个网页.

第二种随机跳转也称为 **teleportation**. 由于 $\frac{1}{n}\mathbf{1}\mathbf{1}^T$ 的每个元素都为 $1/n$, 矩阵 G 的每个元素都严格为正. 因而从任意网页都有正概率到达任意网页, 这消除了不连通和周期性造成的困难.

矩阵 G 仍然是列随机矩阵. 事实上,

$$\mathbf{1}^T G = \alpha \mathbf{1}^T S + (1 - \alpha) \frac{1}{n} \mathbf{1}^T \mathbf{1} \mathbf{1}^T = \alpha \mathbf{1}^T + (1 - \alpha) \mathbf{1}^T = \mathbf{1}^T.$$

因此 G 同样保持概率分布.

阻尼因子还给出一种直观的收敛解释. 对两个概率分布 x, y , 有 $\mathbf{1}^T x = \mathbf{1}^T y = 1$, 所以

$$\frac{1}{n} \mathbf{1} \mathbf{1}^T (x - y) = 0.$$

于是

$$Gx - Gy = \alpha S(x - y).$$

由于列随机矩阵在 ℓ^1 范数下不会放大概率差异, 得到

$$\|Gx - Gy\|_1 \leq \alpha \|x - y\|_1.$$

这说明 G 把任意两个概率分布之间的距离至少按因子 α 收缩. 因而从任意初始分布出发做迭代

$$x_{k+1} = Gx_k$$

都会收敛到唯一的平稳分布 π , 即

$$G\pi = \pi, \quad \sum_{i=1}^n \pi_i = 1.$$

这就是 PageRank 算法中阻尼因子的线性代数意义: 它把一个可能不稳定、不唯一的特征向量问题, 改造成一个具有唯一极限的矩阵迭代问题.

注 8.3. 在实际计算中, *PageRank* 通常不直接求解 $(G - I)x = 0$, 而是从某个初始概率分布 x_0 出发, 重复计算 $x_{k+1} = Gx_k$. 这称为 **幂迭代** (*power iteration*). 当 $G^k x_0$ 收敛时, 极限向量就是特征值 1 对应的 *PageRank* 向量.

习题 8.1. 设 P 是列随机矩阵. 证明若 x 是概率分布, 则 Px 仍是概率分布.

习题 8.2. 设 S 是列随机矩阵, $G = \alpha S + (1 - \alpha) \frac{1}{n} \mathbf{1} \mathbf{1}^T$. 证明 G 是列随机矩阵, 且 G 的所有元素均大于等于 $(1 - \alpha)/n$.

习题 8.3. 设 S 是列随机矩阵. 证明对任意 $u \in \mathbb{R}^n$,

$$\|Su\|_1 \leq \|u\|_1.$$

提示: 使用三角不等式以及 S 的元素非负、列和为 1.

习题 8.4. 在上一题基础上, 证明对任意两个概率分布 x, y ,

$$\|Gx - Gy\|_1 \leq \alpha \|x - y\|_1.$$

这说明阻尼因子越小, 收敛越快; 但 α 太小也会削弱真实链接结构对排名的影响.

8.5 代数重数与几何重数

定义 8.8. 对于矩阵 $A \in M_{n \times n}(\mathbb{F})$, 特征值 λ_0 作为特征多项式 $\chi_A(\lambda)$ 的根 (定义 7.6) 的重数称为 λ_0 的**代数重数** (algebraic multiplicity), 即 $(\lambda - \lambda_0)^{n_0} \mid \chi_A(\lambda)$ 且 $(\lambda - \lambda_0)^{n_0+1} \nmid \chi_A(\lambda)$ 时, n_0 为代数重数.

定义 8.9. 对于矩阵 $A \in M_{n \times n}(\mathbb{F})$, 特征值 λ 的特征子空间 V_λ 的维数称为 λ 的**几何重数** (geometric multiplicity).

例 8.4. 假设矩阵 $A \in M_{n \times n}(\mathbb{F})$ 只有一个特征值 λ_1 , 即其特征多项式为 $(\lambda - \lambda_1)^n$. 根据定理 8.4 可知 $(A - \lambda_1 I_n)^n = 0$, 因此 $\mathbb{F}^n = \ker(A - \lambda_1 I_n)^n$. 特别地, A 的特征值 λ_1 的代数重数为

$$n = \dim\{v \in \mathbb{F}^n \mid (\lambda_1 I_n - A)^n v = 0\}$$

命题 8.4. 对于矩阵 $A \in M_{n \times n}(\mathbb{F})$, 特征值 λ 的代数重数为 $\dim V'_\lambda$, 其中

$$V'_\lambda = \{v \in \mathbb{F}^n \mid \text{存在 } k \in \mathbb{N}_{\geq 0} \text{ 使得 } (\lambda I_n - A)^k v = 0\}$$

称为 λ 对应的**广义特征子空间** (generalized eigenspace).

注 8.4. 上述命题的完整证明需要用到 Cayley-Hamilton 定理 (定理 8.4) 以及特征多项式的互素因子分解, 参见 §8.6. 这里的关键思路是: 设特征多项式为 $\chi_A(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{n_i}$, 则由 Cayley-Hamilton 定理 $\chi_A(A) = 0$, 再利用互素多项式的核分解 (本质是多元裴蜀恒等式, 推论 7.1) 可得 $\mathbb{F}^n = \bigoplus_{i=1}^s V'_{\lambda_i}$, 从而 $\dim V'_{\lambda_i} = n_i$. 广义特征子空间分解的完整叙述和证明见定理 13.1; 在该定理中, 我们也使用记号 $V[\lambda_i] := \ker(T - \lambda_i I)^{n_i}$ 表示广义特征子空间.

推论 8.2. 对于矩阵 $A \in M_{n \times n}(\mathbb{F})$ 的特征值 λ , 其几何重数小于等于代数重数.

证明. 注意到对于特征值 λ 我们有 $V_\lambda \subseteq V'_\lambda$. □

定理 8.3. 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 可对角化当且仅当对于每一个特征值 λ 其几何重数等于代数重数.

证明. 假设 A 的特征多项式为 $f(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_s)^{n_s}$. 由 Cayley-Hamilton 定理 (定理 8.4), $f(A) = 0$. 注意到 $(\lambda - \lambda_1)^{n_1}, \dots, (\lambda - \lambda_s)^{n_s}$ 两两互素, 根据多元裴蜀恒等式 (推论 7.1) 的核分解, 我们得到广义特征子空间的直和分解

$$\mathbb{F}^n = V'_{\lambda_1} \oplus \cdots \oplus V'_{\lambda_s},$$

且 $\dim V'_{\lambda_i} = n_i$ (即代数重数). 注意到代数重数等于几何重数当且仅当对任意 $1 \leq i \leq s$ 有 $V'_{\lambda_i} = V_{\lambda_i}$, 此时 $\mathbb{F}^n = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}$, 根据定理8.2可知 A 可对角化. 反之, 若 A 可对角化, 则 $\mathbb{F}^n = \bigoplus V_{\lambda_i}$, 每个 $V_{\lambda_i} \subseteq V'_{\lambda_i}$ 且 $\sum \dim V_{\lambda_i} = n = \sum n_i$, 因此 $\dim V_{\lambda_i} = n_i$. \square

8.6 Cayley-Hamilton 定理

定义 8.10. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 多项式 $f(\lambda) \in \mathbb{F}[\lambda]$ 称为其**零化多项式** (*annihilation polynomial*), 如果 $f(T) = 0$.

注 8.5. 类似的, 我们可以对矩阵定义其零化多项式, 即将矩阵视作线性映射. 本节之后所有的概念以及结果都可以用矩阵的语言叙述, 在此不再赘述.

引理 8.2. 对于任何 \mathbb{F} -线性变换 $T: V \rightarrow V$, 零化多项式总是存在.

证明. 任意取 V 的一组基, 考虑 T 在这组基下对应的矩阵 A . 假设 V 的维数为 n , 那么全体矩阵组成的线性空间的维数是 n^2 , 从而 $I_n, A, A^2, \dots, A^{n^2}$ 一定线性相关, 即存在不全为零的 a_0, a_1, \dots, a_{n^2} 使得

$$a_0 I_n + a_1 A + \cdots + a_{n^2} A^{n^2} = 0,$$

从而 $f(x) = a_0 + a_1 x + \cdots + a_{n^2} x^{n^2}$ 是零化多项式. \square

给定 \mathbb{F} -线性变换 $T: V \rightarrow V$, Cayley-Hamilton 定理改进上述结果, 证明总是存在一个 n 次的多项式是 T 的零化多项式, 其中 n 是 V 的维数.

定理 8.4 (Cayley-Hamilton). 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其特征多项式是其零化多项式.

为了证明这个结果, 我们先定义多项式环 $\mathbb{F}[\lambda]$ 在线性空间 V 上的数乘: 对于 $h(\lambda) \in \mathbb{F}[\lambda]$ 和 $v \in V$, 定义

$$h(\lambda) \cdot v := h(T)v.$$

不难验证上述数乘有如下的性质:

- (1) 对任意的 $f_1, f_2 \in \mathbb{F}[\lambda], v \in V, (f_1 f_2) \cdot v = f_1 \cdot (f_2 \cdot v)$;
- (2) 对任意的 $f_1, f_2 \in \mathbb{F}[\lambda], v \in V, (f_1 + f_2) \cdot v = f_1 \cdot v + f_2 \cdot v$;
- (3) 对任意的 $f \in \mathbb{F}[\lambda], c \in \mathbb{F}, v \in V, (cf) \cdot v = c(f \cdot v)$;
- (4) 对任意的 $f \in \mathbb{F}[\lambda], v, w \in V, f \cdot (v + w) = f \cdot v + f \cdot w$;
- (5) 对任意的 $f \in \mathbb{F}[\lambda], c \in \mathbb{F}, v \in V, f \cdot (cv) = c(f \cdot v)$.

特别地, λ 作为 $\mathbb{F}[\lambda]$ 的元素数乘 V 中的向量时, $\lambda \cdot v = Tv$.

Cayley-Hamilton 定理的证明. 任取 V 的一组基 $B = (v_1, \dots, v_n)$, 设 T 在 B 下的表示矩阵为 $A = (a_{ij})$, 则

$$\lambda \cdot (v_1, \dots, v_n) = T(v_1, \dots, v_n) = (v_1, \dots, v_n)A.$$

将上述等式转置, 得到

$$\lambda \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = A^T \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

即

$$(\lambda I_n - A^T) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \quad (10)$$

注意上述等式中, $\lambda I_n - A^T$ 应理解为元素在 $\mathbb{F}[\lambda]$ 中的矩阵, 而 v_1, \dots, v_n 是 V 中的向量; 等式的意义由 $\mathbb{F}[\lambda]$ 在 V 上的数乘给出. 对于 $\mathbb{F}[\lambda]$ 系数的方阵, 我们仍可以定义其行列式和伴随矩阵 (因为这些运算只涉及 $\mathbb{F}[\lambda]$ 中的加法与乘法), 且如下恒等式依然成立:

$$(\lambda I_n - A^T)^* \cdot (\lambda I_n - A^T) = |\lambda I_n - A^T| \cdot I_n.$$

在(10)两侧左乘伴随矩阵 $(\lambda I_n - A^T)^*$, 得到

$$|\lambda I_n - A^T| \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

从而对任意的 $1 \leq i \leq n$, 有 $|\lambda I_n - A^T| \cdot v_i = 0$. 由于 $|\lambda I_n - A^T| = \chi_T(\lambda)$, 而 $\mathbb{F}[\lambda]$ 的数乘由 T 定义, 这意味着 $\chi_T(T)v_i = 0$ 对所有基向量 v_i 成立, 故 $\chi_T(T) = 0$. \square

8.7 极小多项式

选学提示

极小多项式是判断可对角化的高效工具, 但抽象程度高于直接计算特征子空间. 初学时可以先掌握二阶、三阶矩阵的特征值和特征向量, 再回到本小节理解可对角化判据的统一表述.

定义 8.11. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其次数最低的首一零化多项式被称为**极小多项式** (*minimal polynomial*).

例 8.5 (二阶矩阵的极小多项式). 极小多项式记录的是“用多低次数的多项式就能把矩阵消成零”. 先看三个 2×2 矩阵:

$$A_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

对 A_1 来说,

$$(A_1 - 2I)(A_1 - 3I) = 0,$$

且 $A_1 - 2I \neq 0$, $A_1 - 3I \neq 0$, 所以

$$m_{A_1}(\lambda) = (\lambda - 2)(\lambda - 3).$$

对 A_2 来说, 令 $N = A_2 - 2I = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, 则 $N^2 = 0$ 但 $N \neq 0$. 因而

$$m_{A_2}(\lambda) = (\lambda - 2)^2.$$

对 $A_3 = 2I$ 来说, 一次多项式已经足够:

$$m_{A_3}(\lambda) = \lambda - 2.$$

注意 A_2 与 A_3 的特征多项式都是 $(\lambda - 2)^2$, 但极小多项式不同. 这正说明极小多项式能看出“同一个特征值背后有没有不可对角化的方向”.

命题 8.5. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其极小多项式整除其任何一个零化多项式.

证明. 假设 $m(\lambda)$ 是 T 的极小多项式, $f(\lambda)$ 是 T 的某个零化多项式, 作带余除法则有

$$f(\lambda) = m(\lambda)q(\lambda) + r(\lambda)$$

其中 $r(\lambda)$ 显然也是 T 的零化多项式. 如果 $r(\lambda)$ 不为零, 根据带余除法 (定理7.1) 的结果我们有 $\deg r(\lambda) < \deg m(\lambda)$, 这与极小多项式的定义矛盾. \square

推论 8.3. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其极小多项式是唯一的.

证明. 假设 $m_1(\lambda), m_2(\lambda)$ 都是 T 的极小多项式, 从而有 $m_1(\lambda) \mid m_2(\lambda)$ 以及 $m_2(\lambda) \mid m_1(\lambda)$, 因此 $m_1(\lambda), m_2(\lambda)$ 之间相差一个非零常数 c , 再利用首一性可知 $m_1(\lambda) = m_2(\lambda)$. \square

推论 8.4. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其极小多项式整除其特征多项式.

证明. 根据定理8.4可知特征多项式是零化多项式. \square

命题 8.6. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 如果 $f(\lambda)$ 是其零化多项式, 则其特征值 λ 也是该多项式的根. 特别地, 是其极小多项式的根.

证明. 设 λ 是 T 的特征值, $v \neq 0$ 是对应的特征向量, 则 $Tv = \lambda v$. 对任意多项式 $f(\lambda) = \sum_i a_i \lambda^i$, 有

$$f(T)v = \sum_i a_i T^i v = \sum_i a_i \lambda^i v = f(\lambda)v.$$

若 f 是零化多项式, 则 $f(T) = 0$, 从而 $f(\lambda)v = 0$. 由 $v \neq 0$ 知 $f(\lambda) = 0$. □

注 8.6. 根据推论 8.4 以及命题 8.6 可知, 如果 \mathbb{F} -线性映射 $T: V \rightarrow V$ 的特征多项式分解为一次因式的乘积

$$f(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_s)^{n_s},$$

那么其极小多项式为

$$m(\lambda) = (\lambda - \lambda_1)^{k_1} \cdots (\lambda - \lambda_s)^{k_s},$$

其中 $k_i \leq n_i, 1 \leq i \leq s$.

定理 8.5. 对于 \mathbb{F} -线性映射 $T: V \rightarrow V$, 其在 \mathbb{F} 上可对角化当且仅当极小多项式 $m(\lambda)$ 在 $\mathbb{F}[\lambda]$ 中可分解为一次因式的乘积, 且没有重根.

证明. 如果 T 可对角化, 即其在某一组基下的矩阵 A 是对角阵, 其不同的特征值分别记为 $\lambda_1, \dots, \lambda_s$, 此时 A 的极小多项式 $m(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_s)$; 另一方面, 假设 T 的极小多项式为 $m(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_s)$, 其中 $\lambda_1, \dots, \lambda_s$ 互不相同, 考虑

$$h_i(\lambda) = \frac{m(\lambda)}{(\lambda - \lambda_i)},$$

则 $\gcd(h_1, \dots, h_s) = 1$, 从而根据多元裴蜀恒等式 (推论 7.1) 存在 $k_1(\lambda), \dots, k_s(\lambda) \in \mathbb{F}[\lambda]$ 使得

$$k_1(\lambda)h_1(\lambda) + \cdots + k_s(\lambda)h_s(\lambda) = 1.$$

即

$$k_1(T)h_1(T) + \cdots + k_s(T)h_s(T) = I_n,$$

其中 $n = \dim V$. 任取 $v \in V$, 我们可以将其分解为 $v = v_1 + \cdots + v_s$, 其中

$$v_i = k_i(T)h_i(T)v.$$

如果我们记 $V_i = \ker(\lambda_i I - T)$, 那么

(1) $v_i \in V_i$, 这是因为 $(A - \lambda_i I)v_i = k_i(T)m(T)v = 0$.

(2) 任取 $1 \leq i \leq s$ 以及 $v \in V_i \cap \sum_{j \neq i} V_j$, 则有

$$0 = (k_1(T)h_1(T) + \cdots + k_s(T)h_s(T))v = v.$$

从而根据命题3.15有

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s}.$$

根据定理8.1可知 T 可对角化. \square

推论 8.5. n 维 \mathbb{F} -线性空间 V 上的 \mathbb{F} -线性映射如果有 n 个不同的特征值, 则其可对角化.

证明. 假设特征多项式 $f(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n)$, 其中 $\lambda_1, \dots, \lambda_n$ 互不相同. 根据命题8.6, 极小多项式 $m(\lambda)$ 的每个根都是特征值, 因此 $m(\lambda)$ 以 $\lambda_1, \dots, \lambda_n$ 为根. 又因为 $m(\lambda) \mid f(\lambda)$ (推论8.4) 且 $\deg m \leq n$, 而 $m(\lambda)$ 至少有 n 个不同的根 (因而 $\deg m \geq n$), 从而 $m(\lambda) = f(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n)$ 是没有重根的一次因式乘积, 由定理8.5知 T 可对角化. \square

推论 8.6. \mathbb{F} -线性映射 $T: V \rightarrow V$ 可对角化, 假设 W 是 T -不变子空间, 则 $T|_W: W \rightarrow W$ 也可对角化.

证明. 假设 $m_V(\lambda)$ 是 $T: V \rightarrow V$ 的极小多项式, 那么其也是 $T|_W: W \rightarrow W$ 的零化多项式, 从而 $m_W(\lambda)$ 整除 $m_V(\lambda)$. 从而如果 $m_V(\lambda)$ 可以分解为没有重根的一次因式乘积, $m_W(\lambda)$ 也可以分解为没有重根的一次因式乘积, 从而 $T|_W$ 可对角化. \square

定义 8.12. 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 称为**幂等矩阵** (*idempotent matrix*), 如果 $A^2 = A$.

命题 8.7. 幂等矩阵 A 在任何域 \mathbb{F} 上都可对角化.

证明. 注意到 $\lambda^2 - \lambda = \lambda(\lambda - 1)$ 是 A 的零化多项式, 从而其极小多项式整除 $\lambda(\lambda - 1)$. 由于 $0 \neq 1$ 在任何域中成立, $\lambda(\lambda - 1)$ 是没有重根的一次因式乘积, 根据定理8.5可知 A 可对角化. \square

定义 8.13. 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 称为**对合矩阵** (*involution*), 如果 $A^2 = I_n$.

命题 8.8. 假设 \mathbb{F} 的特征不为 2, 则对合矩阵 A 在 \mathbb{F} 上可对角化.

证明. 注意到 $\lambda^2 - 1$ 是 A 的零化多项式, 从而其极小多项式整除 $\lambda^2 - 1$. 如果 \mathbb{F} 的特征不为 2, $\lambda^2 - 1$ 在 \mathbb{F} 可以分解为 $(\lambda - 1)(\lambda + 1)$, 其中 $1 \neq -1$, 从而根据定理8.5可知 A 可对角化. \square

定义 8.14. 矩阵 $A \in M_{n \times n}(\mathbb{F})$ 被称为**幂零矩阵** (*nilpotent matrix*), 如果存在 $k \in \mathbb{N}_{\geq 0}$ 使得 $A^k = 0$.

命题 8.9. 幂零矩阵的特征值都为零.

证明. 如果 A 是幂零矩阵, 则某个单项式 λ^k 是 A 的零化多项式, 特别地, 根据命题8.6有幂零矩阵的特征值都为零. \square

推论 8.7. 幂零矩阵可对角化当且仅当其为零矩阵.

证明. 一方面, 如果其可对角化, 由于其特征值都为零从而有其为零矩阵; 另一方面, 零矩阵当然是可对角化的幂零矩阵. \square

注 8.7. 上述推论也可以通过极小多项式的观点看出: 如果 A 是非零的幂零矩阵, 那么其极小多项式为 $\lambda^k (k \geq 2)$, 从而不是没有重根的一次因式的乘积.

8.8 友阵

选学提示

友阵把“多项式”直接做成“矩阵”, 是通向若尔当标准型和有理标准型的桥梁. 本小节属于挑战性内容; 若主线目标是计算特征值和判断对角化, 可先略读定义和例子.

在上一小节中, 我们看到极小多项式精确地刻画了线性变换的可对角化性. 自然的问题是: 极小多项式和特征多项式之间还有什么更深的联系? 本小节引入**友阵**的概念, 它建立了多项式与矩阵之间的直接桥梁, 并在后续的若尔当标准型理论中扮演重要角色.

定义 8.15 (友阵). 给定首一多项式 $f(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0 \in \mathbb{F}[\lambda]$, 其**友阵** (*companion matrix*) 定义为

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in M_{n \times n}(\mathbb{F}).$$

友阵的结构非常简洁: 次对角线全为 1, 最后一列由多项式的系数 (取负号) 决定, 其余位置为 0. 下面的命题说明友阵完美地“实现”了给定的多项式.

例 8.6 (二阶友阵的手算). 取

$$f(\lambda) = \lambda^2 - 3\lambda + 2.$$

这里 $a_1 = -3$, $a_0 = 2$, 因而

$$C(f) = \begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}.$$

直接计算

$$\lambda I - C(f) = \begin{pmatrix} \lambda & 2 \\ -1 & \lambda - 3 \end{pmatrix}, \quad \det(\lambda I - C(f)) = \lambda(\lambda - 3) + 2 = \lambda^2 - 3\lambda + 2 = f(\lambda).$$

同时

$$C(f)^2 - 3C(f) + 2I = 0.$$

而 $C(f) - 2I \neq 0$, $C(f) - I \neq 0$, 所以没有一次多项式能消去 $C(f)$. 因此这个例子中

$$\chi_{C(f)}(\lambda) = m_{C(f)}(\lambda) = f(\lambda).$$

从基向量角度看, $C(f)e_1 = e_2$, 而

$$C(f)e_2 = -2e_1 + 3e_2.$$

也就是说, 前一步不断把 e_1 推到下一个基向量, 最后一步才由多项式 f 的系数给出回收关系.

命题 8.10. 友阵 $C(f)$ 的特征多项式等于 $f(\lambda)$.

证明. 我们对 n 做归纳法. 当 $n = 1$ 时, $C(f) = (-a_0)$, 特征多项式为 $\lambda + a_0 = f(\lambda)$, 结论成立.

设结论对 $n - 1$ 阶友阵成立. 对 n 阶友阵 $C(f)$, 按第一行展开行列式:

$$\det(\lambda I_n - C(f)) = \det \begin{pmatrix} \lambda & 0 & \cdots & 0 & a_0 \\ -1 & \lambda & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \lambda + a_{n-1} \end{pmatrix}.$$

按第一列展开, 得到

$$\det(\lambda I_n - C(f)) = \lambda \cdot \det(\lambda I_{n-1} - C(g)) + (-1)^{n+1} \cdot (-1) \cdot (-1)^{n-1} a_0,$$

其中 $g(\lambda) = \lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_1$ 是去掉常数项并降一次后的多项式, 对应 $C(f)$ 删去第一行第一列后的 $(n - 1)$ 阶矩阵. 由归纳假设 $\det(\lambda I_{n-1} - C(g)) = g(\lambda)$, 从而

$$\det(\lambda I_n - C(f)) = \lambda \cdot g(\lambda) + a_0 = \lambda(\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \cdots + a_1) + a_0 = f(\lambda).$$

□

命题 8.11. 友阵 $C(f)$ 的极小多项式也等于 $f(\lambda)$.

证明. 设 $A = C(f)$, 记标准基 e_1, \dots, e_n 为 \mathbb{F}^n 的列向量. 注意到 A 的结构给出

$$Ae_1 = e_2, \quad Ae_2 = e_3, \quad \dots, \quad Ae_{n-1} = e_n,$$

即 $A^{k-1}e_1 = e_k$ 对所有 $1 \leq k \leq n$ 成立. 假设 $m(\lambda) = \lambda^d + b_{d-1}\lambda^{d-1} + \cdots + b_0$ 是 A 的极小多项式, 则 $m(A) = 0$. 特别地,

$$m(A)e_1 = A^d e_1 + b_{d-1}A^{d-1}e_1 + \cdots + b_0 e_1 = e_{d+1} + b_{d-1}e_d + \cdots + b_0 e_1 = 0.$$

由于 e_1, \dots, e_n 线性无关, 上式要求 $d+1 \leq n$ (否则 e_{d+1} 不存在) 时各系数为零. 但若 $d < n$, 则 e_{d+1} 的系数为 $1 \neq 0$, 矛盾. 因此 $d \geq n$. 又因为极小多项式整除特征多项式 $f(\lambda)$ (推论 8.4), 且 $\deg f = n$, 故 $d \leq n$, 从而 $d = n$, 即 $m(\lambda) = f(\lambda)$. \square

注 8.8. 从线性变换的角度看, 友阵的本质含义如下: 考虑 \mathbb{F}^n 上的线性变换 $T: x \mapsto C(f)x$, 则向量 e_1 在 T 的反复作用下生成了整个空间:

$$e_1, Te_1 = e_2, T^2e_1 = e_3, \dots, T^{n-1}e_1 = e_n.$$

这样的向量 e_1 称为 T 的一个 **循环向量** (cyclic vector). 友阵恰好是线性变换在循环向量所生成的有序基下的表示矩阵.

下面的定理是本小节的核心结果, 它精确刻画了矩阵何时相似于友阵:

定理 8.6. 矩阵 $A \in M_n(\mathbb{F})$ 相似于某个 $n \times n$ 友阵当且仅当 A 的极小多项式等于其特征多项式.

证明. (\Rightarrow) 若 A 相似于友阵 $C(f)$, 则 A 和 $C(f)$ 有相同的特征多项式和极小多项式. 由命题 8.10 和命题 8.11, $C(f)$ 的特征多项式和极小多项式都等于 $f(\lambda)$. 因此 $m_A(\lambda) = \chi_A(\lambda)$.

(\Leftarrow) 假设 $m_A(\lambda) = \chi_A(\lambda)$. 因为 χ_A 是 n 次首一多项式, 所以 $\deg m_A = n$. 我们先证明存在 $v \in \mathbb{F}^n$, 使得 v 关于 A 的极小零化多项式等于 m_A .

对非零向量 $x \in \mathbb{F}^n$, 记 $\mu_x(\lambda)$ 为满足 $\mu_x(A)x = 0$ 的首一最低次多项式. 若 $q(A)x = 0$, 对 q 除以 μ_x 作带余除法, 可知 $\mu_x \mid q$.

取 \mathbb{F}^n 的一组基 b_1, \dots, b_n . 一个多项式 q 满足 $q(A) = 0$ 当且仅当 $q(A)b_i = 0$ 对所有 i 成立, 因而

$$m_A = \text{lcm}(\mu_{b_1}, \dots, \mu_{b_n}).$$

将 m_A 在 $\mathbb{F}[\lambda]$ 中分解为两两不同的首一不可约多项式的乘积

$$m_A(\lambda) = \pi_1(\lambda)^{e_1} \cdots \pi_r(\lambda)^{e_r}.$$

由于 m_A 是上述 μ_{b_i} 的最小公倍式, 对每个 j , 存在某个基向量 $u_j = b_i$ 使得 μ_{u_j} 含有因子 $\pi_j^{e_j}$. 写

$$\mu_{u_j}(\lambda) = \pi_j(\lambda)^{e_j} s_j(\lambda), \quad \text{gcd}(\pi_j, s_j) = 1.$$

令 $w_j = s_j(A)u_j$. 由于 $\pi_j(A)^{e_j}w_j = 0$, 且若 $h(A)w_j = 0$ 则 $\mu_{u_j} \mid hs_j$, 从而 $\pi_j^{e_j} \mid h$, 可得

$$\mu_{w_j} = \pi_j^{e_j}.$$

下面说明互素因子可以相加拼合. 若非零向量 u, w 满足 $\gcd(\mu_u, \mu_w) = 1$, 则 $\mu_{u+w} = \mu_u \mu_w$. 一方面, $\mu_u(A)\mu_w(A)(u+w) = 0$, 所以 $\mu_{u+w} \mid \mu_u \mu_w$. 另一方面, 若 $h(A)(u+w) = 0$, 则

$$h(A)u = -h(A)w.$$

左边属于由 u 生成的 A -循环子空间, 右边属于由 w 生成的 A -循环子空间. 若某向量同时属于这两个循环子空间, 它同时被 $\mu_u(A)$ 和 $\mu_w(A)$ 消去. 由 $\gcd(\mu_u, \mu_w) = 1$ 和裴蜀恒等式, 这个公共向量只能为 0. 因此 $h(A)u = 0$ 且 $h(A)w = 0$, 于是 $\mu_u \mid h$ 且 $\mu_w \mid h$. 由于 μ_u, μ_w 互素, 有 $\mu_u \mu_w \mid h$. 这证明 $\mu_{u+w} = \mu_u \mu_w$.

反复应用上面的结论, 对

$$v = w_1 + \cdots + w_r$$

有

$$\mu_v = \mu_{w_1} \cdots \mu_{w_r} = \pi_1^{e_1} \cdots \pi_r^{e_r} = m_A.$$

于是 $\deg \mu_v = \deg m_A = n$. 如果 $v, Av, \dots, A^{n-1}v$ 线性相关, 则存在次数小于 n 的非零多项式 q 使得 $q(A)v = 0$, 这与 μ_v 的次数为 n 矛盾. 因此

$$B = (v, Av, \dots, A^{n-1}v)$$

是 \mathbb{F}^n 的一组基.

设

$$m_A(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0.$$

在基 B 下, 前 $n-1$ 个基向量满足

$$v \mapsto Av, \quad Av \mapsto A^2v, \quad \dots, \quad A^{n-2}v \mapsto A^{n-1}v.$$

而 $m_A(A)v = 0$ 给出

$$A^n v = -a_0 v - a_1 Av - \cdots - a_{n-1} A^{n-1} v.$$

因此 A 在基 B 下的矩阵为

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix},$$

也就是 $m_A(\lambda)$ 的友阵. 故 A 相似于友阵. □

注 8.9. 上述定理的“ \Leftarrow ”方向的关键是循环向量的存在性. 证明中并不是比较不同向量的零化多项式次数, 而是先用一组基向量的零化多项式取最小公倍式得到 m_A , 再利用不可约因子的互素分解和裴蜀恒等式, 拼出一个零化多项式恰好为 m_A 的向量.

例 8.7. 考虑多项式 $f(\lambda) = \lambda^3 - 6\lambda^2 + 11\lambda - 6 = (\lambda - 1)(\lambda - 2)(\lambda - 3)$, 其友阵为

$$C(f) = \begin{pmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{pmatrix}.$$

$C(f)$ 的特征多项式为 $f(\lambda)$, 极小多项式也是 $f(\lambda)$. 由于 f 有三个不同的根, $C(f)$ 可对角化, 并且相似于 $\text{diag}(1, 2, 3)$.

例 8.8. 考虑矩阵 $A = \text{diag}(1, 1, 2) \in M_{3 \times 3}(\mathbb{R})$. 其特征多项式为 $\chi_A(\lambda) = (\lambda - 1)^2(\lambda - 2)$, 但极小多项式为 $m_A(\lambda) = (\lambda - 1)(\lambda - 2)$ (因为 $(A - I_3)(A - 2I_3) = 0$). 由于 $m_A \neq \chi_A$, 根据定理 8.6, A 不相似于任何友阵.

8.9 计算示例

例 8.9. 考虑矩阵

$$A = \begin{pmatrix} 4 & -1 & 1 \\ 2 & 1 & 1 \\ -2 & 1 & 1 \end{pmatrix} \in M_{3 \times 3}(\mathbb{R}).$$

(1) **特征多项式.** 计算

$$\chi_A(\lambda) = \det(\lambda I_3 - A) = (\lambda - 1)(\lambda - 2)(\lambda - 3).$$

(2) **特征值与特征子空间.** 特征值为 $\lambda_1 = 1, \lambda_2 = 2, \lambda_3 = 3$. 解齐次方程组可得

$$V_1 = \text{span} \left\{ \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \right\}, \quad V_2 = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \right\}, \quad V_3 = \text{span} \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

每个特征子空间的维数为 1, 等于相应的代数重数.

(3) **可对角化判断.** 由于 A 有 3 个互不相同的特征值 (引理 8.1), 取这三个特征向量组成过渡矩阵

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

则 $P^{-1}AP = \text{diag}(1, 2, 3)$.

例 8.10. 考虑矩阵

$$B = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in M_{2 \times 2}(\mathbb{R}).$$

其特征多项式为 $\chi_B(\lambda) = (\lambda - 2)^2$, 唯一的特征值 $\lambda = 2$ 的代数重数为 2. 而

$$V_2 = \ker(2I_2 - B) = \ker \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} = \text{span} \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\},$$

其几何重数为 $1 < 2 =$ 代数重数. 因此 B 不可对角化.

从极小多项式的角度看, $m_B(\lambda) = (\lambda - 2)^2$ (因为 $B - 2I_2 \neq 0$ 但 $(B - 2I_2)^2 = 0$), 极小多项式有重根, 故不满足定理 8.5 的可对角化判据.

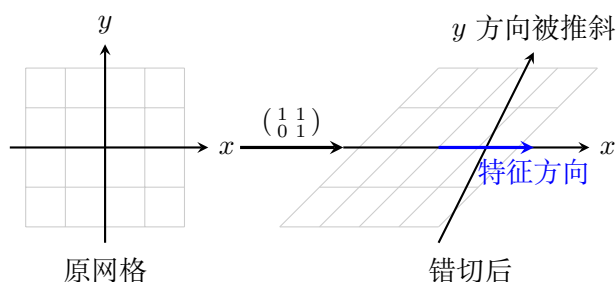


图 14: 错切矩阵保持水平方向不变, 但没有足够多的特征方向, 因此不可对角化.

8.10 习题

8.10.1 练习题

习题 8.5 (二维人口模型). 某种群分为幼年 and 成年两类. 每一年后, 幼年个体中有一半成长为成年个体, 成年个体平均产生 2 个幼年个体, 且成年个体有一半存活到下一年. 令

$$x_k = \begin{pmatrix} \text{第 } k \text{ 年幼年数量} \\ \text{第 } k \text{ 年成年数量} \end{pmatrix}.$$

1. 写出矩阵 A 使得 $x_{k+1} = Ax_k$.
2. 求 A 的特征值.
3. 哪个特征值决定长期增长率? 对应特征向量如何解释长期年龄比例?

习题 8.6 (不可对角化时的矩阵幂). 设

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = I + N, \quad N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

1. 验证 $N^2 = 0$.
2. 利用二项式公式计算 A^n .

3. 说明为什么 A^n 中出现了 n 这一因子, 而对角矩阵的幂只会出现 λ^n .

习题 8.7. 求矩阵

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$$

的特征多项式、全部特征值及其代数重数和几何重数, 并判断 A 是否可对角化.

习题 8.8. 设 $A \in M_{n \times n}(\mathbb{F})$ 可逆, 特征多项式为 $\chi_A(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_0$. 利用 Cayley-Hamilton 定理 (定理 8.4) 证明:

$$A^{-1} = -\frac{1}{c_0} (A^{n-1} + c_{n-1}A^{n-2} + \cdots + c_1 I_n).$$

由此说明 A^{-1} 可以表示为 A 的多项式.

习题 8.9. 设 $A \in M_{n \times n}(\mathbb{F})$ 为幂等矩阵 ($A^2 = A$), 证明 $\text{tr}(A) = \text{rank}(A)$.

习题 8.10. 证明: 相似矩阵有相同的极小多项式. 反过来, 给出一个例子说明极小多项式相同的两个矩阵不一定相似.

习题 8.11. 设 $T: V \rightarrow V$ 是 \mathbb{F} -线性映射, T 可对角化, W 是 T -不变子空间. 利用商空间上的诱导映射 (命题 4.11), 证明 $\bar{T}: V/W \rightarrow V/W$ 也可对角化.

习题 8.12. 设 $A, B \in M_{n \times n}(\mathbb{F})$, 且 $AB = BA$. 如果 A, B 都可对角化, 证明存在可逆矩阵 P 使得 $P^{-1}AP$ 和 $P^{-1}BP$ 同时为对角矩阵.

(提示: 对 A 的某个特征子空间 V_λ , 证明 $B(V_\lambda) \subseteq V_\lambda$, 然后考虑 B 在每个 V_λ 上的限制.)

习题 8.13 (计算练习). 判断下列矩阵 A 是否可在复数域上对角化. 在可对角化的情形, 给出可逆矩阵 P , 使得 $P^{-1}AP$ 是对角矩阵.

1. $A = \begin{bmatrix} -1 & 3 & -1 \\ -3 & 5 & -1 \\ -3 & 3 & 1 \end{bmatrix}$

2. $A = \begin{bmatrix} 4 & 7 & -5 \\ -4 & 5 & 0 \\ 1 & 9 & -4 \end{bmatrix}$

3. $A = \begin{bmatrix} 4 & 2 & -5 \\ 6 & 4 & -9 \\ 5 & 3 & -7 \end{bmatrix}$

$$4. A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

习题 8.14. 求矩阵

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

的特征值与对应特征向量。

习题 8.15. 求矩阵

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

的特征值，并判断它是否有两条不同的特征方向。

习题 8.16. 求矩阵

$$A = \begin{pmatrix} 4 & 1 \\ 2 & 3 \end{pmatrix}$$

的特征多项式、特征值和特征向量。

习题 8.17. 判断矩阵

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

是否可对角化。若可对角化，写出一个对角化。

习题 8.18. 设线性变换 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 关于标准基的矩阵为

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

从几何上解释它的两个特征方向。

习题 8.19. 设数列满足

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}.$$

求矩阵的特征值，并说明为什么这有助于研究数列的长期变化。

习题 8.20. 给出一个 2×2 实矩阵，使它没有实特征值。解释其几何意义。

8.10.2 思考题

习题 8.21. 已知 $A \in M_n(\mathbb{C})$ 的特征值 (按代数重数计) 为 $\lambda_1, \lambda_2, \dots, \lambda_n$ (其中可能有相同的数). 对多项式 $f = a_m X^m + \dots + a_0 \in \mathbb{C}[X]$, 定义 $f(A) = a_m A^m + \dots + a_0 I_n$. 则 $f(A)$ 的特征值集合 (按代数重数计) 是什么?

习题 8.22. 固定复数 $b, c \in \mathbb{C}$. 假设有数列 (a_n) 满足递推公式 $a_{n+1} = ba_n + ca_{n-1}$. 以下你将利用矩阵对角化和上三角化来求通项公式.

1. 令向量 $x_n = (a_n, a_{n-1})^T$. 写下 x_n 的递推公式 $x_n = Ax_{n-1}$. 其中 A 是二阶复方阵.
2. 求矩阵 A 的特征值 λ_1, λ_2 并判断在复数域上是否可以对角化.
3. 如果 A 可以对角化, 利用对角化求 A^n .
4. 如果 A 不能对角化, 证明 A 相似于矩阵 $\lambda_1 I_2 + N$, 其中 $N^2 = 0$. 利用二项展开求 A^n .

习题 8.23. 证明复循环矩阵

$$\begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{bmatrix}$$

(在复数域上) 可对角化, 并求该矩阵的特征值以及行列式. (Hint: 考虑循环方阵

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

和习题 8.21.)

习题 8.24. 设 $A \in M_n(\mathbb{C})$ 满足 $\text{tr}(A^k) = 0$, 对任何 $0 < k \leq n$. 证明 $A^n = 0$. (Hint: 考虑习题 8.21.)

习题 8.25. 设 $A, B \in M_n(\mathbb{C})$ 满足 $AB = BA$, 证明 A 的某个特征值对应的特征子空间也是 B 的不变子空间.

习题 8.26. 设 $\mathcal{T} \subset M_n(\mathbb{C})$ 是一些交换矩阵构成的集合, 即对任何 $T_1, T_2 \in \mathcal{T}$, $T_1 T_2 = T_2 T_1$. 证明, \mathcal{T} 可以同时上三角化, 即存在 $P \in \text{GL}_n(\mathbb{C})$, 使得对任何 $T \in \mathcal{T}$, $P^{-1} T P$ 是上三角矩阵.

习题 8.27. 考虑平面上绕原点的旋转变换对应的矩阵, 求其复特征值, 并判断在复数域上是否可以对角化.

习题 8.28. 对域 F 上的二阶方阵 A , 请通过直接计算验证 *Cayley-Hamilton* 定理: A 的特征多项式为 $f_A(x) = x^2 - \text{tr}(A)x + \det(A)$, 则 A 满足 $f_A(A) = 0$. 请思考该定理中将域上的方阵替换成任意环上是否依然成立.

习题 8.29. 利用 *Cayley-Hamilton* 定理, 证明域 F 上的任意可逆方阵 A 的伴随都可以写成 A 的多项式. 请思考对于环 R 上的一般方阵 A (不要求可逆) 这个结论是否依然成立.

习题 8.30. 假设 T 是 F -线性空间 V 上的线性变换, W 是 T 的不变子空间. 如果 T 可对角化, 请问 T 在 W 的限制是否一定可对角化? 如果是请证明, 如果不是请给出反例.

习题 8.31. 对域 F 上的方阵 A , 如果 μ 是 A 的特征值, 证明 μ 一定是 A 的极小多项式的根.

习题 8.32. 假设复方阵 A 满足 $A^n = I$, 证明 A 可以复对角化.

习题 8.33. 假设两个实方阵在复数域上相似, 证明其在实数域上也相似.

习题 8.34. 假设 n 阶实方阵 A 满足 $A^2 = -I$, 证明 A 的阶数 n 为偶数, 且 A 在实数域上不能对角化, 在复数域上可以对角化. 请对每个偶数 n 给出一个这样的矩阵的例子.

习题 8.35. 找出以下矩阵 A 的极小多项式.

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

习题 8.36. 设 $A, B \in M_n(\mathbb{C})$ 满足 $AB - BA = A$, 证明 A, B 有公共的特征向量.

习题 8.37 (Gershgorin 圆盘定理). 假设 $A = (a_{ij})$ 是复方阵. 定义 $D_i = \{z \in \mathbb{C} \mid |z - a_{ii}| \leq \sum_{j \neq i, 1 \leq j \leq n} |a_{ij}|\}$ 为复平面上的圆盘. 证明 A 的特征值落在这些圆盘的并里 $\cup_i D_i$. (这称为 *Gershgorin circle theorem*, 有更精细的估计在哪些圆盘里有多少特征值的版本. 在估计特征值范围时还可以用对角矩阵 Λ 共轭作用于 A , 即考虑 $\Lambda^{-1}A\Lambda$ 来改变圆盘的位置, 请思考如何选取 Λ 来得到更精细的估计.)

习题 8.38 (PageRank 与列随机矩阵). 在 *Google PageRank* 算法中, 我们写下了一个 n 维向量 $x = (x_1, x_2, \dots, x_n)^T$, 表示一个网页的权重. 我们假设每个网页都有一个初始权重 x_i , 并且第 j 个网页都有一个链到其他网页 i 的概率 p_{ij} . 我们可以用一个 $n \times n$ 的矩阵 $P = (p_{ij})$ 来表示这个概率分布; 按此约定 P 是**列随机矩阵**, 即每一列元素非负且列和为 1. 求解权重向量时, 我们写下方程 $Px = x$. 请证明 P 有特征值 1, 并且所有复特征值的绝对值小于等于 1.

习题 8.39. 假设写出一个用极小多项式判定域 F 上的 n 阶方阵 A 是可上三角化的充分必要条件, 并证明.

习题 8.40. 假设域 F 上的 n 阶方阵 A 是对角化的, 证明 A^T 也是对角化的. 请思考当 A 可以上三角化时, A^T 是否也可以上三角化.

习题 8.41. 假设域 F 上的 n 阶方阵 A 是对角化的, m 阶方阵 B 也是可以对角化的, 证明 F 线性空间 $M_{n \times m}(F)$ 上的线性变换 $T, T(X) = AXB$ 也是对角化的. 请找出 T 的 *determinant* 和 *trace* 与 A 和 B 的关系. 请思考 A 和 B 可以上三角化时, T 是否也可以上三角化.

习题 8.42. 假设域 F 上的有限维线性空间有线性变换 T , 和 T 的不变子空间 W , 则 T 诱导了商空间上 V/W 上的线性变换 \tilde{T} . 证明 T 的特征多项式等于 $T|_W$ 和 \tilde{T} 的特征多项式的乘积.

习题 8.43 (AB 与 BA 的非零特征值). 设 $A, B \in M_n(\mathbb{C})$.

1. 证明 AB 和 BA 具有相同的非零特征值 (含重数).
2. 证明 $\text{rank}(AB - I_n) = \text{rank}(BA - I_n)$, 并推出若 $AB = I_n$, 则 $BA = I_n$.
3. 若 A 是 $m \times n$ 矩阵, B 是 $n \times m$ 矩阵, $m \neq n$, 证明

$$\lambda^n \det(\lambda I_m - AB) = \lambda^m \det(\lambda I_n - BA).$$

习题 8.44. 对域 F 上的 n 阶方阵 A , 特征多项式 $\det(\lambda I - A) = \lambda^n + s_1 \lambda^{n-1} + \cdots + s_n$ 的展开系数 s_k 定义了函数 $S_k: M_n(F) \rightarrow F, A \mapsto s_k$. 证明这些函数满足 $S_k(AB) = S_k(BA)$. 请思考将域 F 换成任意交换环 R , 这个结论是否成立.

习题 8.45. 假设可交换的复方阵 A 和 B , 满足 $B^n = 0$. 证明 A 和 $A+B$ 有相同的特征多项式. 请思考将复数域换成任意域 F , 这个结论是否成立.

习题 8.46. 考虑复数域 \mathbb{C} 上的 n 阶方阵组成的线性空间 $V = M_n(\mathbb{C})$, 以及 V 上的线性变换

$$T: V \rightarrow V, X \mapsto A^T X A.$$

1. 假设 W 是对称矩阵组成的 V 的子空间, U 是反对称矩阵组成的 V 的子空间, 证明 $V = W \oplus U$, 且 W 和 U 都是 T 的不变子空间.
2. 求线性变换 $T|_W: W \rightarrow W$ 和 $T|_U: U \rightarrow U$ 的行列式以及迹, 请用 A 的行列式以及迹表示.

习题 8.47. 如下归纳地定义方阵

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, A_n = \begin{bmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{bmatrix}.$$

求 A_n 的特征多项式.

习题 8.48. 请对以下 $f, g \in F[t]$ 求以下带余除法, $f = gq + r$.

1. $f = t^3 + 2t^2 + 3t + 4, g = t^2 + t + 1$.
2. $f = t^5 + t^4 + t^3 + t^2 + t + 1, g = t^3 + t^2 + t + 1$.

习题 8.49. 假设域 F 上的 n -阶矩阵 A 的特征多项式 $f_A(\lambda)$ 等于其极小多项式, 证明 A 相似于 f_A 的友阵.

习题 8.50. 请用直接计算行列式的方法计算出友阵的特征多项式.

习题 8.51.

1. 假设 I 是环 R 的理想, 请在商集 R/I 上定义加法和乘法, 使得 R/I 成为一个环.
2. 如果一个 F 线性空间 V 上的线性变换 T 对应的极小多项式是 $m(\lambda)$, 请证明 V 有 $F[\lambda]/(m(\lambda))$ -模结构.
3. 假设 n -维实线性空间 V 上有一个线性变换 T 满足 $T^2 = -I_n$. 请利用 T 给出 V 的一个复线性空间结构.
4. 在以上的条件下, 假设 A 是 V 上的所有和 T 交换的实线性变换组成的实线性空间. 请求出 $\dim_{\mathbb{R}} A$. (提示: 构造 A 和 $\text{End}_{\mathbb{C}} V$ 之间的同构.)

习题 8.52. 以下是使用对角化的极小多项式判定法则来求解微分方程的例子. 假设 V 是 \mathbb{R} 上无穷次可导的实值函数组成的线性空间. 线性变换 $D: V \rightarrow V$ 定义为 $D(f) = f'$. 令 $a_1 \cdots a_n$ 是互不相同的实数, W 是线性变换 $(D - a_1 Id) \circ \cdots \circ (D - a_n Id)$ 的 kernel. 证明

1. W 是 D 的不变子空间.
2. 模仿线性代数中对角化的极小多项式判定法则, 证明 W 是 $\ker(D - a_i Id)$ 的直和, 即 $W = \bigoplus_{i=1}^n \ker(D - a_i I)$.
3. 已知 $f' = f$ 的解形如 $f(x) = Ce^x$, 其中 C 是任意实数. 求解

$$f'' - 3f' + 2f = 0.$$

4. 进一步思考: 请尝试推广以上结论到齐次的常系数线性微分方程的情形. 你需要求解哪些基础的微分方程来得到所有的解.

习题 8.53. 假设 R 是交换环, $m \leq n$ 是正整数. 假设 $A \in M_{m \times n}(R)$ 是一个元素取值在 R 上的 $m \times n$ 矩阵. 假设 I 是 A 的 $m \times m$ 子式生成的 R 的理想. 对任意 $f \in I$, 存在矩阵 $B \in M_{n \times m}(R)$ 使得 $AB = fI_m$. 这里 $m \times m$ 子式指的是 A 中任意取出不重复的 m 行 m 列得到的行列式.

习题 8.54 (单特征值的一阶微扰公式). 设 n 阶实矩阵 A 的某个特征值为 $\lambda_0 \in \mathbb{R}$, 且代数重数为 1. 设 A 有右特征向量 v , A^T 有对应特征向量 u .

1. 证明 $u^T v$ 不可能为零.
2. 令 $A(t) = A + tC$. 在 $t = 0$ 附近设 $\lambda(t)$ 是对应的可微特征值函数, 且 $\lambda(0) = \lambda_0$. 求 $\lambda'(0)$.

习题 8.55 (实对称矩阵的 Stieltjes 变换与相似). 对于实对称矩阵 $A \in M_n(\mathbb{R})$, 定义

$$m_A(z) = \operatorname{tr}((A - zI)^{-1}), \quad z \in \mathbb{C} \setminus \mathbb{R}.$$

若 A_1, A_2 是两个 n 阶实对称矩阵, 且对 n 个不同的上半平面复数 z_1, \dots, z_n , 都有

$$m_{A_1}(z_k) = m_{A_2}(z_k) \quad (k = 1, \dots, n),$$

问是否一定有 A_1 与 A_2 相似? 请证明或给出反例.

习题 8.56 (半正定矩阵乘积的特征值界). 假设 A, B 都是正定实对称矩阵, 且最大特征值严格小于 1. 证明:

1. $2I - AB - BA$ 是正定矩阵;
2. $AB + BA + \frac{1}{2}I$ 是正定矩阵.

习题 8.57 (迹矩与谱半径). 设 A 是 $n \times n$ 实对称矩阵, 其特征值为 $\lambda_1, \dots, \lambda_n$. 证明: $\operatorname{tr}(A^{2m}) \leq C^m$ 对任意正整数 m 和某个常数 $C > 0$ 成立, 当且仅当 A 的所有特征值绝对值都不超过 \sqrt{C} .

习题 8.58 (秩一扰动与特征值交错). 设 A 是 $n \times n$ 实对称矩阵, 特征值为 $\lambda_1 \geq \dots \geq \lambda_n$. 设 $v \in \mathbb{R}^n$ 非零, $t > 0$, 令

$$\tilde{A} = A + tvv^T,$$

其特征值为 $\tilde{\lambda}_1 \geq \dots \geq \tilde{\lambda}_n$.

1. 证明秩一扰动的交错不等式.
2. 若 v 不与任何 A 的特征向量正交, 证明 \tilde{A} 的特征向量不与 v 正交, 且 \tilde{A} 的每个特征值都是关于 t 的严格单调函数.

习题 8.59 (强正则图的邻接矩阵). 设 G 是强正则图, 参数为 $\text{srg}(n, d, \lambda, \mu)$, 邻接矩阵为 A , J 为全 1 矩阵。

1. 证明

$$A^2 = dI + \lambda A + \mu(J - I - A),$$

并推出 A 至多有三个不同特征值。

2. 对 Petersen 图求出 A 的全部特征值及其重数。

习题 8.60 (Walsh–Hadamard 矩阵的谱). 对 $n \geq 0$, 递归定义

$$H_0 = (1), \quad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix} \quad (n \geq 1).$$

求 H_n ($n \geq 1$) 的全部特征值及其对应特征子空间的维数。

习题 8.61 (正交矩阵的负行列式). 假设实方阵 A 是 n 阶正交阵, 满足 $A^T A = I_n$, 且 $\det(A) < 0$ 。证明:

$$\det(I_n + A) = 0.$$

习题 8.62 (Perron–Frobenius 应用). 设 A 是一个 $n \times n$ 严格正矩阵, 所有元素 $a_{ij} > 0$, 并且每列元素之和都为 1。证明 $\lambda = 1$ 是 A 的特征值, 并且对于任意初始概率向量 $v > 0$, 序列 $A^k v$ 的极限存在。

9 双线性型与二次型

在前面的章节中, 我们系统地研究了线性空间上的线性变换理论. 从本节开始, 我们转向另一个核心问题: 在线性空间上引入“度量”结构. 这一问题的数学抽象正是双线性型的理论.

双线性型理论的核心内容包括: 对称双线性型(及其对应的二次型)的分类——Sylvester 惯性定理; 反对称双线性型的分类——辛标准形; 以及推广到复数域上的厄米特型. 这些理论不仅是下一节引入内积空间和谱定理的基础, 也在微分几何(黎曼度量)、辛几何和量子力学等领域有着广泛的应用.

从几何角度看, 二次型之所以重要, 是因为方程

$$ax^2 + bxy + cy^2 = 1$$

这样的表达式虽然外形复杂, 但经过适当的坐标变换后往往能够化成椭圆、双曲线或抛物线的标准形式. 也就是说, 对角化并不只是代数技巧, 而是在帮助我们识别一个几何对象真正的形状. 从分析和力学角度看, 二次型又经常扮演局部能量的角色: 正定时像一个碗, 不定时像一个马鞍, 因而它自然地联系到稳定性与极值问题. 甚至在狭义相对论中, Minkowski 度量对应的也是一个不定二次型, 其符号结构区分了不同类型的时空方向.

二次型与优化中的“地形”

多元函数在临界点附近常可用二次型近似:

$$f(x_0 + h) \approx f(x_0) + \frac{1}{2}h^T H h,$$

其中 H 是 Hessian 矩阵. 若 H 正定, 临界点附近像一个碗底, 是局部极小值; 若 H 有正有负, 附近像马鞍面, 不是极值点. 因此二次型的正定性不只是代数分类问题, 也帮助我们读懂函数局部的几何形状.

如无特殊说明, 本节中 \mathbb{F} 表示特征不为 2 的域.

9.1 双线性型与格拉姆矩阵

对偶空间

我们首先回顾对偶空间的概念, 它为理解双线性型提供了重要的视角.

定义 9.1. \mathbb{F} -线性空间 V 的**对偶空间** (*dual space*) 定义为

$$V^* := \text{Hom}_{\mathbb{F}}(V, \mathbb{F}) = \{f: V \rightarrow \mathbb{F} \mid f \text{ 是 } \mathbb{F}\text{-线性映射}\}.$$

V^* 中的元素称为 V 上的**线性函数** (*linear functional*).

命题 9.1. 设 $\{v_1, \dots, v_n\}$ 是 V 的一组基, 定义 $v_i^* \in V^*$ 为

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

则 $\{v_1^*, \dots, v_n^*\}$ 构成 V^* 的一组基, 称为 $\{v_1, \dots, v_n\}$ 的**对偶基** (*dual basis*). 特别地, $\dim V^* = \dim V$.

证明. 张成性: 任取 $f \in V^*$, 令 $a_i = f(v_i)$, 则 $f = \sum_{i=1}^n a_i v_i^*$, 因为两者在基向量 v_j 上的取值相同: $(f - \sum_{i=1}^n a_i v_i^*)(v_j) = a_j - a_j = 0$.

线性无关: 假设 $\sum_{i=1}^n a_i v_i^* = 0$, 则对任意 j 有 $0 = \sum_{i=1}^n a_i v_i^*(v_j) = a_j$. □

命题 9.2. 设 $B = \{v_1, \dots, v_n\}$, $C = \{w_1, \dots, w_n\}$ 是 V 的两组基, $(w_1, \dots, w_n) = (v_1, \dots, v_n)P$, 则对偶基之间满足

$$(w_1^*, \dots, w_n^*) = (v_1^*, \dots, v_n^*)(P^T)^{-1}.$$

注 9.1. 存在**典范同构** $(V^*)^* \cong V$, 由如下映射给出:

$$V \rightarrow (V^*)^*, \quad v \mapsto \text{ev}_v, \quad \text{ev}_v(f) := f(v), \quad \forall f \in V^*.$$

该同构的给出不依赖于基的选取.

双线性型

有了对偶空间的概念, 我们现在引入双线性型的定义.

定义 9.2. \mathbb{F} -线性空间 V 上的一个**双线性型** (*bilinear form*)是一个映射 $b: V \times V \rightarrow \mathbb{F}$, 满足对 V 中的任意向量 x, y, z 和 \mathbb{F} 中的任意标量 λ :

1. $b(x + y, z) = b(x, z) + b(y, z)$, $b(\lambda x, y) = \lambda b(x, y)$;
2. $b(x, y + z) = b(x, y) + b(x, z)$, $b(x, \lambda y) = \lambda b(x, y)$.

即 b 关于每个分量都是 \mathbb{F} -线性的.

定义 9.3. V 上的双线性型 b 称为

1. **对称的** (*symmetric*), 如果 $b(x, y) = b(y, x)$ 对任意 $x, y \in V$ 成立;
2. **反对称的** (*skew-symmetric*), 如果 $b(x, y) = -b(y, x)$ 对任意 $x, y \in V$ 成立.

注 9.2. 给定双线性型 $b: V \times V \rightarrow \mathbb{F}$, 固定第二个分量可以得到线性映射 $l_b: V \rightarrow V^*$, $v \mapsto b(v, -)$; 固定第一个分量可以得到 $r_b: V \rightarrow V^*$, $v \mapsto b(-, v)$. 反之, 任何 \mathbb{F} -线性映射 $\varphi: V \rightarrow V^*$ 都可以定义双线性型 $b(v, w) := (\varphi(v))(w)$. 因此 V 上的双线性型与 $\text{Hom}_{\mathbb{F}}(V, V^*)$ 中的元素一一对应.

格拉姆矩阵及其基变换

双线性型的具体表示依赖于基的选取, 这由格拉姆矩阵来刻画.

定义 9.4. 设 $B = \{v_1, \dots, v_n\}$ 是 V 的一组基, V 上双线性型 b 关于基 B 的**格拉姆矩阵** (Gram matrix) 定义为

$$G_B := (b(v_i, v_j))_{n \times n}.$$

对任意 $v = \sum_i x_i v_i, w = \sum_j y_j v_j \in V$, 有

$$b(v, w) = (x_1, \dots, x_n) G_B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

命题 9.3 (格拉姆矩阵的基变换公式). 设 $B = \{v_1, \dots, v_n\}, C = \{w_1, \dots, w_n\}$ 是 V 的两组基, $(w_1, \dots, w_n) = (v_1, \dots, v_n)P$, 则

$$G_C = P^T G_B P.$$

证明. 直接计算: $(G_C)_{ij} = b(w_i, w_j) = b(\sum_k p_{ki} v_k, \sum_l p_{lj} v_l) = \sum_{k,l} p_{ki} p_{lj} b(v_k, v_l) = (P^T G_B P)_{ij}$. □

注 9.3. 格拉姆矩阵的基变换公式说明: b 是对称的当且仅当 G_B 是对称矩阵; b 是反对称的当且仅当 G_B 是反对称矩阵. 这些性质不依赖于基的选取.

定义 9.5. 给定矩阵 $A, B \in M_n(\mathbb{F})$, 如果存在 $P \in GL_n(\mathbb{F})$ 满足 $B = P^T A P$, 则称 A 和 B **相合** (congruent). 因此, 同一个双线性型在不同基下的格拉姆矩阵是相合的.

定义 9.6. 给定带有双线性型的 \mathbb{F} -线性空间 $(V_1, b_1), (V_2, b_2)$, 一个**等距同构** (isometry) 是指线性同构 $f: V_1 \rightarrow V_2$, 满足

$$b_2(f(v), f(w)) = b_1(v, w), \quad \forall v, w \in V_1.$$

下面我们来看一个基本的例子. 设 \mathbb{F}^n 表示 \mathbb{F} 上 n 阶列向量空间, 任何方阵 $A \in M_n(\mathbb{F})$ 决定了 \mathbb{F}^n 上的一个双线性型:

$$b_A: \mathbb{F}^n \times \mathbb{F}^n \rightarrow \mathbb{F} \\ (x, y) \mapsto x^T A y$$

b_A 关于 x 和 y 都是线性的:

$$b_A(\lambda_1 x_1 + \lambda_2 x_2, \mu_1 y_1 + \mu_2 y_2) = \sum_{i,j=1}^2 \lambda_i \mu_j \cdot b_A(x_i, y_j), \quad \forall x_i, y_j \in \mathbb{F}^n, \lambda_i, \mu_j \in \mathbb{F}.$$

当 A 对称时 ($A = A^T$), b_A 也是对称的: $b_A(x, y) = b_A(y, x)$. 事实上, A 正是 b_A 关于标准基 $\{e_1, \dots, e_n\}$ 的格拉姆矩阵.

下面给出更多重要的例子.

例 9.1 (Minkowski 空间). 设 $V = \mathbb{R}^{n+1}$, 定义 **Lorentz 型**为

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n - x_{n+1} y_{n+1}.$$

这是一个对称双线性型, 在狭义相对论中有重要应用. 它的格拉姆矩阵为 $\text{diag}(1, \dots, 1, -1)$, 惯性指数为 $(n, 1)$.

例 9.2 (矩阵空间上的迹内积). 设 $V = M_{m \times n}(\mathbb{R})$, 定义

$$\langle A, B \rangle = \text{tr}(A^T B).$$

这是 V 上的一个对称双线性型. 在奇异值分解一节中, 我们将看到它实际上是一个内积, 称为 **Frobenius 内积**.

例 9.3 (函数空间上的积分双线性型). 设 V 是 $[0, 1]$ 上连续实值函数构成的 (无穷维) 线性空间, 定义

$$\langle f, g \rangle = \int_0^1 f(x)g(x) dx.$$

这是 V 上的一个对称双线性型. 可以验证它也是正定的, 因此定义了 V 上的一个内积. 这个例子表明双线性型理论远不限于有限维空间.

反之, 从上面 b_A 的例子可以看到, 任何 $n \times n$ 矩阵 A 都可以定义 \mathbb{F}^n 上的一个双线性型. 因此, 我们有以下命题.

命题 9.4 (双线性型空间与矩阵空间的同构). 设 V 是 n 维 \mathbb{F} -线性空间, B 是 V 的一组基. 记 $\text{Bil}(V)$ 为 V 上所有双线性型构成的 \mathbb{F} -线性空间, 则映射

$$\text{Bil}(V) \rightarrow M_n(\mathbb{F}), \quad b \mapsto G_B$$

是 \mathbb{F} -线性空间的同构. 特别地, $\dim \text{Bil}(V) = n^2$. 在此同构下, 对称双线性型对应对称矩阵, 反对称双线性型对应反对称矩阵.

9.2 对称双线性型与二次型

对称双线性型是双线性型理论中最重要的特殊情形. 在 $\text{char}(\mathbb{F}) \neq 2$ 的假设下, 对称双线性型和二次型之间存在一一对应, 这使得代数的和几何的观点可以自由转换. 本小节建立这一对应, 并证明对称双线性型的对角化定理.

二次型与极化恒等式

设 $A \in M_n(\mathbb{F})$ 对称, $x = (x_1, \dots, x_n)^T \in \mathbb{F}^n$, 则:

$$Q(x) = x^T A x$$

称为 \mathbb{F} 上 n 个变量 x_1, \dots, x_n 的二次型, 也称为线性空间 \mathbb{F}^n 上的二次型. 设 $A = (a_{ij})$, 则:

$$\begin{aligned} Q(x) &= (x_1, \dots, x_n) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i,j=1}^n a_{ij} x_i x_j \\ &= \sum_{i=1}^n a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j \end{aligned}$$

所以 $Q(x)$ 本质上是关于 x_1, \dots, x_n 的二次齐次多项式. 反之, 任何一个 n 元二次齐次多项式都可以唯一写成

$$f(x_1, \dots, x_n) = \sum_{i=1}^n c_{ii} x_i^2 + \sum_{i<j} c_{ij} x_i x_j.$$

它来自对称矩阵 $B = (b_{ij})$, 其中

$$b_{ii} = c_{ii}, \quad b_{ij} = b_{ji} = \frac{c_{ij}}{2} \quad (i < j).$$

矩阵 A 、双线性型 b 和二次型 Q 之间的关系为:

$$\begin{cases} Q(x) = b(x, x), \\ b(x, y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)). \end{cases}$$

因此 A 、 b 、 Q 中任一个决定另外两个. 并且 Q 满足平行四边形法则:

$$Q(x+y) + Q(x-y) = 2(Q(x) + Q(y)).$$

定义 9.7. 对于有限维向量空间 V 和域 \mathbb{F} , 函数 $Q: V \rightarrow \mathbb{F}$ 称为 V 上的二次型, 如果:

$$Q(\lambda x) = \lambda^2 Q(x), \quad \forall \lambda \in \mathbb{F}, x \in V$$

且由下式定义的函数:

$$b(x, y) := \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

是 V 上的对称双线性型. 此时称 b 为 Q 诱导的双线性型 (associated bilinear form).

上面的关系可以总结为以下命题.

命题 9.5 (极化恒等式). 设 b 是 \mathbb{F} -线性空间 V ($\text{char}(\mathbb{F}) \neq 2$) 上的对称双线性型, $Q(v) = b(v, v)$ 是对应的二次型. 则 b 由 Q 唯一确定:

$$b(v, w) = \frac{1}{2}(Q(v+w) - Q(v) - Q(w)).$$

推论 9.1. 设 b 是 V 上非零的对称双线性型 ($\text{char}(\mathbb{F}) \neq 2$), 则存在 $v \in V$ 使得 $b(v, v) \neq 0$ (即存在非迷向向量).

证明. 若对任意 $v \in V$ 都有 $b(v, v) = 0$, 则由极化恒等式, 对任意 $v, w \in V$ 有 $b(v, w) = 0$, 矛盾. \square

对角化定理

利用极化恒等式和正交补, 我们可以给出对称双线性型对角化的一个简洁证明.

定理 9.1 (对角化定理/正交基的存在性). 设 V 是 \mathbb{F} -线性空间 ($\text{char}(\mathbb{F}) \neq 2$), b 是 V 上的对称双线性型. 则存在 V 的一组基 $\{v_1, \dots, v_n\}$ 使得 b 的格拉姆矩阵为对角矩阵, 即 $b(v_i, v_j) = 0$ 对所有 $i \neq j$ 成立. 这样的基称为 b 的**正交基** (orthogonal basis).

证明. 对 $n = \dim V$ 用归纳法. $n = 0$ 或 $b \equiv 0$ 时显然成立. 设 $n \geq 1$ 且 b 不恒为零. 由推论 9.1, 存在 $v_1 \in V$ 使得 $b(v_1, v_1) \neq 0$. 令

$$W = \{w \in V \mid b(v_1, w) = 0\} = v_1^\perp.$$

考虑线性映射 $\varphi: V \rightarrow \mathbb{F}$, $w \mapsto b(v_1, w)$. 由于 $b(v_1, v_1) \neq 0$, φ 是满射, 故 $\dim W = \dim(\ker \varphi) = n - 1$.

我们证明 $V = \text{span}\{v_1\} \oplus W$. 对任意 $v \in V$, 令

$$w = v - \frac{b(v, v_1)}{b(v_1, v_1)}v_1,$$

则 $b(v_1, w) = b(v_1, v) - \frac{b(v, v_1)}{b(v_1, v_1)}b(v_1, v_1) = 0$, 故 $w \in W$, 于是 $v \in \text{span}\{v_1\} + W$. 又 $v_1 \notin W$ (因为 $b(v_1, v_1) \neq 0$), 故 $\text{span}\{v_1\} \cap W = \{0\}$.

由归纳假设, $b|_W$ 有正交基 $\{v_2, \dots, v_n\}$, 则 $\{v_1, v_2, \dots, v_n\}$ 是 V 关于 b 的正交基. \square

注 9.4. 定理 9.1 的证明也可以通过配方法来实现, 即下面要介绍的方法. 两种方法本质上是等价的: 归纳法中投影到 W 的过程正对应于配方法中的一步配方.

相合与二次型的对角化

给定:

$$Q(x_1, \dots, x_n) = (x_1, \dots, x_n)A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

设 P 为 $n \times n$ 可逆矩阵, 考虑变量替换:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P \begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix}, \quad \text{即 } x = P\tilde{x}$$

则:

$$Q(x) = (P\tilde{x})^T A (P\tilde{x}) = \tilde{x}^T (P^T A P) \tilde{x}$$

即变量替换对应的矩阵变换恰好是相合变换 (参见定义 9.5).

例 9.4. 考虑:

$$Q(x) = ax_1^2 + 2bx_1x_2 + cx_2^2.$$

先设 $a \neq 0$. 通过配方有

$$Q(x) = a \left(x_1 + \frac{b}{a}x_2 \right)^2 + \left(c - \frac{b^2}{a} \right) x_2^2$$

令:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \quad \text{或} \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

则:

$$P = \begin{pmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}, \quad P^T A P = \begin{pmatrix} a & 0 \\ 0 & c - \frac{b^2}{a} \end{pmatrix}$$

如果 $a > 0$ 且 $c - \frac{b^2}{a} > 0$, 则二次型是正定的.

若 $a = 0$ 但 $c \neq 0$, 则交换 x_1 与 x_2 后回到上面的情形. 若 $a = c = 0$, 则

$$Q(x) = 2bx_1x_2 = \frac{b}{2}((x_1 + x_2)^2 - (x_1 - x_2)^2),$$

这也给出了对角化形式.

一般来说, 对于 $Q(x) = x^T A x$ (A 对称), 通过反复配方, 可以找到可逆矩阵 P 使得

$$P^T A P = \text{diag}(\lambda_1, \dots, \lambda_n),$$

即对称矩阵总可以通过相合变换对角化. 这就是定理9.1的配方法证明.

9.3 非退化性与正交补

对角化定理 (定理9.1) 保证了正交基的存在性, 但还没有回答一个关键问题: 对角化后对角线上非零元素的个数及符号是否由双线性型本身唯一确定? 为了解答这一问题, 我们需要引入非退化性和正交补的概念. 这些概念不仅适用于对称双线性型, 也适用于反对称双线性型, 是后续所有分类定理的基础.

定义 9.8. 设 $b: V \times V \rightarrow \mathbb{F}$ 为双线性型. 定义 b 的核 (kernel) 或根 (radical) 为

$$\ker(b) := \{v \in V \mid b(v, w) = 0, \forall w \in V\}.$$

如果 $\ker(b) = 0$, 则称 b 是非退化的 (non-degenerate).

命题 9.6. 设 $\dim V = n$, B 是 V 的一组基, G_B 是 b 关于 B 的格拉姆矩阵. 则如下条件等价:

(i) b 是非退化的;

(ii) $\det G_B \neq 0$;

(iii) 映射 $l_b: V \rightarrow V^*, v \mapsto b(v, -)$ 是同构.

证明. (i) \Leftrightarrow (ii): $v = \sum x_i v_i \in \ker(b)$ 当且仅当 $G_B x = 0$, 其中 $x = (x_1, \dots, x_n)^T$. 所以 $\ker(b) = 0$ 当且仅当 G_B 可逆.

(i) \Leftrightarrow (iii): $\ker(l_b) = \{v \in V \mid b(v, w) = 0, \forall w \in V\} = \ker(b)$. 由于 $\dim V = \dim V^*$, l_b 是同构当且仅当 $\ker(l_b) = 0$. \square

定义 9.9. 对于任何子空间 $W \subseteq V$, 定义 W 的**正交补** (orthogonal complement) 为

$$W^\perp = \{v \in V \mid b(v, w) = 0, \forall w \in W\}.$$

命题 9.7. 设 b 是 V 上的对称或反对称双线性型, $W \subseteq V$ 是子空间, 则

$$\dim W + \dim W^\perp = \dim V + \dim(W \cap \ker(b)).$$

特别地, 若 b 非退化, 则 $\dim W^\perp = \dim V - \dim W$.

证明. 记 $R = \ker(b)$. 因为 b 对称或反对称, R 同时也是右根: 若 $u \in R$, 则 $b(v, u) = \pm b(u, v) = 0$. 因此 b 诱导出商空间 $\bar{V} = V/R$ 上的非退化双线性型.

令 $\bar{W} = (W + R)/R \subseteq \bar{V}$. 在非退化空间 \bar{V} 中, 正交补维数公式给出

$$\dim \bar{W} + \dim \bar{W}^\perp = \dim \bar{V}.$$

而 W^\perp 是 \bar{W}^\perp 在 V 中的原像, 所以

$$\dim W^\perp = \dim R + \dim \bar{W}^\perp.$$

又

$$\dim \bar{W} = \dim W - \dim(W \cap R), \quad \dim \bar{V} = \dim V - \dim R.$$

合并这些等式, 得

$$\dim W^\perp = \dim V - \dim W + \dim(W \cap R),$$

即所需公式. \square

注 9.5. 双线性型 b 的核 $\ker(b)$ 也常记为 $\text{Rad}(b)$, 称为 b 的**根** (radical). 根的概念对于统一处理对称、反对称和厄米特双线性型非常有用.

命题 9.8 (根的正交分解). 设 b 是 V 上的双线性型 (对称或反对称), 则存在子空间 $W \subseteq V$ 使得

$$V = \ker(b) \oplus W,$$

且 $b|_W$ 是非退化的. 特别地, $\text{rank}(b) = \dim W$.

证明. 取 $\ker(b)$ 的任意补空间 W (即 $V = \ker(b) \oplus W$). 若 $w \in W$ 满足 $b(w, w') = 0$ 对任意 $w' \in W$, 则对任意 $v = u + w' \in V$ ($u \in \ker(b)$, $w' \in W$), 因 b 对称或反对称, 有 $b(w, u) = \pm b(u, w) = 0$, 从而

$$b(w, v) = b(w, u) + b(w, w') = 0.$$

故 $w \in \ker(b)$, 从而 $w \in \ker(b) \cap W = \{0\}$. 因此 $b|_W$ 非退化. \square

引理 9.1. 设 b 是 V 上的对称或反对称双线性型. 若 b 非退化, 则对任意子空间 $W \subseteq V$, 以下等价:

(i) $V = W \oplus W^\perp$ (正交直和分解)

(ii) $b|_W$ 是非退化的

(iii) $b|_{W^\perp}$ 是非退化的

证明. (i) \Rightarrow (ii): 若 $v \in W$ 满足 $b(v, w) = 0$ 对任意 $w \in W$, 则 $v \in W \cap W^\perp = \{0\}$.

(ii) \Rightarrow (i): 由 b 非退化, $\dim W^\perp = \dim V - \dim W$, 故只需 $W \cap W^\perp = \{0\}$. 若 $v \in W \cap W^\perp$, 则 $b(v, w) = 0$ 对任意 $w \in W$, 由 $b|_W$ 非退化得 $v = 0$.

(i) \Rightarrow (iii): 类似 (i) \Rightarrow (ii).

(iii) \Rightarrow (i): 由 $b|_{W^\perp}$ 非退化, $(W^\perp)^\perp \cap W^\perp = \{0\}$. 注意 $W \subseteq (W^\perp)^\perp$, 又由维数公式 $\dim(W^\perp)^\perp = \dim V - \dim W^\perp = \dim W$, 故 $W = (W^\perp)^\perp$, 从而 $W \cap W^\perp = \{0\}$. \square

注 9.6. 上述引理的证明只用到了正交补的维数公式, 并不依赖 b 的对称性. 因此, 该引理同时适用于对称和反对称双线性型. 特别地, 在反对称双线性型标准型 (定理 9.3) 的证明中, 我们将反复使用这一引理.

9.4 Sylvester 惯性定理与正定性

利用上一小节建立的非退化性和正交补工具, 我们现在可以给出实对称双线性型分类的完整理论. Sylvester 惯性定理表明, 实对称双线性型在相合意义下由三个不变量 (p, q, r) 唯一确定, 其中 $r = \dim \ker(b)$. 由此自然引出正定性的概念, 它是下一节内积空间理论的出发点.

定理 9.2 (Sylvester 惯性定理). 对于带有对称双线性型 b 的实向量空间 V , 存在正交基:

$$v_1, \dots, v_p, v_{p+1}, \dots, v_{p+q}, v_{p+q+1}, \dots, v_n$$

使得 Gram 矩阵为:

$$\begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0 \end{pmatrix}$$

并且 p 和 q 是唯一确定的 (分别称为 b 的正、负惯性指数, $p - q$ 称为符号差).

为了证明定理, 我们首先引入正定性.

定义 9.10. 实向量空间 V 上的对称双线性型 b 称为:

- 正定的 ($b > 0$), 如果对所有 $v \neq 0$ 有 $b(v, v) > 0$;
- 半正定的 ($b \geq 0$), 如果对所有 v 有 $b(v, v) \geq 0$;
- 负定的 ($b < 0$), 如果对所有 $v \neq 0$ 有 $b(v, v) < 0$;
- 半负定的 ($b \leq 0$), 如果对所有 v 有 $b(v, v) \leq 0$.

定理 9.2 的证明. **存在性.** 由命题 9.8 (根的正交分解), 存在子空间 U 使得 $V = \ker(b) \oplus U$ 且 $b|_U$ 非退化. 设 $\dim \ker(b) = r$, 则只需证明 $(U, b|_U)$ 有正交基使得格拉姆矩阵为 $\text{diag}(I_p, -I_q)$.

对 $\dim U$ 归纳. 若 $\dim U = 0$ 则无需证明. 设 $\dim U \geq 1$. 由推论 9.1, 存在 $v_1 \in U$ 使得 $b(v_1, v_1) \neq 0$. 令 $W_1 = \text{span}\{v_1\}$, 则 $b|_{W_1}$ 非退化. 由引理 9.1, $U = W_1 \oplus W_1^\perp$, 且 $b|_{W_1^\perp}$ 也非退化. 对 W_1^\perp 施用归纳假设, 得到 U 的正交基 $\{v_1, \dots, v_{p+q}\}$, 其中 $b(v_i, v_i) \neq 0$ 对每个 i 成立. 令 $e_i = \frac{v_i}{\sqrt{|b(v_i, v_i)|}}$, 则 $b(e_i, e_i) = \pm 1$. 适当重排, 使得前 p 个为 $+1$, 后 q 个为 -1 . 再取 $\ker(b)$ 的一组基 $\{v_{p+q+1}, \dots, v_n\}$, 合在一起即得所求正交基.

唯一性. 设 $V = W_+ \perp W_- \perp W_0$, 其中 $b|_{W_+} > 0$, $b|_{W_-} < 0$, $W_0 = \ker(b)$, $\dim W_+ = p$, $\dim W_- = q$. 我们证明 p 和 q 只依赖于 (V, b) 本身.

若存在子空间 $W \subset V$ 满足 $\dim W \geq p+1$ 且 $b|_W > 0$, 则 $W \cap (W_- \oplus W_0) \neq \{0\}$ (维数比较), 取 $0 \neq v \in W \cap (W_- \oplus W_0)$, 则 $b(v, v) \leq 0$, 与 $b|_W > 0$ 矛盾. 从而

$$p = \max\{\dim W \mid W \subset V, b|_W > 0\}.$$

类似地, $q = \max\{\dim W \mid W \subset V, b|_W < 0\}$. 所以 p, q 由 (V, b) 唯一确定. \square

注 9.7. 存在性的证明也可以通过对角化定理 (定理 9.1) 得到: 先取正交基使格拉姆矩阵对角化, 再做适当伸缩. 但上述证明更直接地利用了命题 9.8 和引理 9.1 的正交直和分解.

正定性与欧几里得空间

上面 Sylvester 惯性定理的唯一性证明表明, 正定性是分类对称双线性型的关键概念. 下面我们系统整理正定性的基本性质.

命题 9.9. 设 A 是 $n \times n$ 实对称矩阵, 则以下条件等价:

- (i) A 正定 (即 $x^T A x > 0$ 对所有 $x \neq 0$);
- (ii) 存在可逆矩阵 P 使得 $A = P^T P$ (即 A 相合于 I_n);

(iii) A 的所有顺序主子式为正 (即 $\det(A_k) > 0$ 对 $k = 1, \dots, n$, 其中 A_k 是 A 的左上 $k \times k$ 子矩阵).

证明. (i) \Rightarrow (ii): 由 Sylvester 惯性定理, 惯性指数 $(p, q) = (n, 0)$, 故 A 相合于 I_n .

(ii) \Rightarrow (i): 若 $A = P^T P$, 则 $x^T A x = x^T P^T P x = \|P x\|^2 > 0$ 对 $x \neq 0$ 成立 (因 P 可逆).

(i) \Rightarrow (iii): 若 A 正定, 则 A 限制到 $\text{span}\{e_1, \dots, e_k\}$ 上仍正定, 故 A_k 也是正定实对称矩阵. 由 Sylvester 惯性定理, A_k 相合于 I_k , 因而 $\det(A_k) > 0$.

(iii) \Rightarrow (i) 的证明留作习题 (参见习题9.24), 这就是 Sylvester 顺序主子式判据. \square

注 9.8. 学完第10章的谱定理后, 还会得到一个常用判据: 实对称矩阵 A 正定当且仅当 A 的所有特征值都为正. 一个方向很直接: 若 $Ax = \lambda x$, $x \neq 0$, 则 $\lambda \|x\|^2 = x^T A x > 0$.

命题 9.10 (谱定理后的半正定判据). 设 A 是 $n \times n$ 实对称矩阵, 则以下条件等价:

(i) A 半正定 (即 $x^T A x \geq 0$ 对所有 x);

(ii) 存在 (可能不可逆) 矩阵 B 使得 $A = B^T B$;

(iii) A 的所有特征值非负.

注 9.9. 这个命题的证明需要用到谱定理: 若 $A = Q^T \Lambda Q$, 则 $x^T A x$ 的符号完全由对角线上的特征值决定; 若所有特征值非负, 可取 $B = \Lambda_+^{1/2} Q$, 其中 $\Lambda_+^{1/2}$ 是非负平方根对角矩阵.

正定的对称双线性型自然地给出了线性空间上的“度量”结构.

定义 9.11. 实线性空间 V 上的正定对称双线性型称为 V 上的**内积** (inner product). 配备了内积的实有限维线性空间 $(V, \langle \cdot, \cdot \rangle)$ 称为**欧几里得空间** (Euclidean space). 内积空间的详细理论将在第10节中系统发展.

注 9.10. 上述理论可以推广到复数域. 在 \mathbb{C} -线性空间上, 对称双线性型的自然类比是**厄米特型** (Hermitian form), 即满足 $h(v, w) = \overline{h(w, v)}$ 的半双线性型. 正定厄米特型给出**酉空间**的概念, 类比于实数域上的欧几里得空间. 这些内容将在第10节的10.6小节中详细讨论.

9.5 反对称双线性型与辛矩阵

本节讨论反对称双线性型的分类. 与对称情形不同, 反对称双线性型在任何域 (特征 $\neq 2$) 上有一个干净的标准型, 且没有惯性指数的歧义.

命题 9.11. 设 b 是 \mathbb{F} -线性空间 V 上的反对称双线性型 (即 $b(v, w) = -b(w, v)$). 则对任意 $v \in V$ 有 $b(v, v) = 0$.

证明. $b(v, v) = -b(v, v)$, 故 $2b(v, v) = 0$. 当 $\text{char}(\mathbb{F}) \neq 2$ 时, $b(v, v) = 0$. \square

命题 9.12 (选读: 辛矩阵的行列式). 对任意 $M \in \text{Sp}_{2n}(\mathbb{F})$, 有 $\det M = 1$.

证明. 由 $M^T J_{2n} M = J_{2n}$ 两边取行列式, $(\det M)^2 \det J_{2n} = \det J_{2n}$. 由于 $\det J_{2n} = 1 \neq 0$, 故 $(\det M)^2 = 1$, 即 $\det M = \pm 1$.

为证 $\det M = 1$, 利用 Pfaffian (普法夫值). 对 $2n \times 2n$ 反对称矩阵 A , 其 Pfaffian $\text{Pf}(A)$ 满足 $\text{Pf}(A)^2 = \det A$ 和 $\text{Pf}(M^T A M) = \det M \cdot \text{Pf}(A)$. 由 $M^T J_{2n} M = J_{2n}$ 得 $\text{Pf}(J_{2n}) = \det M \cdot \text{Pf}(J_{2n})$. 由于 $\text{Pf}(J_{2n}) = 1 \neq 0$, 故 $\det M = 1$. \square

命题 9.13. 若 $M \in \text{Sp}_{2n}(\mathbb{F})$, 则 $M^T \in \text{Sp}_{2n}(\mathbb{F})$.

证明. 由 $M^T J_{2n} M = J_{2n}$, 两边求逆得 $M^{-1} J_{2n}^{-1} (M^T)^{-1} = J_{2n}^{-1}$. 注意 $J_{2n}^{-1} = -J_{2n}$, 故 $M^{-1} (-J_{2n}) (M^T)^{-1} = -J_{2n}$, 即 $(M^T)^{-1} (-J_{2n})^{-1} M^{-1} = (-J_{2n})^{-1}$, 化简得 $(M^{-1})^T J_{2n} M^{-1} = J_{2n}$. 再由 $M^T J_{2n} M = J_{2n}$ 得 $M^{-1} = J_{2n}^{-1} (M^T)^{-1} J_{2n} = -J_{2n} (M^T)^{-1} J_{2n}$, 代入可验证 $(M^T)^T J_{2n} M^T = J_{2n}$. \square

例 9.5. $\text{Sp}_2(\mathbb{F}) = \text{SL}_2(\mathbb{F})$, 因为 $M^T J M = J$ 等价于 $\det M = 1$ (对 2×2 矩阵).

9.6 习题

9.6.1 练习题

习题 9.1 (二维二次型的正定性). 判断下列二次型是否正定、负定、不定或半正定, 并尽量用配方法解释几何形状.

$$Q_1(x, y) = x^2 + 2xy + 2y^2,$$

$$Q_2(x, y) = x^2 - 4xy + y^2,$$

$$Q_3(x, y) = x^2 + 2xy + y^2.$$

习题 9.2. 设 V 是 n 维 \mathbb{F} -线性空间, $\{v_1, \dots, v_n\}$ 是 V 的一组基, $\{v_1^*, \dots, v_n^*\}$ 是对偶基. 证明对偶空间的如下性质:

(1) 对任意 V 的子空间 W , 定义 $W^0 = \{f \in V^* \mid f(w) = 0, \forall w \in W\}$ (称为 W 的零化子). 证明 $\dim W^0 = \dim V - \dim W$.

(2) 证明映射 $W \mapsto W^0$ 给出 V 的子空间格到 V^* 的子空间格的一个反序双射.

习题 9.3. 设 b 是 n 维 \mathbb{F} -线性空间 V 上的双线性型, G_B 是 b 关于基 B 的格拉姆矩阵. 证明:

- (1) $\text{rank}(b) := \text{rank}(G_B)$ 不依赖于基的选取;
- (2) $\text{rank}(b) = n - \dim \ker(b)$;
- (3) b 是对称的当且仅当 G_B 是对称矩阵 (对任意基 B).

习题 9.4. 设 $A \in M_n(\mathbb{R})$ 对称. 证明存在可逆矩阵 P 使得 $P^T A P$ 为对角矩阵 (利用配方法, 对 n 归纳).

习题 9.5. 设 A 是 4×4 实对称矩阵, 已知 A 的特征值为 $3, 3, -1, 0$. 求 A 的惯性指数 (p, q) .

习题 9.6. 设 $A \in M_n(\mathbb{R})$ 满足 $A^T = -A$ (反对称). 证明:

(1) $\text{rank}(A)$ 为偶数;

(2) 若 n 为奇数, 则 $\det A = 0$;

(3) 对任意 $x \in \mathbb{R}^n$, $x^T A x = 0$.

习题 9.7. 设 b 是 V 上的非退化对称双线性型, W 是 V 的子空间. 证明 $(W^\perp)^\perp = W$.

习题 9.8. 设 b 是 V 上的对称双线性型, $V = W_1 \perp W_2$ (正交直和). 证明 $\ker(b) = \ker(b|_{W_1}) \oplus \ker(b|_{W_2})$.

习题 9.9. 对实二次型 $Q(x_1, x_2, x_3) = x_1^2 + 4x_1x_2 + 4x_2^2 + 2x_1x_3 + 4x_2x_3 + x_3^2$, 用配方法化为标准型, 并求惯性指数.

习题 9.10. 设 $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ 是实对称矩阵. 证明 A 正定当且仅当 $a > 0$ 且 $ac - b^2 > 0$.

习题 9.11. 设 A 是 $n \times n$ 正定实对称矩阵, B 是 $n \times m$ 实矩阵且 $\text{rank}(B) = m$. 证明 $B^T A B$ 也是正定的.

习题 9.12. 设

$$B(x, y) = x_1y_1 + 2x_1y_2 + 2x_2y_1 + 3x_2y_2.$$

写出双线性型 B 的矩阵。

习题 9.13. 把二次型

$$q(x, y) = 2x^2 + 4xy + 5y^2$$

写成矩阵形式 $\begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}$ 。

习题 9.14. 用配方法化简

$$q(x, y) = x^2 + 4xy + 5y^2.$$

习题 9.15. 判断二次型

$$q(x, y) = x^2 + 2xy + y^2$$

是否正定、半正定或不定。

习题 9.16. 设

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

判断 $x^T Ax$ 是否正定。

习题 9.17. 画出或描述方程

$$x^2 + 4y^2 = 1$$

表示的曲线, 并说明它与二次型的关系。

9.6.2 思考题

习题 9.18. (*Williamson 定理*) 设 A 是 $2n \times 2n$ 实正定对称矩阵. 证明存在 $M \in \text{Sp}_{2n}(\mathbb{R})$ 使得

$$M^T A M = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix},$$

其中 $D = \text{diag}(d_1, \dots, d_n)$, $d_i > 0$. (提示: 考虑 $A^{-1} J_{2n}$ 的特征值.)

习题 9.19. 设 V 是 \mathbb{F} -线性空间 ($\text{char}(\mathbb{F}) \neq 2$), b 是 V 上的非退化反对称双线性型. 设 $W \subset V$ 是满足 $b|_W = 0$ 的子空间 (称为**迷向子空间**). 证明 $\dim W \leq \frac{1}{2} \dim V$.

习题 9.20. 证明: 矩阵 $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_{2n}(\mathbb{F})$ 属于 $\text{Sp}_{2n}(\mathbb{F})$ 当且仅当

$$A^T C - C^T A = 0, \quad B^T D - D^T B = 0, \quad A^T D - C^T B = I_n.$$

习题 9.21. 设 V 上有一个非退化双线性型 b (不一定对称). 对任意线性变换 $\varphi: V \rightarrow V$, 定义**伴随变换** φ^* 为满足 $b(\varphi(v), w) = b(v, \varphi^*(w))$ 的唯一线性变换.

(1) 证明 φ^* 存在且唯一;

(2) 设 b 对称, 证明 $(\varphi^*)^* = \varphi$;

(3) 设 b 对称且 A 是 φ 关于正交基的矩阵, 证明 φ^* 对应的矩阵是 A^T .

习题 9.22. 设 b_1, b_2 是 \mathbb{F} -线性空间 V 上的两个非退化对称双线性型. 证明存在唯一的线性同构 $T: V \rightarrow V$ 使得 $b_2(v, w) = b_1(Tv, w)$ 对任意 $v, w \in V$ 成立.

习题 9.23. 设 V 是域 $\mathbb{F} (\text{char}(\mathbb{F}) \neq 2)$ 上的 n 维线性空间, $\langle \cdot, \cdot \rangle$ 是 V 上的非退化对称双线性型.

(1) 设 W 是 V 的子空间. 证明 $V = W \oplus W^\perp$ 当且仅当 $\langle \cdot, \cdot \rangle$ 限制在 W 上是非退化的.

(2) 当 $\mathbb{F} = \mathbb{R}$ 时, 证明正定的对称双线性型一定是非退化的.

(3) 对于 \mathbb{R} 上的内积空间 V , 证明对任意子空间 W 有 $V = W \oplus W^\perp$.

(4) 在四维 Minkowski 空间 $(\mathbb{R}^4, \langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4)$ 中, 找到一个一维子空间 W 使得 W 和 W^\perp 不能直和为整个空间.

习题 9.24. (顺序主子式判据) 设 A 是 $n \times n$ 实对称矩阵, 记 A_k 为 A 的左上 $k \times k$ 子矩阵 ($k = 1, \dots, n$).

(1) 证明: 若 A 正定, 则所有主子式 (即删去某些行和对应列后的子矩阵的行列式) 均为正. (提示: 考虑双线性型限制到相应子空间.)

(2) 证明: 若 A 的所有顺序主子式 $\det(A_k) > 0$ ($k = 1, \dots, n$), 则 A 正定. (提示: 对 n 归纳, 利用非退化双线性型的正交分解.)

习题 9.25. 设 A 是 $n \times n$ 实对称矩阵, 对角线元素均为 2, 两条次对角线上的元素均为 -1 , 其余元素为 0. 证明 A 正定.

习题 9.26. 证明: 实线性空间 V 上的任何双线性型 b 都可以唯一分解为一个对称双线性型与一个反对称双线性型之和:

$$b = b_s + b_a, \quad b_s(v, w) = \frac{1}{2}(b(v, w) + b(w, v)), \quad b_a(v, w) = \frac{1}{2}(b(v, w) - b(w, v)).$$

习题 9.27. 设 g 是实线性空间 V 上的双线性型. 证明: 若 g 满足 $g(x, y) = 0 \Leftrightarrow g(y, x) = 0$, 则 g 要么是对称的, 要么是反对称的.

习题 9.28. (Gram-Schmidt 正交化练习) 以下两题任选一题.

(1) 设 $V = P_{\leq 2}(\mathbb{R})$ 是次数 ≤ 2 的实多项式空间, 内积定义为 $\langle f, g \rangle = \int_0^1 f(x)g(x) dx$. 对基 $\{1, x, x^2\}$ 实施 Gram-Schmidt 正交化, 求 V 的标准正交基.

(2) 计算矩阵 $A = \begin{pmatrix} 3 & 2 & 100 \\ 4 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix}$ 的 QR 分解.

习题 9.29. 证明 QR 分解的唯一性: 若 A 是 $n \times n$ 实可逆矩阵, 则存在唯一的正交矩阵 Q 和唯一的对角线元素为正的上三角矩阵 R , 使得 $A = QR$.

习题 9.30. (Cauchy-Schwarz 不等式) 设 $(V, \langle \cdot, \cdot \rangle)$ 是内积空间, $\|u\| = \sqrt{\langle u, u \rangle}$. 证明对任意 $u, v \in V$:

$$|\langle u, v \rangle| \leq \|u\| \cdot \|v\|,$$

且等号成立当且仅当 u, v 线性相关. (提示: 考虑 $f(\lambda) = \langle u - \lambda v, u - \lambda v \rangle$.)

习题 9.31. (*Hilbert 矩阵*) 证明 n 阶 *Hilbert 矩阵*

$$H_n = \left(\frac{1}{i+j-1} \right)_{n \times n}$$

是正定矩阵. (提示: 利用 $\langle f, g \rangle = \int_0^1 f(x)g(x) dx$, 考虑 $f_i(x) = x^{i-1}$.)

习题 9.32. (*Minkowski 空间的逆 Cauchy-Schwarz 不等式*) 对于 $v = (v_0, v_1, \dots, v_n), w = (w_0, w_1, \dots, w_n) \in \mathbb{R}^{n+1}$, 设 Lorentz 型 $\langle v, w \rangle = v_0w_0 - v_1w_1 - \dots - v_nw_n$. 若 $\langle v, v \rangle > 0$ 且 $\langle w, w \rangle > 0$ (即 v, w 是“类时向量”), 证明

$$\langle v, v \rangle \langle w, w \rangle \leq \langle v, w \rangle^2,$$

并确定等号成立的充要条件. (注意不等号方向与 *Cauchy-Schwarz 不等式* 相反!)

习题 9.33. (*ADE Dynkin 图的 Cartan 矩阵*) 对于图 Γ , 顶点集为 $\{v_1, \dots, v_n\}$, 定义 $n \times n$ 实对称矩阵 $A_\Gamma = (a_{ij})$ 如下: $a_{ii} = 2$; 若 v_i, v_j 相邻则 $a_{ij} = -1$; 否则 $a_{ij} = 0$. 证明以下图 Γ 对应的 A_Γ 是正定矩阵:

- (1) A_n : n 个顶点排成一排, 相邻顶点连边;
- (2) D_n : A_{n-1} 加上一个额外顶点连接到第 $n-2$ 个顶点;
- (3) E_6, E_7, E_8 : 参见 *Dynkin 图* 的定义.

习题 9.34. 设 V 是二乘二实矩阵组成的线性空间, 定义 V 上的双线性型

$$g(X, Y) = \text{tr}(XY).$$

- (1) 证明 g 是对称双线性型.
- (2) 对于 V 的一组基

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

求 g 在这组基下的格拉姆矩阵.

- (3) 求 g 的正、负惯性指标 p, q .

习题 9.35. 对以下的对称实矩阵 A , 找到可逆矩阵 P , 使得 $P^T A P$ 是对角线为 $1, -1, 0$ 的对角矩阵.

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

习题 9.36. 假设 V 是关于 x 的次数小于或等于 3 次的实系数多项式组成的实线性空间. 定义 V 上的对称双线性型为 $B(f, g) = \int_{-1}^1 f(x)g(x)dx$. 求 B 的符号 (正负惯性指数).

习题 9.37. 定义 $M_n(\mathbb{R})$ 上的一个对称双线性型

$$g(X, Y) = \text{tr}(X^T Y).$$

证明这个双线性型是正定的.

习题 9.38. 定义 $M_n(\mathbb{R})$ 上的一个对称双线性型

$$g(X, Y) = \text{tr}(XY).$$

求这个双线性型的正、负惯性指标.

习题 9.39. 计算下列对称矩阵 A 的符号 (p, q, r) , 需要过程:

$$(1) A = \begin{bmatrix} 2 & -2 & 0 \\ -2 & 1 & -2 \\ 0 & -2 & 0 \end{bmatrix};$$

$$(2) A = \begin{bmatrix} 2 & 2 & -2 \\ 2 & 5 & -4 \\ -2 & -4 & 5 \end{bmatrix};$$

$$(3) A = \begin{bmatrix} 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 4 \\ 4 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \end{bmatrix};$$

$$(4) A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

习题 9.40. 请分类 \mathbb{C} 上有限维线性空间上的对称双线性型. 或者等价的, 分类 \mathbb{C} 上的 n 阶对称矩阵的相合类 (合同类).

习题 9.41. 证明如果 A 是正定实对称矩阵, 则 A 的伴随矩阵也是正定对称实矩阵. 反之是否成立呢?

习题 9.42. 请判断以下结论是否成立, 并说明理由.

(1) 如果 A 是半正定实矩阵, 则 A 的所有主子式都非负.

(2) 如果 A 的所有顺序主子式非负, 则 A 是半正定实矩阵.

(3) 如果 A 的所有主子式 (第 i_1, \dots, i_r 行, 第 i_1, \dots, i_r 列组成的子矩阵的行列式) 非负, 则 A 是半正定实矩阵.

习题 9.43. 假设 A 是正定实对称矩阵, B 是实对称矩阵, 证明存在实数 c 使得 $cA + B$ 是正定矩阵.

习题 9.44. 假设 A 是一个半正定的实对称矩阵, 证明对 $x \in \mathbb{R}^n$, $x^T Ax = 0$ 等价于 $Ax = 0$.

习题 9.45. 假设 A 和 B 是 n 阶正定实对称方阵, 证明 $\det(A + B) > \det(A)$.

习题 9.46 (Hermitian 矩阵空间上的双线性型). 设 W 为 2×2 厄米特矩阵构成的实向量空间:

$$W = \{A \in M_2(\mathbb{C}) \mid \overline{A}^T = A\}.$$

证明

$$\langle A, A' \rangle = \det(A + A') - \det(A) - \det(A')$$

是 W 上的一个对称双线性型, 并计算它的符号差 (或惯性指数).

习题 9.47 (三维对称双线性型的标准形). 设 $V = \mathbb{R}^3$, 双线性型 B 在标准基下的矩阵为

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 5 & 1 \\ 0 & 1 & 3 \end{pmatrix}.$$

1. 判断 B 是否为对称双线性型, 并求其符号差.

2. 利用配方法或 *Sylvester* 消去法将 B 化为标准形 $\sum \lambda_i y_i^2$.

习题 9.48 (反对称双线性型与最大全零子空间). 假设 V 是一个 n 维复向量空间, ω 是 V 上非退化反对称双线性型.

1. 求

$$\max\{\dim W \mid W \subset V, \omega(v, u) = 0, \forall v, u \in W\}.$$

2. 如果将 ω 改为非退化对称双线性型 B , 求对应最大值.

习题 9.49 (可逆对称矩阵与反对称矩阵). 设 A 为可逆实对称矩阵, S 为实反对称矩阵.

1. 若 $AS = SA$, 证明 $A + S$ 可逆.

2. 若 A 正定, 证明 $A + S$ 可逆, 并进一步证明 $\det(A + S) > 0$.

习题 9.50 (对称与反对称矩阵空间上的迹). 设 A 是一个 $n \times n$ 的实矩阵, 特征多项式为

$$p_A(\lambda) = \det(\lambda I - A) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0.$$

设 V, W 分别为 n 阶对称矩阵和反对称矩阵组成的线性空间. 分别求线性变换

$$L: V \rightarrow V, \quad L(X) = AXA^T,$$

$$S: W \rightarrow W, \quad S(Y) = AY A^T$$

的迹。

习题 9.51 (Schur 补与正定判别). 设

$$M = \begin{pmatrix} A & B \\ B^T & D \end{pmatrix},$$

其中 $A \in M_n(\mathbb{R})$ 与 $D \in M_m(\mathbb{R})$ 都是实对称矩阵. 证明: M 正定的充要条件是 A 正定, 且

$$D - B^T A^{-1} B$$

正定。

习题 9.52 (图对应的二次型). 设 G 是简单无向图, 邻接矩阵为 $A = (a_{ij})$. 定义二次型

$$Q_G(x_1, \dots, x_n) = \sum_{i=1}^n 2x_i^2 - 2 \sum_{i < j} a_{ij} x_i x_j,$$

对应矩阵 $C_G = 2I - A$. 已知 G 连通且 Q_G 半正定. 证明:

1. 对 G 任意去掉一条边得到的新图 G' , $Q_{G'}$ 严格正定。
2. G 中没有五重点。
3. G 中的三重点个数小于或等于 2。

习题 9.53 (二次型的负惯性指数下界). 假设 b_1, \dots, b_n 是 n 个复数, q 是关于 $2n$ 个实变元 $x_1, y_1, \dots, x_n, y_n$ 的正定二次型. 定义

$$Q = \operatorname{Re}(b_1(x_1 + \sqrt{-1}y_1)^2 + \cdots + b_n(x_n + \sqrt{-1}y_n)^2) - q(x_1, y_1, \dots, x_n, y_n).$$

证明 Q 的负惯性指数大于或等于 n 。

习题 9.54 (复对称矩阵的秩—线性组合). 设 A, B, C, D 是 3×3 的复对称矩阵. 证明存在不全为零的复数 a, b, c, d , 使得

$$\operatorname{rank}(aA + bB + cC + dD) \leq 1.$$

习题 9.55 (矩阵的惯性指数). 计算以下对称矩阵 A 的惯性指数 $(p, q, n - p - q)$:

$$A = \begin{bmatrix} 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 4 \\ 4 & 1 & 0 & 0 \\ 1 & 4 & 0 & 0 \end{bmatrix}.$$

习题 9.56 (反对称矩阵的二次型刻画). 证明 n 阶实方阵 A 是反对称的, 当且仅当对任意列向量 $x \in \mathbb{R}^n$ 有

$$x^T A x = 0.$$

习题 9.57 (二次型映射的凸性). 假设 A 和 B 是两个 n 阶实对称矩阵. 证明映射

$$f: \mathbb{R}^n \rightarrow \mathbb{R}^2, \quad f(x) = \begin{pmatrix} x^T A x \\ x^T B x \end{pmatrix}$$

的像是一个凸集。

习题 9.58 (正定性的迹判别). 假设 A 是一个 n 阶可逆实对称矩阵. 证明: A 正定等价于对于任意 n 阶正定实对称矩阵 B , 都有

$$\text{tr}(AB) > 0.$$

习题 9.59 (反对称矩阵空间). 设 \mathcal{S}_n 表示所有 $n \times n$ 反对称实矩阵构成的实向量空间, 内积为

$$\langle X, Y \rangle = \text{tr}(X^T Y) = -\text{tr}(XY).$$

1. 求所有对称线性变换 $\mathfrak{R}: \mathcal{S}_n \rightarrow \mathcal{S}_n$ 构成的空间维数。
2. 证明 $X \in \mathcal{S}_n$ 的秩为 2 当且仅当存在线性无关的 $u, v \in \mathbb{R}^n$, 使 $X = uv^T - vu^T$ 。
3. 当 $n = 4$ 时证明某半正定判别, 并通过 $n = 6$ 的例子说明逆命题不成立。

10 内积空间与谱定理

本章研究正定对称双线性型 (内积) 赋予线性空间的丰富几何结构. 在第9章中, 我们已经建立了双线性型的一般理论和分类. 现在我们聚焦于正定情形, 依次发展内积空间、正交矩阵、实对称矩阵的正交对角化 (谱定理), 以及厄米特型与酉空间的类似理论. 奇异值分解及其应用将在下一节中专门讨论.

内积空间之所以重要, 是因为它把纯代数对象变成了可以谈论长度、夹角、距离和投影的几何对象. 在数据拟合中, 最小二乘法寻找的正是离目标最近的点, 其几何本质是正交投影; 在力学中, 多个耦合振子可以通过谱定理分解成彼此正交的正常模; 在量子力学中, 可观测量对应厄米特算子. 因此本章的定义虽然熟悉, 背后却在为一整套几何与物理语言奠基.

10.1 内积空间

在第9节中, 我们已经建立了对称双线性型的一般理论, 包括正定性的等价刻画 (命题9.9) 和欧几里得空间的定义 (定义9.11). 本节系统发展内积空间的几何理论.

回顾定义9.11, 内积空间 (V, g) 是配备了正定对称双线性型的实有限维线性空间. 由正定性, g 一定是非退化的, 从而对任意子空间 $W \subset V$ 有正交分解 $V = W \oplus W^\perp$.

定义 10.1.

(i) 设 (V, g) 是 \mathbb{R} -向量空间, $g > 0$, 则称 (V, g) 为**内积空间**(*inner product space*), g 称为**内积**(*inner product*).

(ii) 若 $\dim V = n$, 则 $(\mathbb{R}^n, \text{标准内积})$ 称为**标准内积空间**.

特别地, 对于任意 n 维内积空间 V , 存在基 $B = (v_1, \dots, v_n)$ 使得 $g(v_i, v_j) = \delta_{ij}$ (称为**标准正交基**(*orthonormal basis*)), 进而有同构 $(V, g) \cong (\mathbb{R}^n, \langle \cdot, \cdot \rangle)$.

定义 10.2. 给定内积空间 (V, g) , 定义二次型 $Q(v) = g(v, v)$, 则 $Q(v) > 0$ 对 $v \neq 0$. 定义 $|v| = \sqrt{Q(v)}$ 为 v 的长度, $d(v, w) = |v - w|$ 为 v, w 的距离.

定理 10.1 (Cauchy-Schwarz 与三角不等式).

(i) (*Cauchy-Schwarz*) 对任意 $v, w \in V$, 有 $|g(v, w)| \leq |v| \cdot |w|$. 等号成立当且仅当 v, w 线性相关;

(ii) (向量三角不等式) 对任意 $v, w \in V$, 有 $|v + w| \leq |v| + |w|$. 等号成立当且仅当 v, w 同向, 即存在 $\lambda \geq 0$ 使得 $v = \lambda w$ 或 $w = \lambda v$;

(iii) (距离三角不等式) 对任意 $u, v, w \in V$, 有 $d(u, v) \leq d(u, w) + d(w, v)$. 等号成立当且仅当存在 $\lambda \in [0, 1]$ 使得 $w = \lambda u + (1 - \lambda)v$ (即 w 在 u, v 的连线段上).

证明. (i) 若 $w = 0$ 显然. 若 $w \neq 0$, 考虑

$$0 \leq Q(v - \lambda w) = |w|^2 \lambda^2 - 2g(v, w)\lambda + |v|^2$$

作为关于实数 λ 的二次函数, 其判别式不大于 0, 即得 Cauchy-Schwarz 不等式. 等号成立当且仅当某个 $v - \lambda w = 0$, 即 v, w 线性相关.

(ii) 由 (i) 有

$$|v + w|^2 = |v|^2 + 2g(v, w) + |w|^2 \leq (|v| + |w|)^2.$$

等号成立当且仅当 $g(v, w) = |v||w|$, 即 v, w 同向.

(iii) 对 $v - u = (v - w) + (w - u)$ 应用 (ii) 即可. 等号条件正是两个向量 $v - w$ 与 $w - u$ 同向, 也就是 w 位于 u 到 v 的线段上. \square

定义 10.3. 对 $v, w \in V \setminus \{0\}$, 定义夹角 $\theta \in [0, \pi]$ 满足

$$\cos \theta = \frac{g(v, w)}{|v||w|}.$$

若 $g(v, w) = 0$, 则 $\theta = \frac{\pi}{2}$, 称 v, w 正交.

欧几里得空间的几何

Cauchy-Schwarz 不等式使我们能够在内积空间中建立完整的度量几何结构. 我们首先系统整理范数的基本性质.

命题 10.1 (范数的性质). 设 (V, g) 是内积空间, $\|v\| = \sqrt{g(v, v)}$, 则:

(i) **正性:** $\|v\| \geq 0$, 且 $\|v\| = 0$ 当且仅当 $v = 0$;

(ii) **齐次性:** $\|\lambda v\| = |\lambda| \cdot \|v\|, \forall \lambda \in \mathbb{R}$;

(iii) **三角不等式:** $\|v + w\| \leq \|v\| + \|w\|$;

(iv) **平行四边形法则:** $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$.

命题 10.2 (勾股定理). 若 $v_1, \dots, v_k \in V$ 两两正交 (即 $g(v_i, v_j) = 0$ 对 $i \neq j$), 则

$$\|v_1 + \dots + v_k\|^2 = \|v_1\|^2 + \dots + \|v_k\|^2.$$

证明. $\|v_1 + \dots + v_k\|^2 = g(\sum_i v_i, \sum_j v_j) = \sum_{i,j} g(v_i, v_j) = \sum_i g(v_i, v_i) = \sum_i \|v_i\|^2$. \square

距离函数 $d(v, w) = \|v - w\|$ 满足度量空间的公理.

命题 10.3 (度量空间). 设 (V, g) 是内积空间, 定义 $d: V \times V \rightarrow \mathbb{R}, d(v, w) = \|v - w\|$, 则:

(i) **正性:** $d(v, w) \geq 0$, 且 $d(v, w) = 0$ 当且仅当 $v = w$;

(ii) 对称性: $d(v, w) = d(w, v)$;

(iii) 三角不等式: $d(u, v) \leq d(u, w) + d(w, v)$.

因此 (V, d) 构成一个度量空间 (metric space).

对于 V 的子集 S , 定义 v 到 S 的距离为

$$d(v, S) := \inf_{w \in S} \|v - w\|.$$

当 $S = W$ 是子空间时, 下面的正交投影命题给出了距离的精确公式.

到子空间的距离与正交投影

内积空间中, 距离函数可以用来衡量向量到子空间的距离, 这是最小二乘法等应用的数学基础.

正交投影就是“最佳近似”

当目标向量 b 不在子空间 W 中时, W 中离 b 最近的点是 b 在 W 上的正交投影. 最小二乘法正是这个命题的矩阵版本: 若方程 $Ax = b$ 无解, 我们就在列空间 $\text{im } A$ 中找离 b 最近的向量 Ax . 因此“残差垂直于列空间”不是一个孤立公式, 而是最近点的几何必要条件.

命题 10.4 (正交投影). 设 (V, g) 是内积空间, W 是 V 的子空间. 对任意 $v \in V$, 存在唯一的 $w_0 \in W$ 使得

$$d(v, W) = d(v, w_0),$$

且 $v - w_0 \in W^\perp$. 若 $\{u_1, \dots, u_k\}$ 是 W 的一组标准正交基, 则

$$w_0 = \text{Proj}_W(v) = \sum_{i=1}^k g(v, u_i)u_i.$$

证明. 对任意 $w \in W$, 有

$$d(v, w)^2 = \|v - w\|^2 = \|v - w_0\|^2 + \|w_0 - w\|^2 \geq \|v - w_0\|^2,$$

其中第二个等号利用了 $v - w_0 \perp w_0 - w$ (因为 $w_0 - w \in W$ 而 $v - w_0 \in W^\perp$). 等号成立当且仅当 $w = w_0$. \square

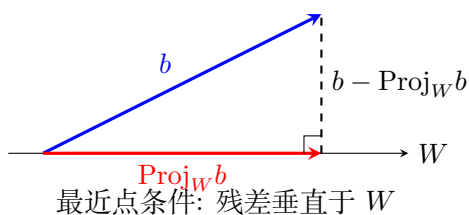


图 15: 正交投影给出子空间中的最佳近似.

定义 10.4. 映射 $\text{Proj}_W: V \rightarrow W, v \mapsto w_0$ 称为到 W 的**正交投影**(orthogonal projection). 它是一个线性变换, 且满足 $\text{Proj}_W \circ \text{Proj}_W = \text{Proj}_W$.

注 10.1. 正交投影 Proj_W 还满足**自伴随性**: 对任意 $u, v \in V$,

$$g(\text{Proj}_W(u), v) = g(u, \text{Proj}_W(v)).$$

这是因为 $u - \text{Proj}_W(u) \in W^\perp$, 故 $g(u, \text{Proj}_W(v)) = g(\text{Proj}_W(u), \text{Proj}_W(v)) = g(\text{Proj}_W(u), v)$. 自伴随算子的概念将在谱定理中起到核心作用.

注 10.2. 正交投影也可以推广到**仿射子空间** (affine subspace) 的情形: 设 $S = w_0 + W$ 是 V 中的一个仿射子空间, 则 v 到 S 的最近点为 $w_0 + \text{Proj}_W(v - w_0)$, 最小距离为 $\|v - w_0 - \text{Proj}_W(v - w_0)\|$.

10.2 Gram-Schmidt 正交化与 QR 分解

正交投影给出了计算向量到子空间最近点的方法. 自然的问题是: 如何从任意一组基出发, 构造标准正交基? Gram-Schmidt 正交化是解决这一问题的经典算法, 而 QR 分解则是它在矩阵语言中的表述.

设 (V, g) 是内积空间, (v_1, \dots, v_n) 是任意一组基, 我们可以通过如下的办法得到一组标准正交基 $\{w_1, \dots, w_n\}$:

$$\begin{aligned} w_1 &= \frac{v_1}{\|v_1\|} \\ w_2 &= \frac{v_2 - \langle v_2, w_1 \rangle w_1}{\|v_2 - \langle v_2, w_1 \rangle w_1\|} \\ w_3 &= \frac{v_3 - \langle v_3, w_1 \rangle w_1 - \langle v_3, w_2 \rangle w_2}{\|v_3 - \langle v_3, w_1 \rangle w_1 - \langle v_3, w_2 \rangle w_2\|} \\ &\vdots \\ w_n &= \frac{v_n - \sum_{i=1}^{n-1} \langle v_n, w_i \rangle w_i}{\|v_n - \sum_{i=1}^{n-1} \langle v_n, w_i \rangle w_i\|}. \end{aligned}$$

这个操作被称为格拉姆-施密特正交化 (Gram-Schmidt process).

定理 10.2 (QR 分解). 设 $A \in M_n(\mathbb{R})$ 是可逆矩阵, 则存在分解

$$A = QR,$$

其中 Q 是正交矩阵, R 是上三角矩阵. 如果还要求 R 对角线元 > 0 , 则这样的分解有唯一性.

证明. A 的列向量 v_1, v_2, \dots, v_n 构成 \mathbb{R}^n 的一组基. 对它们做 Gram-Schmidt 正交化, 得到标准正交基 q_1, \dots, q_n . 每个 v_j 都属于 $\text{span}(q_1, \dots, q_j)$, 因而

$$v_j = \sum_{i=1}^j r_{ij} q_i, \quad r_{jj} > 0.$$

令 $Q = (q_1, \dots, q_n)$, $R = (r_{ij})$, 则 Q 是正交矩阵, R 是对角线元素为正的上三角矩阵, 且 $A = QR$.

设这样的分解有两个

$$A = Q_1 R_1 = Q_2 R_2$$

则

$$Q_2^T Q_1 = R_2 R_1^{-1}.$$

由于上式中左侧是正交矩阵, 右侧是上三角矩阵且对角线均 > 0 . 上三角正交矩阵的列向量长度为 1 且彼此正交, 从最后一列向前看可知它必须是对角矩阵, 再由对角线为正得它只能是单位矩阵. 因此 $Q_1 = Q_2$, $R_1 = R_2$. \square

注 10.3. 也可以将 A 分解成正交矩阵乘以下三角矩阵, 上三角矩阵乘以正交矩阵, 下三角矩阵乘以正交矩阵, 证明类似.

10.3 正交变换与正交群

Gram-Schmidt 正交化和 QR 分解给出了标准正交基的构造方法. 自然的问题是: 什么样的线性变换保持标准正交基的结构不变? 换言之, 如果我们进行一次基变换, 变换前后的基都是标准正交基, 那么这个基变换矩阵必须满足什么条件? 答案就是**正交矩阵**, 即满足 $A^T A = I$ 的矩阵. 所有正交矩阵构成的集合称为**正交群**, 它对矩阵乘法封闭 (两个正交矩阵的乘积仍是正交矩阵) 且对取逆封闭 (正交矩阵的逆 $A^{-1} = A^T$ 也是正交矩阵).

定义 10.5. n 阶正交群(orthogonal group) 定义为

$$O_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid A^T A = I\}.$$

对于内积空间 (V, g) , 也记

$$O(V) := \{T \in \text{GL}(V) \mid g(T(u), T(v)) = g(u, v), \forall u, v \in V\}.$$

注 10.4. “群”这个名称来自抽象代数,指的是一个带有结合律运算、有单位元且每个元素可逆的集合. 在本书中,不需要系统学习群论,只需知道 $O_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ (可逆矩阵全体)的一个子集,且对乘法和求逆封闭即可. 类似地,前面出现的“辛群” $Sp_{2n}(\mathbb{F})$ 也是一类矩阵集合.

对于正交矩阵 A , 由 $A^T A = I$ 取行列式得 $(\det A)^2 = 1$, 即 $\det A = \pm 1$. 根据行列式的正负, 可以将正交矩阵分为两类.

定义 10.6. n 阶**特殊正交群**(*special orthogonal group*) 定义为

$$SO_n(\mathbb{R}) := \{A \in O_n(\mathbb{R}) \mid \det(A) = 1\}.$$

命题 10.5. 设 (V, g) 是内积空间, $T: V \rightarrow V$ 是线性变换. 则以下条件等价:

- (1) T 保持内积, 即 $g(T(u), T(v)) = g(u, v)$ 对所有 $u, v \in V$ 成立;
- (2) T 保持范数, 即 $\|T(v)\| = \|v\|$ 对所有 $v \in V$ 成立;
- (3) T 将标准正交基映为标准正交基;
- (4) T 在某组标准正交基下的矩阵是正交矩阵.

满足上述条件的 T 称为**正交变换**(*orthogonal transformation*) 或**等距变换**(*isometry*).

例 10.1. 通过直接计算 \mathbb{R}^2 中的正交基可知

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\} \sqcup \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}.$$

计算行列式可知

$$SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

恰好是 \mathbb{R}^2 中所有旋转构成的集合, 而 $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ (行列式为 -1 的那一类) 恰好是所有反射. 一个重要的观察是: 两个反射的复合是旋转, 即若反射轴的夹角为 $\frac{\theta}{2}$, 则两个反射的复合是旋转角 θ .

10.4 实对称矩阵的谱定理

正交变换提供了内积空间中“刚性”的基变换(保持距离和角度不变). 在对角化理论中, 一个自然的问题是: 什么样的矩阵可以用正交基变换来对角化? 答案是实对称矩阵——这就是谱定理. 谱定理是线性代数最深刻的定理之一, 它将代数(特征值)、几何(正交分解)和分析(二次型优化)三个方面统一起来.

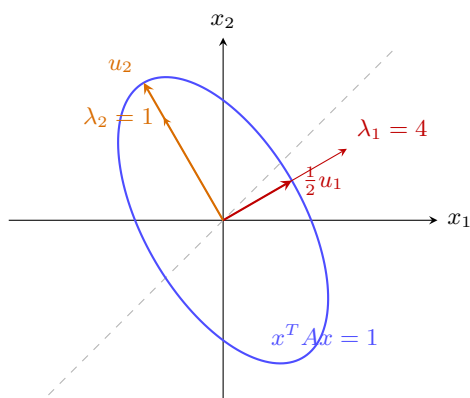
例 10.2 (二维谱定理的几何图解). 设

$$Q = \begin{pmatrix} \cos 30^\circ & -\sin 30^\circ \\ \sin 30^\circ & \cos 30^\circ \end{pmatrix}, \quad A = Q \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} Q^T.$$

矩阵 Q 只是把坐标轴旋转 30° , 所以 A 是一个实对称矩阵. 若令 $y = Q^T x$, 则

$$x^T A x = y^T \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} y = 4y_1^2 + y_2^2.$$

因此曲线 $x^T A x = 1$ 在旋转后的坐标 y_1, y_2 中就是椭圆 $4y_1^2 + y_2^2 = 1$. 它的两条主轴方向正是 A 的两个互相垂直的特征向量方向.



这个例子可以作为谱定理的图像版本来记: **实对称矩阵总能通过一次正交旋转, 把含有交叉项的二次型化成沿互相垂直方向的平方和.** 特征向量给出主轴方向, 特征值给出每个方向上的伸缩强弱.

定义 10.7.

- (1) 对 $A, B \in M_n(\mathbb{R})$, 如果存在 $Q \in O_n(\mathbb{R})$ 满足 $A = Q^T B Q = Q^{-1} B Q$, 则称 A, B **正交相似** (orthogonally similar).
- (2) 若 A 正交相似于一个对角阵, 则称 A (在 \mathbb{R} 上) **可正交对角化** (orthogonally diagonalizable).

在证明谱定理之前, 我们先建立一个关于实矩阵不变子空间的基本命题.

命题 10.6 (实矩阵的不变子空间). 设 V 是 \mathbb{R} 上的有限维线性空间, $f: V \rightarrow V$ 是线性变换. 则 f 有一个一维或二维的不变子空间.

证明. 设 $n = \dim V$, 取 V 的一组基将 f 表示为矩阵 $A \in M_n(\mathbb{R})$. 由代数学基本定理, A 在 \mathbb{C} 上有特征值 $\lambda = a + b\sqrt{-1} \in \mathbb{C}$ (其中 $a, b \in \mathbb{R}$), 设 $v = u + \sqrt{-1}w$ 是对应的特征向量 ($u, w \in \mathbb{R}^n$). 则

$$A(u + \sqrt{-1}w) = (a + b\sqrt{-1})(u + \sqrt{-1}w).$$

比较实部和虚部有

$$Au = au - bw, \quad Aw = bu + aw.$$

从而 $\text{span}_{\mathbb{R}}\{u, w\}$ 是 A 的不变子空间, 其维数为 1(当 $b = 0$ 时) 或 2(当 $b \neq 0$ 时). \square

注 10.5. 上述命题的证明表明: 实矩阵若有复特征值 $a \pm b\sqrt{-1}$ (其中 $b \neq 0$), 则对应一个二维不变子空间, f 在该子空间上的矩阵为

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

定理 10.3 (实对称矩阵的谱定理). 实对称矩阵可以正交对角化. 即对任意 $A \in M_n(\mathbb{R})$, $A = A^T$, 存在正交矩阵 $Q \in O_n(\mathbb{R})$ 使得 $Q^T A Q$ 为对角矩阵.

证明. 设 $A \in M_n(\mathbb{R})$, $A = A^T$, 我们对 n 归纳. 我们先证明 A 有一个实特征值. 设 $\lambda \in \mathbb{C}$ 为 A 的特征值, 设 $Av = \lambda v$, $v \in \mathbb{C}^n$, 则

$$\bar{v}^T Av = \lambda \bar{v}^T v$$

, 其中 $\bar{v}^T v > 0$. 由于

$$(\bar{v}^T Av)^T = \bar{v}^T Av,$$

从而有 $\lambda \in \mathbb{R}$. 由于 $A - \lambda I$ 是退化的实矩阵, 它的实零空间非零, 因而存在 $0 \neq u \in \mathbb{R}^n$ 满足 $Au = \lambda u$.

不妨取 $|u| = 1$, 并将 $u = v_1$ 扩充成 \mathbb{R}^n 的一个标准正交基, 记作

$$Q_1 = (v_1, v_2, \dots, v_n)$$

则

$$\begin{aligned} AQ_1 &= (Av_1, Av_2, \dots, Av_n) \\ &= (\lambda v_1, Av_2, \dots, Av_n) \\ &= (v_1 \cdots v_n) \begin{pmatrix} \lambda & * \\ 0 & * \end{pmatrix} \end{aligned}$$

从而有

$$A = Q_1 \begin{pmatrix} \lambda & * \\ * & * \end{pmatrix} Q_1^{-1} = Q_1 \begin{pmatrix} \lambda & * \\ * & * \end{pmatrix} Q_1^T$$

由于 A 是对称矩阵, 从而上述分解实际上形如

$$A = Q_1 \begin{pmatrix} \lambda & 0 \\ 0 & * \end{pmatrix} Q_1^{-1},$$

接下来对 n 做归纳即可. \square

自伴随算子与谱定理的内蕴证明

我们接下来给出谱定理的另一个证明, 该证明利用自伴随算子和不变子空间的分解, 揭示了谱定理更深层的结构.

定义 10.8. 给定线性空间 V 及对称双线性型 g . 如果线性映射 $f: V \rightarrow V$ 满足

$$g(f(v), w) = g(v, f(w))$$

对任意 $v, w \in V$ 成立, 则称 f 是**自伴随的** (*self-adjoint*).

引理 10.1. 设 V 是配备了对称双线性型 g 的线性空间, $f: V \rightarrow V$ 是自伴随线性映射. 若 $W \subset V$ 是 f 不变子空间, 则 W^\perp 也是 f 不变子空间.

现在假设 (V, g) 是内积空间, $f: V \rightarrow V$ 是自伴随线性映射, $B = \{e_1, \dots, e_n\}$ 为 V 一个标准正交基, 我们记 A 是 f 在 B 下的表示矩阵, 即

$$f(e_1, \dots, e_n) = (e_1, \dots, e_n)A$$

则由 $g(f(x), y) = g(x, f(y))$ 可知:

$$\begin{pmatrix} f(e_1) \\ \vdots \\ f(e_n) \end{pmatrix} \cdot_g (e_1, \dots, e_n) = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \cdot_g (f(e_1), \dots, f(e_n))$$

即

$$A^T \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \cdot_g (e_1, \dots, e_n) = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \cdot_g (e_1, \dots, e_n)A$$

由于 B 是标准正交基, 从而

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \cdot_g (e_1, \dots, e_n) = G_{g,B} = I_n,$$

从而 $A = A^T$.

注 10.6. 事实上, $f: V \rightarrow V$ 是自伴随当且仅当 f 关于某个标准正交基的矩阵是对称矩阵, 当且仅当 f 关于任意标准正交基的矩阵是对称矩阵.

谱定理的第二个证明. 对任意对称阵 $A \in M_n(\mathbb{R})$, 我们看其对应的一个自伴随算子 $f: V \rightarrow V$. 由命题 10.6, f 有一个一维或二维不变子空间 W_1 . 若 W_1 是二维的, 在其标准正交基下

$f|_{W_1}$ 的矩阵为对称矩阵 $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, 其判别式 $(a-c)^2 + 4b^2 \geq 0$, 故 $f|_{W_1}$ 有实特征值, 从而 W_1 中有 f 的特征向量. 因此我们总可以找到一维不变子空间. 由引理10.1可知 W_1^\perp 也是 f 不变的, 对 $\dim V$ 归纳, 得到正交分解

$$V = W_1 \perp W_2 \perp \cdots \perp W_n,$$

其中每个 W_i 是一维特征子空间.

取 $v_i \in W_i$, $|v_i| = 1$, 则 v_1, \cdots, v_n 为一个标准正交基, 且满足 $f(v_i) = \lambda_i v_i$. 而 $f(e_1, \cdots, e_n) = (e_1, \cdots, e_n)A$. 令 $(v_1, \cdots, v_n) = (e_1, \cdots, e_n)Q$, 其中 Q 正交, 从而

$$\begin{aligned} f(v_1, \cdots, v_n) &= f(e_1, \cdots, e_n)Q \\ &= (e_1, \cdots, e_n)AQ \\ &= (v_1, \cdots, v_n)Q^T AQ. \end{aligned}$$

即

$$Q^T AQ = \text{diag}\{\lambda_1, \dots, \lambda_n\}.$$

□

10.5 正交矩阵的分类

谱定理完整地分类了实对称矩阵 (自伴随变换). 接下来我们利用类似的思路——命题 10.6 中不变子空间的存在性——来研究正交矩阵 (正交变换) 的结构. 与对称矩阵不同, 正交矩阵的特征值可能不是实数, 因此不可约分块可以是二维的旋转.

给定内积空间 (V, g) 以及标准正交基 $B = (e_1, \cdots, e_n)$, 正交矩阵 A 对应正交变换 $f: V \rightarrow V$, 其中

$$f(e_1, \cdots, e_n) = (e_1, \cdots, e_n)A$$

若 $W \subset V$ 是不变子空间, 则 $f: W \cong W$, 并且由于 f 保内积可知 $f: W^\perp \cong W^\perp$. 由命题 10.6, f 有一维或二维不变子空间 W_1 . 归纳地, 可得正交分解 $V = W_1 \perp \cdots \perp W_k$, 其中每个 W_i 不可再分, 从而 $\dim_{\mathbb{R}} W_i$ 为 1 或 2. 若 $\dim W_i = 1$, 则 $f|_{W_i}$ 的特征值为 ± 1 (因为 f 保范数); 若 $\dim W_i = 2$, 则在 W_i 的标准正交基下 $f|_{W_i}$ 是二维正交变换.

定理 10.4 (正交矩阵的标准型). 假设 $A \in O_n(\mathbb{R})$, 则 A 正交相似于

$$\text{diag} \left\{ \begin{pmatrix} \cos \theta_1 & -\sin \theta_1 \\ \sin \theta_1 & \cos \theta_1 \end{pmatrix}, \begin{pmatrix} \cos \theta_2 & -\sin \theta_2 \\ \sin \theta_2 & \cos \theta_2 \end{pmatrix}, \dots, 1, \dots, -1, \dots \right\}.$$

等价地, 对 n 维内积空间 (V, g) 上的任意正交变换 T , 存在 V 的一组标准正交基使得 T 在该基下的矩阵是如上分块对角形式.

证明. 由命题 10.6, A 有一维或二维不变子空间 $W_1 \subset \mathbb{R}^n$. 若 $\dim W_1 = 1$, 则 W_1 由 A 的特征向量张成, 由于 A 正交, 特征值只能为 ± 1 . 若 $\dim W_1 = 2$, 则在 W_1 的标准正交基下, $A|_{W_1}$ 是 $O_2(\mathbb{R})$ 中的矩阵. 若 $A|_{W_1} \in SO_2(\mathbb{R})$, 则它形如

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

若 $A|_{W_1} \notin SO_2(\mathbb{R})$, 则它形如 $\begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$, 其特征多项式为 $\lambda^2 - 1$, 从而有特征值 ± 1 , 此时 W_1 可以进一步分解为两个一维不变子空间. 因此在所有情形中, 不可约块要么是一维的 (± 1), 要么是 $SO_2(\mathbb{R})$ 中的旋转矩阵. 由于 W_1^\perp 也是 A 不变的, 对 n 归纳即得. \square

例 10.3. 对于 $A \in SO_3(\mathbb{R})$, 其正交相似于

$$\begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

设

$$Q^T A Q = \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

以及 $Q = (v_1, v_2, v_3)$, 则

$$A(v_1, v_2, v_3) = (v_1, v_2, v_3) \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

所以 A 作用在 \mathbb{R}^3 上是 $\text{span}_{\mathbb{R}}\{v_1, v_2\}$ 平面中的一个旋转, 而 v_3 是旋转轴.

由此可以得到以下几何推论.

推论 10.1. 三维欧几里得空间中, 两个绕相交直线的旋转的复合仍是一个旋转.

证明. 设 $A, B \in SO_3(\mathbb{R})$, 则 $AB \in SO_3(\mathbb{R})$, 由上述分析 AB 正交相似于绕某轴的旋转. \square

推论 10.2. n 维欧几里得空间中, 两个关于超平面的反射的复合是一个旋转 (即属于 $SO_n(\mathbb{R})$).

定义 10.9 (反射). 给定内积空间 (V, g) , 以及 $0 \neq v \in V$, 关于 v 的反射 (reflection) 定义为

$$s_v: V \rightarrow V$$

$$x \mapsto x - \frac{2g(v, x)}{g(v, v)}v.$$

向量 v 称为反射的**法向量** (normal vector).

注 10.7.

(1) 若 s_v 是关于 v 的反射, 则 $s_v(v) = -v$, $s_v|_{H_v} = I$, 其中

$$H_v = v^\perp = \{x \in V \mid g(x, v) = 0\}$$

是 v 的正交补超平面. 反之, s_v 是相对于超平面 H_v 的镜面反射.

(2) 若 $\{v_1, \dots, v_n\}$ 是 V 的标准正交基, 则 s_{v_i} 关于此基的矩阵为

$$\text{diag}\{1, \dots, \underbrace{-1}_{\text{第 } i \text{ 位}}, \dots, 1\}.$$

(3) s_v 是正交变换, 且 $\det(s_v) = -1$, 从而 $s_v \in O(V) \setminus SO(V)$.

命题 10.7 (正交群的分类). 正交群 $O_n(\mathbb{R})$ 按行列式的符号恰好分成两类:

$$O_n(\mathbb{R}) = SO_n(\mathbb{R}) \sqcup s_v \cdot SO_n(\mathbb{R}),$$

其中 $SO_n(\mathbb{R})$ 是行列式为 1 的正交矩阵全体, $s_v \cdot SO_n(\mathbb{R})$ 是行列式为 -1 的正交矩阵全体 (s_v 是任意一个反射). 因此, 每个行列式为 -1 的正交矩阵都可以表示为一个反射与一个旋转 (行列式为 1 的正交变换) 的复合.

10.6 厄米特型和酉矩阵

定义 10.10. 给定有限维 \mathbb{C} -线性空间 V , $h: V \times V \rightarrow \mathbb{C}$ 叫作**厄米特型**(Hermitian form), 如果满足:

$$(1) h(\lambda_1 x_1 + \lambda_2 x_2, y) = \lambda_1 h(x_1, y) + \lambda_2 h(x_2, y);$$

$$(2) h(x, y) = \overline{h(y, x)}.$$

注 10.8. 条件 (2) 保证了所有的 $h(x, x)$ 都是实数.

例 10.4.

$$h: \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$$
$$(x, y) \mapsto \sum_{i=1}^n x_i \bar{y}_i$$

叫作 \mathbb{C}^n 上的标准厄米特型.

思考 10.1. 思考类似于实线性空间上对称双线性型和二次型, 该如何通过 $h(x, x)$ 得到 h ?

引理 10.2 (厄米特极化恒等式). 对于厄米特型 $h: V \times V \rightarrow \mathbb{C}$, 有

$$\begin{aligned}\operatorname{Re} h(x, y) &= \frac{1}{2}(h(x+y, x+y) - h(x, x) - h(y, y)) \\ \operatorname{Im} h(x, y) &= \frac{1}{2}(h(x + \sqrt{-1}y, x + \sqrt{-1}y) - h(x, x) - h(y, y)).\end{aligned}$$

并且 $\operatorname{Re} h$ 对称, $\operatorname{Im} h$ 反对称.

证明. 直接展开 $h(x+y, x+y)$ 有

$$h(x+y, x+y) = h(x, x) + h(x, y) + h(y, x) + h(y, y) = h(x, x) + h(y, y) + 2\operatorname{Re} h(x, y),$$

其中最后一步用了 $h(y, x) = \overline{h(x, y)}$, 从而 $h(x, y) + h(y, x) = 2\operatorname{Re} h(x, y)$. 类似地,

$$h(x + \sqrt{-1}y, x + \sqrt{-1}y) = h(x, x) + h(y, y) + \sqrt{-1}h(y, x) - \sqrt{-1}h(x, y) = h(x, x) + h(y, y) + 2\operatorname{Im} h(x, y).$$

对称性和反对称性由 $\operatorname{Re} h(x, y) = \operatorname{Re} h(y, x)$ 以及 $\operatorname{Im} h(x, y) = -\operatorname{Im} h(y, x)$ 直接得出. \square

给定厄米特型 $h: V \times V \rightarrow \mathbb{C}$, 取基 $\alpha_1, \dots, \alpha_n$, 则格拉姆矩阵 $(h(\alpha_i, \alpha_j)) = H$ 满足 $H = \overline{H}^T$, 这样的 H 叫作厄米特阵. 为了方便, 我们之后记 $H^* = \overline{H}^T$. 对于厄米特阵 H , 同样有 $\operatorname{Re} H$ 是对称的, $\operatorname{Im} H$ 是反对称的.

定义 10.11. $A, B \in M^n(\mathbb{C})$, 若存在 $P \in \operatorname{GL}_n(\mathbb{C})$, 满足 $PAP^* = B$, 则称 A, B 共轭相合.

现给厄米特型 $h: V \times V \rightarrow \mathbb{C}$, 以及两组基 $(\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n)$ 满足 $\{\beta_1, \dots, \beta_n\} = (\alpha_1, \dots, \alpha_n)P$, 则

$$\begin{aligned}(h(\beta_i, \beta_j))^* &= \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \\ &= P^T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \cdot (\alpha_1, \dots, \alpha_n)P \\ &= P^T (h(\alpha_i, \alpha_j)) \overline{P}\end{aligned}$$

所以同一个厄米特型在不同基下的格拉姆矩阵是共轭相合的.

定理 10.5. 厄米特方阵共轭相合于对角阵, 且对角线元素必为实数.

定义 10.12. \mathbb{C} -线性空间 V 上的厄米特型 h 称为:

- 正定的 ($h > 0$), 如果对所有 $v \neq 0$ 有 $h(v, v) > 0$;
- 半正定的 ($h \geq 0$), 如果对所有 v 有 $h(v, v) \geq 0$;

- 负定的 ($h < 0$), 如果对所有 $v \neq 0$ 有 $h(v, v) < 0$;
- 半负定的 ($h \leq 0$), 如果对所有 v 有 $h(v, v) \leq 0$.

定理 10.6. 对于厄米特阵 H , 则以下等价:

- (1) H 正定;
- (2) H 共轭相合于单位阵;
- (3) $H = PP^*$, 其中 $P \in GL_n(\mathbb{C})$;
- (4) H 的顺序主子式均大于零;
- (5) H 的所有主子式大于零.

定理 10.7. 对于厄米特阵 H , 则以下等价:

- (1) H 半正定;
- (2) H 共轭相合于

$$\begin{pmatrix} I_r & O \\ O & O \end{pmatrix};$$

- (3) $H = PP^*$, 其中 $P \in M_n(\mathbb{C})$;
- (4) H 的所有主子式大于等于零.

定义 10.13. 给定有限维 \mathbb{C} -线性空间 V 以及厄米特型 $h: V \times V \rightarrow \mathbb{C}$, 如果 $h > 0$, 则称 (V, h) 是一个厄米特内积空间, 也叫酉空间 (unitary space).

注 10.9 (复内积的阅读规则). 复内积与实内积的主要差别只有一个: 需要在一个变量上取共轭. 本书采用的约定是

$$\langle ax_1 + bx_2, y \rangle = a\langle x_1, y \rangle + b\langle x_2, y \rangle, \quad \langle x, ay_1 + by_2 \rangle = \bar{a}\langle x, y_1 \rangle + \bar{b}\langle x, y_2 \rangle.$$

也就是说, 它关于第一个变量线性, 关于第二个变量共轭线性. 若读到采用相反约定的教材, 只需把证明中的共轭位置相应交换即可. 初读时可以先记住三件事:

- (1) $\langle x, x \rangle$ 仍然是非负实数, 因而 $|x| = \sqrt{\langle x, x \rangle}$ 仍表示长度;
- (2) 转置在复数情形中要换成共轭转置 $A^* = \overline{A}^T$;
- (3) “正交矩阵/正交基/正交相似”在复数情形中对应为“酉矩阵/标准正交基/酉相似”.

为了方便起见, 我们记 $\langle x, y \rangle := h(x, y)$.

(1) 长度: $x \in V, |x| := \sqrt{\langle x, x \rangle}$.

(2) 角度: $x, y \in V \setminus \{0\}$, 存在 $\theta(x, y) \in [0, \frac{\pi}{2}]$ 使得

$$\cos(\theta(x, y)) = \frac{|\langle x, y \rangle|}{|x||y|}.$$

引理 10.3 (Cauchy-Schwarz 不等式).

$$|\langle x, y \rangle| \leq |x||y|.$$

等价地,

$$|\langle x, y \rangle|^2 \leq \langle x, x \rangle \langle y, y \rangle.$$

证明. 若 $y = 0$, 结论显然. 下设 $y \neq 0$. 令

$$\lambda = \frac{\langle x, y \rangle}{\langle y, y \rangle}.$$

由于内积关于第一个变量线性、第二个变量共轭线性, 有

$$\begin{aligned} 0 &\leq \langle x - \lambda y, x - \lambda y \rangle \\ &= |x|^2 - \bar{\lambda} \langle x, y \rangle - \lambda \langle y, x \rangle + |\lambda|^2 |y|^2 \\ &= |x|^2 - \frac{|\langle x, y \rangle|^2}{|y|^2}. \end{aligned}$$

因此 $|\langle x, y \rangle|^2 \leq |x|^2 |y|^2$, 即 $|\langle x, y \rangle| \leq |x||y|$. 等号成立当且仅当 $x - \lambda y = 0$, 也就是 x, y 在 \mathbb{C} 上线性相关. \square

引理 10.4 (三角不等式). $\forall x, y \in V, |x + y| \leq |x| + |y|$.

证明. 根据定义有

$$|x + y|^2 = |x|^2 + \langle x, y \rangle + \langle y, x \rangle + |y|^2.$$

根据 Cauchy-Schwarz 不等式有

$$|\langle x, y \rangle| \leq |x||y|, \quad |\langle y, x \rangle| \leq |x||y|,$$

从而

$$|x + y|^2 \leq |x|^2 + 2|x||y| + |y|^2 = (|x| + |y|)^2.$$

\square

引理 10.5 (平行四边形等式). $\forall x, y \in V$, 有

$$|x + y|^2 + |x - y|^2 = 2(|x|^2 + |y|^2).$$

定义 10.14. 给定酉空间 (V, h) , 基 $\{\alpha_1, \dots, \alpha_n\}$ 被称为标准正交基, 如果 $\langle \alpha_i, \alpha_j \rangle = \delta_{ij}$.

注 10.10. 和内积空间的情况相同, 从任何一组基出发, 可以通过 *Gram-Schmidt* 正交化得到标准正交基.

定理 10.8. 给定酉空间 (V, h) , 以及标准正交基 $\{\alpha_1, \dots, \alpha_n\}$ 和 $\{\beta_1, \dots, \beta_n\}$, 假设 $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)P$, 则

$$PP^* = I_n.$$

定义 10.15. 矩阵 $P \in M_n(\mathbb{C})$ 被称为酉矩阵 (*unitary matrix*), 如果 $PP^* = I_n$.

引理 10.6. 若 $P \in M_n(\mathbb{C})$ 是酉矩阵, 则 \bar{P}, P^{-1}, P^* 均为酉矩阵.

定义 10.16. 两个复方阵 $A, B \in M_n(\mathbb{C})$ 称为酉相似的, 如果存在酉阵 $U \in M_n(\mathbb{C})$ 使得 $A = U^*BU$.

命题 10.8. 任一复方阵酉相似于上三角阵.

证明. 数学归纳法. 设 $A \in M_n(\mathbb{C})$, 对 n 归纳.

设 λ 为 A 的一个特征值, $v \in \mathbb{C}^n$ 为一个 λ -特征向量, 不妨 $\|v\| = 1$, 扩充 v 为 \mathbb{C}^n 的一个标准正交基 v_1, \dots, v_n , 令 $U = (v_1 \cdots v_n)$ 为酉阵, 则

$$AU = (Av_1 \cdots Av_n) = (v_1 \cdots v_n) \begin{pmatrix} \lambda & * \\ 0 & * \end{pmatrix}$$

$$\text{即 } U^*AU = \begin{pmatrix} \lambda & * \\ 0 & * \end{pmatrix}.$$

归纳即可. □

定义 10.17. 一个方阵 $N \in M_n(\mathbb{C})$ 叫正规的 (*normal*), 若 $NN^* = N^*N$.

引理 10.7. 若正规矩阵 N 酉相似于 $\begin{pmatrix} N_1 & N_2 \\ 0 & N_3 \end{pmatrix}$, N_1, N_3 为方阵, 则必有 $N_2 = 0$, 且 N_1 和 N_3 为正规的.

证明. 设 $\begin{pmatrix} N_1 & N_2 \\ 0 & N_3 \end{pmatrix} = U^*NU$, U 酉阵, 即 U^*NU 与 $(U^*NU)^* = U^*N^*U$ 可交换, 从而 U^*NU 也是正规的. 所以

$$\begin{pmatrix} N_1 & N_2 \\ 0 & N_3 \end{pmatrix} \begin{pmatrix} N_1^* & 0 \\ N_2^* & N_3^* \end{pmatrix} = \begin{pmatrix} N_1^* & 0 \\ N_2^* & N_3^* \end{pmatrix} \begin{pmatrix} N_1 & N_2 \\ 0 & N_3 \end{pmatrix}$$

比较 (1,1) 分块: 左边为 $N_1N_1^* + N_2N_2^*$, 右边为 $N_1^*N_1$. 两边取迹有

$$\text{tr}(N_1N_1^*) + \text{tr}(N_2N_2^*) = \text{tr}(N_1^*N_1).$$

由于 $\operatorname{tr}(N_1 N_1^*) = \operatorname{tr}(N_1^* N_1)$ (迹的循环性), 故 $\operatorname{tr}(N_2 N_2^*) = 0$, 而 $\operatorname{tr}(N_2 N_2^*) = \sum_{i,j} |n_{ij}|^2 \geq 0$, 故 $N_2 = 0$. 此时 $N_1 N_1^* = N_1^* N_1$, $N_3 N_3^* = N_3^* N_3$, 即 N_1, N_3 均为正规矩阵. \square

定理 10.9 (正规矩阵谱定理). 正规矩阵可酉相似于对角阵.

证明. 设 $A \in M_n(\mathbb{C})$ 正规, 则 A 酉相似于上三角阵

$$\begin{pmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & * \end{pmatrix}$$

由引理 10.7 可知其必为对角阵. \square

例 10.5. 实对称、实反对称、正交阵、厄米特阵、酉阵、斜厄米特阵都是正规矩阵.

推论 10.3.

1. 厄米特阵 (包含了实对称阵) 必酉相似于 $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, λ_i 为实数.
2. 酉阵 (包含正交阵) 必酉相似于 $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, $\lambda_i = e^{\sqrt{-1}\theta_i}$, $\theta_i \in \mathbb{R}$.
3. 斜厄米特阵 (包含反对称阵) 必酉相似于 $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, $\lambda_i = \sqrt{-1}g_i$, $g_i \in \mathbb{R}$.

证明.

1. 设厄米特阵酉相似于 $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, 则该对角阵也为厄米特 $\Rightarrow \lambda_i$ 为实.
2. 设酉阵酉相似于对角阵 $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$, 而相似保酉性 \Rightarrow 每个 λ_i 模长 = 1.
3. 类似.

\square

定义 10.18. 设 $(V, \langle \cdot, \cdot \rangle)$ 为一个 n 维酉空间 (即 $\langle \cdot, \cdot \rangle$ 的一个 Gram 阵是正定厄米特阵). 一个线性变换 $\varphi: V \rightarrow V$ 叫正规变换, 厄米特变换, 酉变换, 或斜厄米特变换, 若 φ 在 V 的一个标准正交基下表示矩阵为相应类型矩阵.

用线性变换观点重述谱定理:

引理 10.8. 酉空间 V 的正规变换 φ 的不变子空间 W 的正交补 W^\perp 也为不变子空间.

定理 10.10 (谱定理, 线性变换形式). 设 V 为 n 维酉空间, $\varphi: V \rightarrow V$ 正规变换. 则存在 V 的标准正交基 v_1, \dots, v_n 使得每一个 v_i 都是 φ 的特征向量. 记 $\lambda_1, \dots, \lambda_k$ 为 φ 的不同特征值, W_i 为 φ 的 λ_i -特征空间, 则

$$\varphi = \lambda_1 \pi_1 + \cdots + \lambda_k \pi_k,$$

其中 $\pi_i: V \rightarrow W_i$ 为正交投影, 称为 φ 的谱分解 (spectral decomposition).

推论 10.4 (矩阵的谱分解). 设 A 是 $n \times n$ 实对称矩阵, 特征值为 $\lambda_1, \dots, \lambda_k$ (两两不同), 对应的特征空间为 W_1, \dots, W_k . 设 P_i 是到 W_i 的正交投影矩阵, 则

$$A = \lambda_1 P_1 + \lambda_2 P_2 + \dots + \lambda_k P_k,$$

其中 $P_i^2 = P_i = P_i^T$, $P_i P_j = 0 (i \neq j)$, $\sum_{i=1}^k P_i = I_n$. 更一般地, 对任意多项式 f , 有 $f(A) = f(\lambda_1)P_1 + \dots + f(\lambda_k)P_k$.

定理 10.11 (伴随算子). 给定 n 维酉空间 V 以及线性变换 $\varphi: V \rightarrow V$, 则存在唯一线性变换 $\varphi^*: V \rightarrow V$, 使得任取 $\alpha, \beta \in V$ 成立

$$\langle \varphi^*(\alpha), \beta \rangle = \langle \alpha, \varphi(\beta) \rangle.$$

称 φ^* 为 φ 的伴随(adjoint). 设 φ, φ^* 在 V 的一个标准正交基下表示矩阵为 A, B , 则 $B = A^* = \overline{A}^T$.

证明. 假设 $\langle \varphi^*(\alpha), \beta \rangle = \langle \alpha, \varphi(\beta) \rangle, \forall \alpha, \beta$. 取一个标准正交基 v_1, \dots, v_n , 则:

$$\begin{pmatrix} \varphi^*(v_1) \\ \vdots \\ \varphi^*(v_n) \end{pmatrix} = B \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad (\varphi(v_1), \dots, \varphi(v_n)) = (v_1, \dots, v_n)A$$

左边内积矩阵 $= B^T \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (v_1, \dots, v_n) = B^T$, 右边内积矩阵 $= \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \cdot (v_1, \dots, v_n) \overline{A} = \overline{A}$, 所以 $B^T = \overline{A} \Rightarrow B = A^*$.

反之, 为构造 φ^* , 只需取一个标准正交基, 设 φ 的矩阵为 A , 然后用 A^* 去得到 φ^* . \square

定理 10.12 (酉等价的等价条件). V_1, V_2 均为 n 维酉空间, $\gamma: V_1 \rightarrow V_2$ 是线性映射, 则以下等价:

1. γ 保内积;
2. γ 保向量长度 (保距);
3. $\gamma: V_1 \rightarrow V_2$ 为线性同构, 且保内积;
4. γ 把任意 V_1 的标准正交基映为 V_2 的标准正交基;
5. γ 把某一标准正交基映为标准正交基;
6. γ 在 V_1 和 V_2 的标准正交基下的方阵表式为酉方阵.

注 10.11. 一维酉群 $U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$ (在乘法下构成群) 与 $SO_2(\mathbb{R})$ 之间有典范同构:

$$U(1) \xrightarrow{\sim} SO_2(\mathbb{R}), \quad e^{\sqrt{-1}\theta} \mapsto \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

更一般地, 特殊酉群 $SU(2) = \{U \in M_2(\mathbb{C}) \mid UU^* = I, \det U = 1\}$ 可以参数化为

$$SU(2) = \left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

作为实流形, $SU(2)$ 同胚于三维球面 $S^3 \subset \mathbb{R}^4$. $SU(2)$ 与三维旋转群 $SO_3(\mathbb{R})$ 之间存在二重覆盖映射 $SU(2) \rightarrow SO_3(\mathbb{R})$, 核为 $\{\pm I\}$. 这一关系在物理学中对应于自旋的概念, 在数学中联系着四元数代数.

10.7 应用: 二次曲线与二次曲面

谱定理的一个经典应用是对实二次曲线和二次曲面的分类. 基本思路是: 通过正交变换消去交叉项, 然后通过配方化为标准形式.

定义 10.19. \mathbb{R}^2 中的二次曲线 (conic) 是满足如下二次方程的点 (x_1, x_2) 的轨迹:

$$Ax_1^2 + Bx_1x_2 + Cx_2^2 + Dx_1 + Ex_2 + F = 0,$$

其中 $A, B, C, D, E, F \in \mathbb{R}$ 且 A, B, C 不全为零.

定理 10.13 (二次曲线的分类). \mathbb{R}^2 中的任意非退化二次曲线 (不退化为直线、两条直线、点或空集) 经过刚性运动 (即正交变换加平移) 可化为如下标准形式之一:

(1) **椭圆**: $\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = 1$, 其中 $a, b > 0$;

(2) **双曲线**: $\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 1$, 其中 $a, b > 0$;

(3) **抛物线**: $x_2^2 = 2px_1$, 其中 $p > 0$.

证明. 二次部分 $Ax_1^2 + Bx_1x_2 + Cx_2^2$ 定义了 \mathbb{R}^2 上的对称双线性型, 其格拉姆矩阵为

$$M = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}.$$

由实对称矩阵的谱定理, 存在正交矩阵 $P \in O_2(\mathbb{R})$ 使得

$$P^T M P = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix},$$

其中 λ_1, λ_2 是 M 的特征值. 作正交变换 $\mathbf{x} = P\mathbf{y}$ 后, 二次曲线方程变为

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + D' y_1 + E' y_2 + F = 0.$$

接下来分情况讨论:

1. 若 λ_1, λ_2 同号, 配方后得到椭圆的标准形式;
2. 若 λ_1, λ_2 异号, 配方后得到双曲线的标准形式;
3. 若 λ_1, λ_2 中有一个为零, 且零方向上的一次项非零, 配方后得到抛物线的标准形式.

若零方向上的一次项也为零, 则方程会退化为空集、直线或两条平行直线等情形, 不属于本定理列出的非退化二次曲线. \square

例 10.6. 考虑方程 $5x_1^2 + 4x_1x_2 + 2x_2^2 = 1$. 对应的格拉姆矩阵为 $M = \begin{pmatrix} 5 & 2 \\ 2 & 2 \end{pmatrix}$, 特征值为 $\lambda_1 = 6, \lambda_2 = 1$. 经正交变换后方程化为 $6y_1^2 + y_2^2 = 1$, 即椭圆 $\frac{y_1^2}{1/6} + \frac{y_2^2}{1} = 1$.

上述分类可以推广到三维:

定义 10.20. \mathbb{R}^n 中的二次曲面 (quadric) 是满足如下二次方程的点的轨迹:

$$\sum_{i=1}^n \sum_{j=1}^n a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c = 0,$$

其中 $a_{ij}, b_i, c \in \mathbb{R}$ 且 (a_{ij}) 不全为零.

定理 10.14 (三维二次曲面的分类). \mathbb{R}^3 中的非退化二次曲面经过刚性运动可化为如下标准形式之一:

- (1) 椭球面: $\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} + \frac{x_3^2}{c^2} = 1$;
- (2) 单叶双曲面: $\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} - \frac{x_3^2}{c^2} = 1$;
- (3) 双叶双曲面: $-\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} + \frac{x_3^2}{c^2} = 1$;
- (4) 椭圆抛物面: $\frac{x_1^2}{a^2} + \frac{x_2^2}{b^2} = 2px_3$;
- (5) 双曲抛物面 (马鞍面): $\frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 2px_3$.

其中 $a, b, c, p > 0$.

证明. 设二次方程的二次部分的格拉姆矩阵为 $A \in M_3(\mathbb{R})$, $A = A^T$. 由谱定理 (定理10.3), 存在正交矩阵 P 使得 $P^T A P = \text{diag}(\lambda_1, \lambda_2, \lambda_3)$. 作正交变换 $\mathbf{x} = P\mathbf{y}$ 后, 方程变为

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + \lambda_3 y_3^2 + D'y_1 + E'y_2 + F'y_3 + G = 0.$$

若二次部分非退化, 即 $\lambda_i \neq 0$ 对所有 i 成立, 分情况讨论:

1. 若三个特征值同号 (不妨设均为正), 对每个 y_i 配方得 $\lambda_i(y_i + \frac{D'_i}{2\lambda_i})^2$, 作平移后化为椭球面;

2. 若两正一负, 类似配方后化为单叶双曲面;
3. 若一正两负, 化为双叶双曲面.

当二次部分秩为 2 时, 对应零特征值方向上的一次项若非零, 配方后得到抛物面型; 根据两个非零特征值的符号相同或相反, 分别得到椭圆抛物面或双曲抛物面. 若零方向上的一次项为零, 或二次部分秩更低, 则会出现柱面、锥面、平面等退化或半退化情形, 这里不列入主分类. \square

10.8 习题

10.8.1 练习题

习题 10.1 (Gram-Schmidt 正交化). 在 \mathbb{R}^3 的标准内积下, 对向量组

$$v_1 = (1, 1, 0)^T, \quad v_2 = (1, 0, 1)^T, \quad v_3 = (0, 1, 1)^T$$

做 Gram-Schmidt 正交化.

1. 求一组正交基 u_1, u_2, u_3 .
2. 将其归一化得到一组标准正交基.
3. 把过程解释为不断减去“已经确定方向上的投影”.

习题 10.2 (正交投影与最小二乘). 用直线 $y = ax + b$ 拟合三个点 $(0, 1), (1, 2), (2, 2)$.

1. 写出矩阵方程 $Ax \approx b$.
2. 写出正规方程 $A^T Ax = A^T b$.
3. 求最小二乘解.
4. 说明残差向量为什么垂直于 A 的列空间.

习题 10.3. 设 A 是 n 阶实对称矩阵, $v \in \mathbb{R}^n$. 证明:

$$|Av| \leq \max\{|\lambda_1|, |\lambda_2|, \dots, |\lambda_n|\} \cdot |v|,$$

其中 $\lambda_1, \dots, \lambda_n$ 是 A 的全部特征值.

习题 10.4 (Courant-Fischer 极大极小原理). 设 (V, g) 是 n 维内积空间, $T: V \rightarrow V$ 是自伴随变换, 特征值为 $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$. 证明:

$$\lambda_k = \min_{\substack{W \subset V \\ \dim W = k-1}} \max_{\substack{x \perp W \\ |x|=1}} g(T(x), x).$$

习题 10.5 (Cauchy 交错定理). 设 A 是 n 阶实对称矩阵, B 是 A 的 m 阶主子矩阵 ($m < n$). 设 A 的特征值为 $\lambda_1 \geq \cdots \geq \lambda_n$, B 的特征值为 $\mu_1 \geq \cdots \geq \mu_m$, 证明对所有 $1 \leq i \leq m$, 有

$$\lambda_i \geq \mu_i \geq \lambda_{i+n-m}.$$

(提示: 利用 Courant-Fischer 极大极小原理.)

习题 10.6 (Sylvester 判据的谱方法证明). 利用 Cauchy 交错定理证明 Sylvester 判据: 实对称矩阵正定当且仅当其所有顺序主子式均为正.

习题 10.7. 证明任意实反对称矩阵 $A \in M_n(\mathbb{R})$ 可以正交相似于分块对角阵, 分块形如

$$\begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix},$$

当 n 为奇数时可能有一个零块. 并利用此结果证明: 任意实反对称矩阵合同于分块对角阵, 分块形如 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 和零块.

习题 10.8. 设 V 是所有 n 阶实反对称矩阵构成的线性空间.

(1) 对任意 $A \in V$, 证明 $I+A$ 可逆.

(2) 对任意 $A \in V$, 定义 $f(A) = (I-A)(I+A)^{-1}$, 证明 $f(A)$ 是正交矩阵.

(3) 刻画 $f: V \rightarrow O_n(\mathbb{R})$ 的像: 哪些正交矩阵可以写成 $(I-A)(I+A)^{-1}$ 的形式? (提示: 用特征值刻画.)

习题 10.9. 考虑群 $O_2(\mathbb{R})$, 其子群 $SO_2(\mathbb{R})$, 以及群 $SO_3(\mathbb{R})$. 判断以下命题是否正确, 正确则证明, 错误则给出反例:

(1) $O_2(\mathbb{R})$ 中两个元素共轭当且仅当它们有相同的迹.

(2) $SO_2(\mathbb{R})$ 中两个元素在 $SO_2(\mathbb{R})$ 中共轭当且仅当它们有相同的迹.

(3) $SO_2(\mathbb{R})$ 中两个元素在 $O_2(\mathbb{R})$ 中共轭当且仅当它们有相同的迹.

(4) $SO_3(\mathbb{R})$ 中两个元素共轭当且仅当它们有相同的迹.

习题 10.10 (Cartan-Dieudonné 定理). 证明欧几里得空间 (V, g) 的任意正交变换可以表示为不超过 $\dim V$ 个反射的复合.

习题 10.11 (循环矩阵). 证明如下循环矩阵是正规矩阵:

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix}.$$

(提示: 将 C 写成移位矩阵的多项式, 然后对角化移位矩阵.)

习题 10.12. 证明: 酉矩阵的任意方子矩阵的复特征值的模不超过 1.

习题 10.13. (1) 若 A 和 B 是正规矩阵, AB 是否一定正规? 若额外假设 $AB = BA$ 呢?

(2) 判断矩阵 $A = \begin{pmatrix} \sqrt{-1} & -\sqrt{-1} \\ -\sqrt{-1} & \sqrt{-1} \end{pmatrix}$ 是否为正规矩阵、厄米特矩阵或酉矩阵.

习题 10.14. 设 $X = A + \sqrt{-1}B$ 是复方阵, 其中 $A, B \in M_n(\mathbb{R})$. 证明 X 是酉矩阵当且仅当

$$\begin{pmatrix} A & -B \\ B & A \end{pmatrix}$$

是正交矩阵.

习题 10.15. 设 $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ 是 2×2 实对称矩阵. 用 a, b, c 写出将 A 正交对角化的正交矩阵 Q .

习题 10.16. 在 \mathbb{R}^3 中计算

$$(1, 2, 2) \cdot (2, -1, 3)$$

以及向量 $(1, 2, 2)$ 的长度.

习题 10.17. 判断向量 $(1, 1, 0)$ 与 $(1, -1, 2)$ 是否正交.

习题 10.18. 求向量 $v = (3, 4)$ 在方向 $u = (1, 1)$ 上的投影.

习题 10.19. 对向量组

$$(1, 1, 0), \quad (1, 0, 1)$$

进行 *Gram-Schmidt* 正交化.

习题 10.20. 求平面

$$x + y + z = 0$$

的一个单位法向量.

习题 10.21. 设

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

求一组正交的特征向量, 并把它们单位化.

习题 10.22. 用最小二乘思想, 为点 $(0, 1)$ 、 $(1, 2)$ 、 $(2, 2)$ 拟合直线 $y = ax + b$. 写出正规方程即可.

10.8.2 思考题

习题 10.23 ($\text{SO}(n, \mathbb{R})$ 的外自同构). 群 G 的一个自同构称为**内自同构**, 如果它形如 $g \mapsto hgh^{-1}$ (对某个固定的 $h \in G$). 不是内自同构的自同构称为**外自同构**. 考虑 $\text{SO}(n, \mathbb{R})$ 的自同构 $\varphi: A \mapsto PAP^{-1}$, 其中 $P \in \text{O}(n, \mathbb{R})$ 且 $\det P = -1$. 问: φ 是内自同构还是外自同构? 证明你的结论. (答案可能依赖于 n .)

习题 10.24 (Lorentz 变换的标准型). 设 e_1, e_2, e_3, e_4 是 \mathbb{R}^4 的标准基, 考虑对称双线性型 $\langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4$. **Lorentz 变换** T 是指满足 $\langle Tx, Ty \rangle = \langle x, y \rangle$ 的线性变换. 证明: 存在标准正交基 (即满足 $\langle f_i, f_j \rangle = \epsilon_i \delta_{ij}$, 其中 $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1, \epsilon_4 = -1$) 使得 T 的矩阵为分块对角形, 每个分块为以下形式之一:

(1) 1×1 块, 值为 ± 1 ;

(2) 2×2 旋转块 $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$;

(3) 2×2 双曲块 $\pm \begin{pmatrix} \cosh \theta & \sinh \theta \\ \sinh \theta & \cosh \theta \end{pmatrix}$;

(4) 3×3 块, 特征值 $\lambda = \pm 1$, 满足 $(T - \lambda I)^3 = 0$ 但 $(T - \lambda I)^2 \neq 0$.

习题 10.25 (Lang 代数学第 XV 章). 设 E 是 \mathbb{C} 上的有限维线性空间.

(1) 设 $h: E \times E \rightarrow \mathbb{C}$ 是厄米特型, 将 $h(x, y) = g(x, y) + \sqrt{-1}f(x, y)$ 分解为实部和虚部. 证明 g, f 都是 \mathbb{R} -双线性的, g 是对称的, f 是反对称的.

(2) 设 $g: E \times E \rightarrow \mathbb{C}$ 是 \mathbb{R} -双线性的, 且对任意 $x \in E$, 映射 $y \mapsto g(x, y)$ 是 \mathbb{C} -线性的. 又假设 $f(x, y) = g(x, y) - g(y, x)$ 在 $E \times E$ 上取实值. 证明存在唯一的厄米特型 h 和唯一的 \mathbb{C} -双线性对称型 ψ 使得 $2\sqrt{-1}g = h + \psi$.

习题 10.26 (辛变换的标准型). 设 (V, ω) 是 \mathbb{C} 上的辛空间 (即 ω 是非退化反对称双线性型). 线性变换 T 称为**辛变换**, 如果 $\omega(T(v), T(w)) = \omega(v, w)$. 证明: 对 \mathbb{C} 上的辛变换 T , 存在辛基使得 T 的矩阵形如

$$\begin{pmatrix} B_n & 0_n \\ 0_n & B_n^T \end{pmatrix},$$

其中 B_n 是 n 维若尔当标准型.

习题 10.27. 设 A 是 n 阶实方阵, $A^T A$ 的特征值为 $\lambda_1^2, \dots, \lambda_n^2$, 其中 $0 \leq \lambda_i \leq 1 (i = 1, \dots, n)$. 证明:

$$\det(I_n - A) \geq (1 - \lambda_1)(1 - \lambda_2) \cdots (1 - \lambda_n).$$

习题 10.28. 求 \mathbb{R}^4 (配标准内积) 中, 下列向量组生成的子空间 W 的正交补 W^\perp 的一组基.

(1) $\{(1, 0, 2, 1), (2, 1, 2, 3), (0, 1, -2, 1)\}$;

(2) $\{(1, 1, 1, 1), (-1, 1, -1, 1), (2, 0, 2, 0)\}$.

习题 10.29. 记 $R_n = \mathbb{R}[x]_{\leq n}$ 为全体次数不超过 n 的多项式构成的线性空间, 其上配有内积

$$(f, g) = \int_{-1}^1 f(x)g(x)dx.$$

(1) 称形如 $P_0(x) = 1, P_k(x) = \frac{1}{2^k k!} \frac{d^k}{dx^k} [(x^2 - 1)^k], k = 1, 2, \dots, n$ 的多项式为 Legendre 多项式. 证明 P_0, P_1, \dots, P_n 构成 R_n 的一组正交基.

(2) 设 f 是次数为 n 的首一多项式, 求 f 长度 (即 $\sqrt{(f, f)}$) 的最小值.

习题 10.30. 设实对称矩阵 $S = \begin{bmatrix} 0 & A \\ A^T & 0 \end{bmatrix}$. 证明

(1) $Sx = \lambda x$ 当且仅当 $x = \begin{bmatrix} y \\ z \end{bmatrix}$, 满足 $Az = \lambda y, A^T y = \lambda z$.

(2) 如果 λ 是 S 的特征值, 则 $-\lambda$ 也是 S 的特征值.

(3) 如果 $\lambda \neq 0$ 是 S 的特征值, 则 λ^2 是 $A^T A$ 的特征值, 也是 AA^T 的特征值.

(4) AA^T 和 $A^T A$ 的非零特征值相同, 且有相同的重数.

习题 10.31. 证明二阶对称实方阵 A 是正定的当且仅当其迹和行列式同时大于零.

习题 10.32. 假设 A 是正定实对称矩阵, 证明存在唯一的正定实对称矩阵 B 使得 $B^2 = A$.

习题 10.33. 设实对称矩阵 A 满足 $A^5 = I_n$, 证明 $A = I_n$.

习题 10.34. 假设 A 和 B 是 n -阶实对称矩阵, 且 A 正定, 证明存在可逆实矩阵 P 使得 $P^T A P$ 和 $P^T B P$ 均为对角矩阵.

习题 10.35. 考虑 $m \times n$ 实矩阵组成的线性空间 $V = M_{m \times n}(\mathbb{R})$ 和内积 $g(A, B) = \text{tr}(A^T B)$. 假设 P 和 Q 分别为 m 阶和 n 正交实矩阵, 证明 $T_{P, Q}(A) = PAQ$ 定义了一个 V 上的正交变换.

习题 10.36. 定义内积空间 E 中任意两个子集 X, Y 之间的距离为

$$\text{dist}(X, Y) = \inf\{|x - y| \mid x \in X, y \in Y\}.$$

对 E 中的向量 v 和子空间 W , 证明

$$\text{dist}(\{v\}, W) = |v - \text{Proj}_W(v)|.$$

习题 10.37. 对任意矩阵 A , 定义 $\|A\| = \sqrt{\operatorname{tr}(A^T A)}$. 设 A 为 n 阶实对称矩阵, v 为任意 n 维非零实列向量. 求证:

$$\|A\|^2 \geq \frac{2n-1}{2(n-1)} \cdot \frac{\|Av\|^2}{\|v\|^2} - \frac{1}{n-1} (\operatorname{tr} A)^2.$$

习题 10.38. 假设 V 是一个 n 维内积空间, 带有正定对称双线性型 $\langle \cdot, \cdot \rangle$. 取 T 是 V 上的自伴随变换.

(1) 对于 V 的子空间 W , 以及 W 的标准正交基 v_1, \dots, v_k , 考虑数

$$\sum_{i=1}^k \langle v_i, T(v_i) \rangle$$

证明这个数只依赖于 W 和 T , 而不依赖于标准正交基的选取. 我们记为广义迹 $\operatorname{tr}(T|_W)$. (注意 W 不一定是 T 的不变子空间.)

(2) 假设 T 的 n 个特征值是 $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots \geq \lambda_n$, 对任意 $1 \leq k \leq n$, 证明

$$\lambda_1 + \dots + \lambda_k = \max_{\dim(W)=k, W \text{ 是 } V \text{ 的子空间}} \operatorname{tr}(T|_W)$$

习题 10.39. 假设 V 实 n 阶实对称阵组成的实线性空间, 在 V 上定义 *Frobenius* 内积 $(A, B) = \operatorname{tr}(AB)$.

(1) 求出 V 的一组标准正交基;

(2) 设 B 是 n 阶实矩阵, 定义 $f(A) = B^T A B$, 这是 V 上的线性变换. 求证: f 是自伴随算子的充分必要条件是 B 为对称阵或反对称阵.

习题 10.40. 假设 V 是带有正定厄米特型的复线性空间, $T: V \rightarrow V$ 是 V 上的自伴算子. 如果 v, w 是 T 的两个不同特征值的对应的特征向量, 证明 v 和 w 是正交的.

习题 10.41. 证明两个酉方阵复相似当且仅当他们酉相似.

习题 10.42. 证明反对称实方阵可以酉对角化, 并且特征值一定是 0 或者纯虚数.

习题 10.43. 假设 A, B 是可交换的厄米特阵, 证明存在一个酉矩阵 P 使得 $P^* A P$ 和 $P^* B P$ 同时都是对角阵.

习题 10.44. 假设 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 是行列式为 1 的酉方阵, 证明 $a = \bar{d}$, $b = -\bar{c}$.

习题 10.45. 证明以下方阵酉相似:

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} e^{\sqrt{-1}\theta} & 0 \\ 0 & e^{-\sqrt{-1}\theta} \end{pmatrix}$$

习题 10.46. 设 A 是一个正规复方阵。证明 A^* 可以写成 A 的多项式。

习题 10.47 (Fischer 不等式). 设 A, B 是 $n \times n$ 半正定实矩阵。证明 Fischer 不等式: 对于任意 $n \times n$ 实方阵 C ,

$$\det \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \leq \det(A) \det(B).$$

并讨论等号成立条件。

习题 10.48 (谱矩、秩一扰动与样本协方差, 综合). 设 A 是一个 $n \times n$ 实对称矩阵, 特征值记为 $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ 。

1. 令 $p_k(A) = \text{tr}(A^k)$ 。证明对任意偶数 $k = 2m$,

$$\lim_{m \rightarrow \infty} (p_{2m}(A))^{1/(2m)} = \max_{1 \leq i \leq n} |\lambda_i|.$$

并说明若 $\text{tr}(A^{2m}) \leq C^m$ 对所有 $m \geq 1$ 成立, 则 A 的所有特征值都落在 $[-\sqrt{C}, \sqrt{C}]$ 中。

2. 设 $v \in \mathbb{R}^n$ 非零, $c > 0$, 令 $\tilde{A} = A + cvv^T$ 。若 \tilde{A} 的特征值为 $\tilde{\lambda}_1 \geq \cdots \geq \tilde{\lambda}_n$, 证明

$$\lambda_i \leq \tilde{\lambda}_i \leq \lambda_{i-1} \quad (1 \leq i \leq n),$$

其中约定 $\lambda_0 = +\infty$ 。提示: 可使用 Courant-Fischer 极大极小原理。

3. 设 X 是 $n \times p$ 矩阵, $A = XX^T$, $B = X^T X$ 。证明 A 与 B 具有完全相同的非零特征值, 且代数重数相同。并说明为何计算 $\text{tr}((X^T X)^k)$ 等效于计算 $\text{tr}((XX^T)^k)$ 。

4. 若 A 是完全图 K_n 的邻接矩阵, 即对角线元素为 0、非对角线元素全为 1, 证明 $\text{tr}(A^k)$ 等于 K_n 中长度为 k 且回到出发点的闭合行走总数。

习题 10.49 (Householder 反射、秩一更新与常对角矩阵). 对任意单位列向量 $u \in \mathbb{R}^n$, 定义 $H = I_n - 2uu^T$ 。

1. 证明 H 是对称正交矩阵。说明它的几何含义, 并求出 H 的所有特征值及其几何重数。

2. 给定任意两个长度相等的非零向量 $x, y \in \mathbb{R}^n$, 且 $x \neq y$ 。构造单位向量 u , 使得 $H_u x = y$ 。并由此说明列满秩矩阵可以通过一系列 Householder 反射化为上三角矩阵。

3. 设 $A = I_n + cxy^T$, 其中 $x, y \in \mathbb{R}^n$ 且 $c \neq 0$ 。给出 A 可逆的充分必要条件, 并在可逆时写出 $(I_n + cxy^T)^{-1}$ 的秩一更新形式。

4. 设 $A \in \mathbb{R}^{n \times n}$ 的所有对角线元素等于 a , 所有非对角线元素等于 $b \neq 0$, 即

$$A = (a - b)I_n + b\mathbf{1}\mathbf{1}^T.$$

不展开特征多项式, 求 A 的全部特征值及其代数重数。

习题 10.50 (A_n 根格与 Gram 矩阵). 设

$$\Lambda_n = \left\{ x = (x_1, \dots, x_{n+1})^T \in \mathbb{R}^{n+1} \mid x_i \in \mathbb{Z}, \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

1. 证明 Λ_n 是秩为 n 的自由阿贝尔群, 并显式写出一组 n 个向量的基。
2. 在这组基下, 计算对应 Gram 矩阵 G 的行列式。
3. 证明 Λ_n 中最短非零向量长度平方为 2, 并求这样的向量个数。

习题 10.51 (图 Laplacian). 设 $G = (V, E)$ 是有限连通简单图, 邻接矩阵为 A , 度矩阵为 D , Laplacian 为 $L = D - A$ 。

1. 证明 L 是半正定矩阵, 且 $\ker L = \text{span}(\mathbf{1})$ 。
2. 对任意 $\sum_{v \in V} f(v) = 0$ 的函数 $f: V \rightarrow \mathbb{R}$, 证明与第二特征值 λ_2 相关的 Poincare 型不等式。
3. 说明或证明 Kirchhoff 矩阵树定理: 生成树个数等于 $\frac{1}{n} \lambda_2 \lambda_3 \cdots \lambda_n$ 。

习题 10.52 (Cayley 变换: Hermite 到酉). 设 V 为 $M_n(\mathbb{C})$ 中 Hermitian 矩阵构成的实向量空间:

$$V = \{A \in M_n(\mathbb{C}) \mid A = \overline{A}^T\}.$$

1. 证明对于每一个 $A \in V$, $A - \sqrt{-1}I$ 均可逆。
2. 定义

$$f(A) = (A + \sqrt{-1}I)(A - \sqrt{-1}I)^{-1}.$$

证明 $f(A)$ 是酉矩阵。

3. 用特征值刻画 $f: V \rightarrow U(n)$ 的像。
4. 判断 f 是否单射。

习题 10.53 (正方体正交对称群的迹). 设 G 是三维欧氏空间中保持中心在原点的正方体不变的所有正交变换组成的集合。求

$$\sum_{A \in G} (\text{tr}(A))^2.$$

习题 10.54 (循环矩阵、DFT 与卷积). 设 $\omega = e^{2\pi i/n}$, $n \times n$ 矩阵 F 定义为

$$F_{jk} = \omega^{jk} \quad (0 \leq j, k \leq n-1).$$

两个向量 $a, b \in \mathbb{C}^n$ 的循环卷积定义为

$$(a * b)_k = \sum_{j=0}^{n-1} a_j b_{(k-j) \bmod n}.$$

1. 证明 $\frac{1}{\sqrt{n}}F$ 是酉矩阵。
2. 证明卷积定理: $\widehat{a * b_k} = \hat{a}_k \hat{b}_k$ 。

习题 10.55 (Hermite 投影的范数判别). 设 $A \in M_n(\mathbb{C})$ 满足 $A^2 = A$. 证明: A 为 Hermite 矩阵的充分必要条件是, 对任意 $x \in \mathbb{C}^n$ 都有

$$\|Ax\| \leq \|x\|.$$

习题 10.56 (酉矩阵的 Cayley 变换). 记

$$\mathfrak{u}(n) = \{X \in M_n(\mathbb{C}) \mid X^* = -X\}.$$

对任意 $X \in \mathfrak{u}(n)$, 定义

$$\mathcal{C}(X) = (I_n - X)(I_n + X)^{-1}.$$

证明:

1. 对任意 $X \in \mathfrak{u}(n)$, 矩阵 $I_n + X$ 可逆, 且 $\mathcal{C}(X) \in U(n)$ 。
2. 若 $U \in U(n)$ 且 -1 不是 U 的特征值, 则存在唯一的 $X \in \mathfrak{u}(n)$ 使

$$U = (I_n - X)(I_n + X)^{-1}.$$

习题 10.57 (内积刻画零变换). 1. 在 \mathbb{C}^n 上取标准内积, 设 $T \in M_n(\mathbb{C})$ 满足

$$\langle Tx, x \rangle = 0 \quad (\forall x \in \mathbb{C}^n).$$

证明 $T = 0$ 。

2. 在 \mathbb{R}^n 上取标准内积, 若 $T \in M_n(\mathbb{R})$ 满足

$$\langle Tx, x \rangle = 0 \quad (\forall x \in \mathbb{R}^n),$$

判断 T 是否必为零矩阵, 并证明结论。

习题 10.58 (酉反射分解). 设 $x \in \mathbb{C}^n$ 是单位向量, $\alpha \in \mathbb{C}$ 满足 $|\alpha| = 1$ 且 $\alpha \neq 1$. 定义

$$R_{x,\alpha} = I_n + (\alpha - 1)xx^*.$$

1. 证明 $R_{x,\alpha}$ 是酉矩阵。
2. 设 $U \in M_n(\mathbb{C})$ 是酉矩阵, 且 $\text{rank}(U - I_n) = r$. 证明 U 可以写成 r 个这类酉反射的乘积; 并证明一般情形下 r 是所需反射个数的最小值。

习题 10.59 (多项式内积空间上的 Gram-Schmidt). 设 V 是关于 x 的次数小于或等于 2 的实系数多项式组成的实线性空间。定义

$$B(f, g) = \int_{-1}^1 x^2 f(x)g(x) dx.$$

求 B 的符号。如果正定, 请用 Gram-Schmidt 正交化和基 $1, x, x^2$ 求出一组标准正交基。

习题 10.60 (二阶矩阵的分解判断). 对二阶可逆实方阵 A , 判断是否总存在满足如下条件的实方阵 B, C 使得 $A = BC$:

1. B 下三角阵, C 上三角阵;
2. B 正交阵, C 上三角阵;
3. B 反对称, C 正交阵;
4. B 对称, C 正交阵;
5. $B = C$ 。

习题 10.61 (对称矩阵空间上的自伴算子). 设 V 是对称实矩阵组成的线性空间, 双线性型定义为

$$\langle A, B \rangle = \text{tr}(AB).$$

1. 证明 \langle, \rangle 是正定的。
2. 假设 C 是一个 n 阶实方阵, 定义线性变换

$$\varphi_C(A) = CAC^T.$$

证明: φ_C 是自伴算子当且仅当 C 是对称矩阵或者反对称矩阵。

11 应用选读：奇异值分解及其应用

选学背景

奇异值分解是现代数据分析、图像压缩和最小二乘法中的核心工具，但完整理论需要内积空间、正交投影和谱定理。本章可作为应用选读安排为主线之后阅读；先掌握二维/三维向量、正交投影和实对称矩阵对角化，再学习本章内容会更便于理解。

历史与动机

奇异值分解 (singular value decomposition, SVD) 是线性代数中最深刻也最实用的工具之一。它的发展历程横跨一个半世纪，汇聚了分析学、代数学和数值计算的智慧，最终在 20 世纪下半叶成为现代科学技术的基石。

奇异值的概念最早可以追溯到 19 世纪后半叶。1873–1874 年，意大利数学家贝尔特拉米 (Eugenio Beltrami) 和法国数学家若尔当 (Camille Jordan) 几乎同时独立地发现了双线性型的“奇异值”：给定实矩阵 A ， $A^T A$ 的特征值的平方根具有特殊的几何意义——它们度量了线性映射在各“主方向”上的伸缩倍率。不久之后，英国数学家西尔维斯特 (James Joseph Sylvester) 在 1889 年提出了“canonical multipliers” (标准乘子) 的概念并给出了现代意义上的命名。值得注意的是，Sylvester 正是最早使用“matrix” (矩阵) 一词的人——他在 1850 年引入了这一术语。在此后的 1 年，他的合作者凯莱 (Arthur Cayley) 系统地发展了矩阵代数。

与“奇异值”密切相关的是“特征值” (eigenvalue) 概念的命名史。“Eigenvalue”一词源自德语“Eigenwert”，其中“eigen”意为“自身的、固有的”。这一术语由希尔伯特 (David Hilbert) 在 1904 年研究积分方程时推广使用。在此之前，特征值在不同语境下有过许多不同名称：拉格朗日 (Lagrange) 称之为“valeur propre” (固有值)，柯西 (Cauchy) 使用“valeur caractéristique” (特征值)，而在力学中它们被称为“主值” (principal value) 或“固有频率” (natural frequency)。特征值刻画的是一个线性变换作用在同一个空间上的伸缩行为，而奇异值刻画的是线性映射在两个不同空间之间的伸缩行为——后者的适用范围更广，因为它不要求矩阵是方阵，也不要求矩阵可对角化。

20 世纪初，施密特 (Erhard Schmidt) 在 1907 年将奇异值分解推广到积分算子 (无穷维情形)，开创了算子理论中的一个重要分支。1936 年，埃卡特 (Carl Eckart) 和杨 (Gale Young) 证明了截断奇异值分解给出最佳低秩逼近 (即 Eckart–Young 定理，定理 11.2)，这一结果奠定了 SVD 在数据压缩中的理论基础。

然而，真正使奇异值分解成为实用工具的，是 20 世纪 60 年代计算机的普及和高效数值算法的发展。1965 年，戈卢布 (Gene Golub) 和卡汉 (William Kahan) 提出了计算奇异值分解的稳定数值算法，使得对大规模矩阵进行 SVD 变得切实可行。此后，SVD 迅速渗透到科学与工程各个角落：

- **数据压缩与降维:** 低秩逼近可用于图像压缩、推荐系统 (如 Netflix Prize 竞赛中的矩阵分解方法) 和基因表达分析;
- **统计学:** 主成分分析 (PCA) 的数学本质就是 SVD, 它是现代多元统计分析的基础工具;
- **信号处理:** SVD 用于噪声过滤——保留大奇异值对应的分量 (信号), 丢弃小奇异值对应的分量 (噪声);
- **数值线性代数:** 伪逆和最小二乘法通过 SVD 给出了对任意矩阵 (包括秩亏缺矩阵) 的统一解法;
- **自然语言处理:** 潜在语义分析 (LSA) 利用 SVD 提取文本的语义结构, 是现代大语言模型的先驱技术之一;
- **控制论与动力系统:** 奇异值刻画了系统的可控性和可观测性, 在鲁棒控制中起核心作用.

SVD 与文本检索

把一个文档集合表示成“词语-文档矩阵”后, 矩阵的每一列代表一篇文档, 每一行代表一个词语. SVD 可以把这个高维矩阵近似为低秩结构, 从而提取若干潜在主题方向. 这样, 即使两篇文章没有使用完全相同的关键词, 只要它们在低维主题空间中接近, 检索系统也可能判断它们语义相关. 这就是早期潜在语义分析的线性代数核心.

可以毫不夸张地说, 如果谱定理 (定理10.3) 是对称世界的“终极分解”, 那么奇异值分解就是一般线性映射的“终极分解”. 在第10章中, 我们学习了内积空间和谱定理——它告诉我们自伴随变换 (对称矩阵) 可以用正交基对角化. 本节将这一思想推广到任意矩阵 (不必对称, 甚至不必是方阵), 发展奇异值分解理论及其在低秩逼近、主成分分析和最小二乘法中的应用.

11.1 奇异值分解

在第10节中, 我们给出了给定线性空间上的自伴随变换的结构定理, 这也称为自伴随变换的谱定理. 如果 $T: V \rightarrow W$ 是两个不同空间之间的线性映射, 如何找到 T 的标准型?

矩阵的相抵标准型理论告诉我们, 给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, 存在 $P \in GL(n, \mathbb{R})$, $Q \in GL(m, \mathbb{R})$ 使得:

$$Q^{-1}AP = \begin{pmatrix} I_r & O \\ O & O \end{pmatrix}$$

其中 $r = \text{rank } A$. 现在我们在线性空间上附加内积结构, 故希望 P, Q 可以做到正交矩阵.

定理 11.1 (奇异值分解). 设 $A \in M_{m \times n}(\mathbb{R})$, 存在 $P \in O(n)$, $Q \in O(m)$ 使得:

$$A = QDP^T,$$

其中

$$D = \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}_{m \times n}, \quad \sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r \geq 0$$

. σ_i 称为 A 的**奇异值**(singular value).

奇异值分解的几何意义

奇异值分解 $A = QDP^T$ 揭示了线性映射最直观的几何本质: **任何线性映射都可以分解为“旋转 (或反射) \rightarrow 沿坐标轴伸缩 \rightarrow 旋转 (或反射)”三步.**

具体地说, 设 $A \in M_{m \times n}(\mathbb{R})$ 的奇异值分解为 $A = QDP^T$, 其中 $P \in O(n)$, $Q \in O(m)$, D 是对角型矩阵. 那么对任意 $\mathbf{x} \in \mathbb{R}^n$, 计算 $A\mathbf{x}$ 可以分为三步:

- (1) **定义域中的正交变换:** 先计算 $\mathbf{y}_1 = P^T\mathbf{x}$. 由于 P 是正交矩阵, 这一步将 \mathbf{x} 从标准基变换到由 P 的列向量组成的标准正交基 $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ 下的坐标. 几何上, 这是一个旋转 (或反射), 不改变长度.
- (2) **沿坐标轴的伸缩:** 再计算 $\mathbf{y}_2 = D\mathbf{y}_1$. 由于 D 是对角型, 这一步只是将第 i 个分量乘以 σ_i . 几何上, 这是沿各坐标轴方向分别拉伸 $\sigma_1, \sigma_2, \dots$ 倍.
- (3) **值域中的正交变换:** 最后计算 $A\mathbf{x} = Q\mathbf{y}_2$. 由于 Q 是正交矩阵, 这一步将伸缩后的结果旋转 (或反射) 到最终位置.

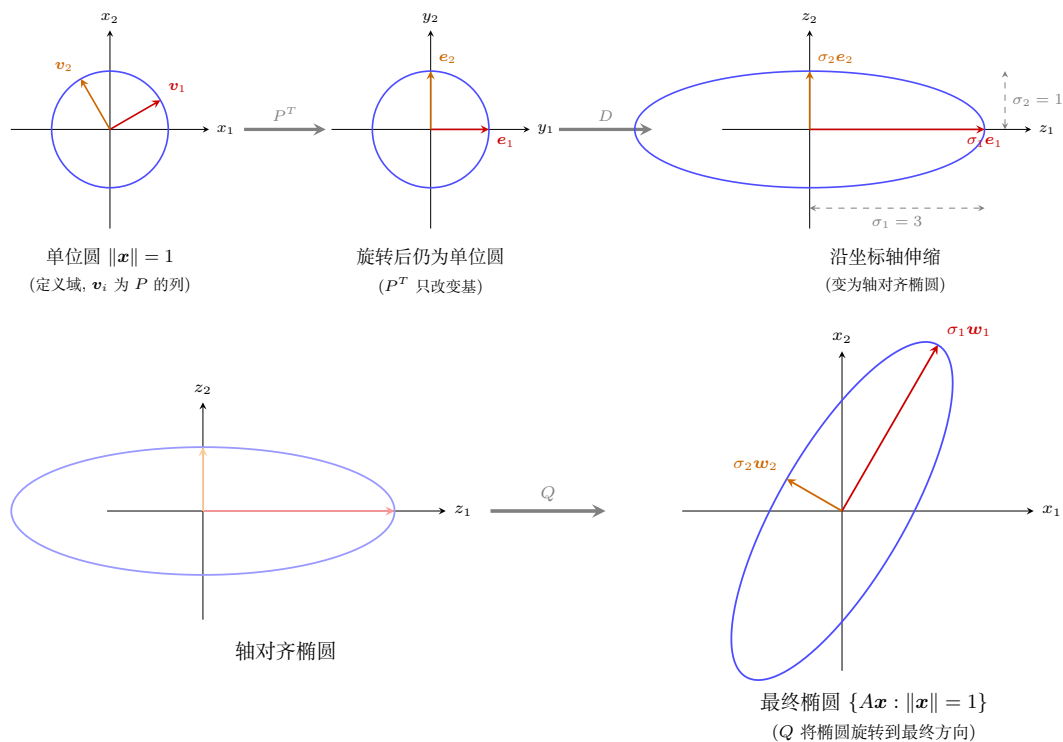
我们以 2×2 的情形来直观说明. 考虑非对称矩阵

$$A = \begin{pmatrix} \sqrt{3} & 0 \\ 2 & \sqrt{3} \end{pmatrix}.$$

它的奇异值分解为 $A = QDP^T$, 其中奇异值 $\sigma_1 = 3, \sigma_2 = 1$, 而

$$D = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} \cos 30^\circ & -\sin 30^\circ \\ \sin 30^\circ & \cos 30^\circ \end{pmatrix}, \quad Q = \begin{pmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{pmatrix}.$$

读者可以直接验证 $QDP^T = A$ (系统的求解方法将在后面的证明中给出). 注意 $P \neq Q$, 这正是非对称矩阵的典型情形: **定义域和价值域中的正交基变换是不同的**. 下图展示了 A 将 \mathbb{R}^2 中的单位圆变为椭圆的过程, 以及每一步的几何含义:



请注意定义域和价值域中的正交基变换是不同的: P 将定义域旋转 30° , 而 Q 将值域旋转 60° . 对于对称矩阵 $A = A^T$, 可以证明 $P = Q$ (即定义域和价值域使用同一组正交基), 此时奇异值分解退化为谱定理.

从图中可以清楚地看到:

- 奇异值 σ_1, σ_2 就是椭圆的两个半轴长度, 度量了线性映射在各“主方向”上的伸缩比率.
- P 的列向量 $\mathbf{v}_1, \mathbf{v}_2$ (称为**右奇异向量**) 是定义域中的“主方向”——单位圆上沿这两个方向的点在映射后成为椭圆的端点.
- Q 的列向量 $\mathbf{w}_1, \mathbf{w}_2$ (称为**左奇异向量**) 是值域中椭圆半轴的方向.
- 若 $\sigma_1 = \sigma_2$, 则椭圆退化为圆, 此时 A 是一个等比例伸缩 (加旋转); 若某个 $\sigma_i = 0$, 则椭圆在对应方向上被压扁, 反映了 A 的秩亏缺.

总之, 奇异值分解 $A = QDP^T$ 的几何意义可以概括为一句话: **选取定义域和价值域中各一组标准正交基 (P 和 Q 的列), 使得线性映射 T_A 在这两组基下的表示变为最简单的对角**

伸缩矩阵 D .

注 11.1. 假设 $A = QDP^T$ 是 A 的奇异值分解, 记 $Q = (w_1, \dots, w_m), P = (v_1, \dots, v_n)$, 则

$$A = \sum_{i=1}^r \sigma_i w_i v_i^T,$$

这是奇异值分解的常用形式.

证明. 我们先证明奇异值的唯一性: 若 $A = QDP^T$, 则

$$A^T A = P \text{diag}\{\sigma_1^2, \dots, \sigma_n^2\} P^T,$$

所以 $\sigma_1^2, \dots, \sigma_n^2$ 是 $A^T A$ 的特征值, 排序后由 A 唯一决定.

下面证明奇异值分解的存在性: 由于 $A^T A$ 对称, 从而存在 $P \in O(n)$ 使得

$$P^{-1}(A^T A)P = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & & \\ & & & & \\ & & & & \lambda_n \end{pmatrix},$$

其中 $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0$. 设 $P = (v_1, \dots, v_n)$, 则 $A^T A v_i = \lambda_i v_i$.

下面我们证明 Av_1, \dots, Av_n 相互正交:

$$\begin{aligned} \langle Av_i, Av_j \rangle_{\mathbb{R}^m} &= (Av_i)^T (Av_j) \\ &= v_i^T (A^T Av_j) \\ &= \lambda_j v_i^T v_j \\ &= \lambda_j \langle v_i, v_j \rangle_{\mathbb{R}^n}. \end{aligned}$$

因此当 $i \neq j$ 时为 0, 当 $i = j$ 时为 λ_i .

假设 $\lambda_1 \geq \dots \geq \lambda_r > 0, \lambda_{r+1} = \dots = \lambda_n = 0$. 取

$$w_i = \frac{Av_i}{\|Av_i\|_{\mathbb{R}^m}} = \frac{Av_i}{\sqrt{\lambda_i}}, \quad i = 1, \dots, r$$

则 w_1, \dots, w_r 标准正交. 如果我们记 $\sigma_i := \sqrt{\lambda_i}$, 则

$$(Av_1, \dots, Av_n) = (w_1, \dots, w_n) \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}_{m \times n}$$

即

$$AP = QD, \quad P \in O(n), \quad Q \in O(m).$$

□

例 11.1 (求解奇异值分解). 设

$$A = \begin{pmatrix} 1 & 2 \\ 1 & -1 \\ 2 & 1 \end{pmatrix} \in M_{3 \times 2}(\mathbb{R}).$$

我们按照上述证明中的步骤求 A 的奇异值分解 $A = QDP^T$.

第一步: 求奇异值. 计算

$$A^T A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & -1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 3 & 6 \end{pmatrix}.$$

$A^T A$ 的特征多项式为

$$\det(\lambda I - A^T A) = (\lambda - 6)^2 - 9 = \lambda^2 - 12\lambda + 27 = (\lambda - 9)(\lambda - 3),$$

故特征值为 $\lambda_1 = 9$, $\lambda_2 = 3$, 奇异值为 $\sigma_1 = 3$, $\sigma_2 = \sqrt{3}$.

第二步: 求右奇异向量 P . $A^T A$ 的特征向量:

- $\lambda_1 = 9$: 解 $(9I - A^T A)\mathbf{v} = \mathbf{0}$, 即 $\begin{pmatrix} 3 & -3 \\ -3 & 3 \end{pmatrix} \mathbf{v} = \mathbf{0}$, 得 $\mathbf{v}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$;
- $\lambda_2 = 3$: 解 $(3I - A^T A)\mathbf{v} = \mathbf{0}$, 即 $\begin{pmatrix} -3 & -3 \\ -3 & -3 \end{pmatrix} \mathbf{v} = \mathbf{0}$, 得 $\mathbf{v}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

因此

$$P = (\mathbf{v}_1, \mathbf{v}_2) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in O(2).$$

第三步: 求左奇异向量 Q . 由 $\mathbf{w}_i = \frac{A\mathbf{v}_i}{\sigma_i}$:

$$\mathbf{w}_1 = \frac{A\mathbf{v}_1}{\sigma_1} = \frac{1}{3} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{w}_2 = \frac{A\mathbf{v}_2}{\sigma_2} = \frac{1}{\sqrt{3}} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}.$$

由于 $m = 3 > n = 2$, 还需补充 \mathbf{w}_3 使 $\{\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$ 成为 \mathbb{R}^3 的标准正交基. \mathbf{w}_3 可以通过求 $\mathbf{w}_1 \times \mathbf{w}_2$ 或解方程组 ($\mathbf{w}_1^T x = 0, \mathbf{w}_2^T x = 0$) 得到. 容易算出

$$\mathbf{w}_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}.$$

因此

$$Q = (\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3) = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{3}} \end{pmatrix} \in O(3).$$

直接计算可验证此时 $A = QDP^T$.

11.2 低秩逼近与应用

在数据科学与工程中, 我们经常遇到高维数据: 一张灰度图片可以看作一个 $m \times n$ 矩阵, 一组实验记录构成一个数据矩阵, 一份推荐系统的用户-商品评分表也是一个矩阵. 这些矩阵往往规模庞大, 但其中蕴含的“有效信息”远少于矩阵元素的总数 mn ——换言之, 矩阵近似地具有较低的秩. 奇异值分解恰好提供了一种自然的方式来提取这些有效信息.

除了图像压缩之外, 低秩逼近在推荐系统和自然语言处理中也很重要. 用户-商品评分矩阵常可近似看成由少数几个“潜在兴趣”和“潜在属性”生成的低秩矩阵, 这正是矩阵分解推荐算法的基本思想. 在文本处理中, 词项-文档矩阵的低秩近似则对应潜在语义分析. 因而低秩并不只是一个技术条件, 而是在刻画数据中隐藏的低维结构.

给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, 利用奇异值分解我们可以将其写成

$$A = \sum_{i=1}^r \sigma_i \mathbf{w}_i \mathbf{v}_i^T, \quad r = \text{rank } A,$$

其中 $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > 0$ 是 A 的奇异值, 每个 $\sigma_i \mathbf{w}_i \mathbf{v}_i^T$ 是一个秩 1 矩阵. 取 $k \ll r$, 则有近似

$$A_k = \sum_{i=1}^k \sigma_i \mathbf{w}_i \mathbf{v}_i^T.$$

存储 A 需要 mn 个数据, 而存储 A_k 只需要 k 个奇异值加上 k 个 m 维向量 \mathbf{w}_i 和 k 个 n 维向量 \mathbf{v}_i , 共 $k(m+n+1)$ 个数据. 当 k 较小时, 这是巨大的压缩.

11.2.1 图像压缩的例子

为了直观地理解低秩逼近的效果, 我们以图像压缩为例. 一张 $m \times n$ 的灰度图片可以用矩阵 $A = (a_{ij})_{m \times n}$ 表示, 其中 a_{ij} 是 (i, j) 点处像素的灰度值 (取值范围 0-255, 其中 0 代表黑色, 255 代表白色).

下面选取两个中文字符来观察结构复杂度与奇异值衰减的关系. 先看汉字“中”. 设 $B = (b_{ij}) \in M_{24 \times 24}(\mathbb{R})$ 是把“中”绘制到 24×24 灰度网格后得到的矩阵, 其显式形式为

$$B = \begin{pmatrix} 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 254 & 255 & 243 & 226 & 235 & 246 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 253 & 255 & 208 & 13 & 38 & 229 & 255 & 254 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 254 & 254 & 255 & 255 & 253 & 255 & 225 & 0 & 42 & 255 & 254 & 255 & 255 & 255 & 254 & 254 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 254 & 252 & 253 & 227 & 1 & 48 & 253 & 252 & 254 & 254 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 251 & 246 & 254 & 255 & 255 & 255 & 255 & 239 & 0 & 49 & 255 & 255 & 255 & 255 & 255 & 253 & 245 & 252 & 255 & 255 & 255 \\ 255 & 255 & 255 & 226 & 39 & 38 & 40 & 45 & 49 & 53 & 49 & 0 & 10 & 54 & 51 & 48 & 44 & 39 & 37 & 37 & 226 & 255 & 255 & 255 \\ 255 & 255 & 255 & 237 & 15 & 0 & 20 & 18 & 17 & 17 & 15 & 0 & 3 & 16 & 17 & 17 & 18 & 19 & 0 & 12 & 232 & 255 & 255 & 255 \\ 255 & 255 & 255 & 243 & 19 & 34 & 250 & 250 & 248 & 251 & 225 & 0 & 46 & 251 & 250 & 249 & 250 & 239 & 19 & 17 & 238 & 255 & 255 & 255 \\ 255 & 255 & 255 & 243 & 17 & 33 & 255 & 255 & 255 & 255 & 231 & 0 & 47 & 255 & 255 & 255 & 255 & 246 & 18 & 16 & 238 & 255 & 255 & 255 \\ 255 & 255 & 255 & 243 & 17 & 33 & 254 & 254 & 252 & 254 & 228 & 0 & 47 & 254 & 253 & 253 & 254 & 243 & 18 & 16 & 238 & 255 & 255 & 255 \\ 255 & 255 & 255 & 243 & 17 & 33 & 255 & 255 & 253 & 255 & 229 & 0 & 47 & 255 & 254 & 254 & 255 & 244 & 18 & 16 & 238 & 255 & 255 & 255 \\ 255 & 255 & 255 & 243 & 17 & 34 & 255 & 255 & 255 & 255 & 234 & 0 & 48 & 255 & 255 & 255 & 255 & 249 & 18 & 16 & 238 & 255 & 255 & 255 \\ 255 & 255 & 255 & 240 & 24 & 5 & 38 & 37 & 37 & 37 & 34 & 0 & 7 & 37 & 37 & 37 & 37 & 3 & 21 & 236 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 236 & 24 & 8 & 33 & 32 & 32 & 32 & 29 & 0 & 6 & 32 & 32 & 32 & 32 & 4 & 19 & 233 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 225 & 0 & 20 & 255 & 255 & 255 & 255 & 232 & 0 & 48 & 255 & 255 & 255 & 255 & 247 & 13 & 0 & 224 & 255 & 255 & 255 \\ 255 & 255 & 255 & 238 & 142 & 159 & 255 & 255 & 253 & 255 & 229 & 0 & 47 & 255 & 254 & 255 & 255 & 252 & 201 & 196 & 247 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 253 & 255 & 229 & 0 & 47 & 255 & 253 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 254 & 251 & 251 & 255 & 255 & 253 & 255 & 228 & 0 & 46 & 255 & 254 & 255 & 255 & 255 & 252 & 252 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 253 & 255 & 220 & 1 & 43 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 253 & 255 & 209 & 0 & 31 & 250 & 255 & 254 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 252 & 255 & 195 & 5 & 25 & 239 & 255 & 254 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 243 & 212 & 214 & 251 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 \\ 255 & 255 \end{pmatrix}$$

这个矩阵的秩为 19, 前 12 个奇异值约为

$$5195, 1063, 773, 506, 54, 44, 26, 16, 11, 7.5, 5.4, 3.6.$$

可以看到, 这里在第 4 个奇异值以后就出现了明显的数量级下降. 相应地,

- $k = 1$: 保留 93.1% 的能量, 相对误差约 26.2%;
- $k = 2$: 保留 97.0% 的能量, 相对误差约 17.2%;
- $k = 4$: 保留 99.979% 的能量, 相对误差约 1.45%;
- $k = 8$: 保留 99.999% 的能量, 相对误差约 0.28%.

原图需要存储 576 个数, 而 B_4 只需存储 196 个数. 由于“中”主要由几条横竖笔画组成, 其主结构非常接近低秩对象, 因而只保留少数几个奇异值就已经足够.

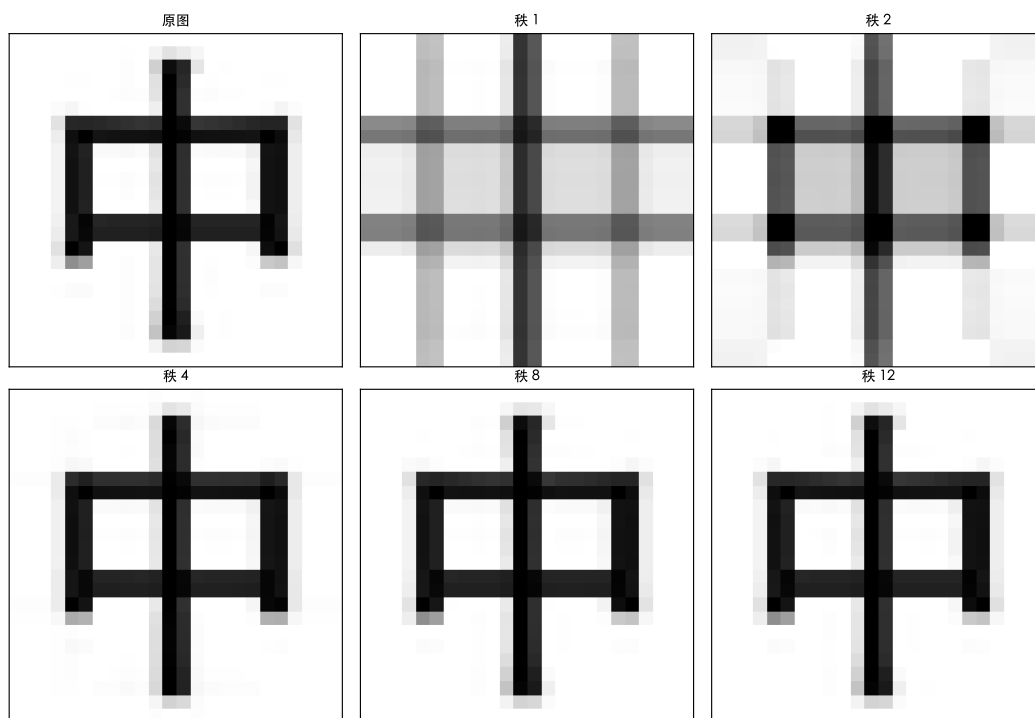


图 16: 汉字“中”灰度矩阵 (24×24 , 秩 19) 的低秩逼近: 秩 1 与秩 2 已经保留横竖主轮廓, 秩 4 后字形已很清楚, 秩 8 与秩 12 时几乎与原图无异.

再看一个更复杂的汉字“国”. 设 $C \in M_{24 \times 24}(\mathbb{R})$ 是它的灰度矩阵, 其显式形式为

$$C = \begin{pmatrix} 255 & 255 \\ 255 & 255 & 249 & 232 & 245 & 254 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 254 & 245 & 232 & 249 & 255 & 255 & 255 \\ 255 & 255 & 232 & 35 & 30 & 27 & 31 & 34 & 36 & 37 & 37 & 38 & 38 & 37 & 37 & 36 & 34 & 31 & 27 & 29 & 36 & 233 & 255 & 255 \\ 255 & 255 & 247 & 27 & 0 & 51 & 49 & 46 & 47 & 47 & 47 & 47 & 47 & 47 & 47 & 46 & 49 & 51 & 0 & 27 & 248 & 255 & 255 \\ 255 & 255 & 252 & 32 & 20 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 20 & 32 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 17 & 248 & 230 & 189 & 202 & 207 & 209 & 207 & 210 & 211 & 209 & 205 & 193 & 229 & 248 & 17 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 15 & 255 & 163 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 157 & 255 & 14 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 16 & 252 & 207 & 112 & 125 & 133 & 109 & 0 & 67 & 138 & 130 & 127 & 111 & 204 & 252 & 16 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 18 & 247 & 255 & 255 & 255 & 255 & 218 & 0 & 132 & 255 & 255 & 255 & 255 & 255 & 247 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 18 & 248 & 253 & 246 & 250 & 255 & 206 & 0 & 125 & 255 & 254 & 254 & 246 & 253 & 248 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 17 & 250 & 252 & 43 & 23 & 31 & 26 & 0 & 17 & 34 & 30 & 23 & 52 & 255 & 248 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 17 & 250 & 252 & 81 & 68 & 79 & 63 & 0 & 37 & 81 & 92 & 77 & 87 & 254 & 248 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 18 & 248 & 255 & 255 & 255 & 255 & 218 & 0 & 133 & 255 & 123 & 154 & 255 & 254 & 248 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 18 & 248 & 252 & 248 & 245 & 247 & 197 & 0 & 122 & 237 & 17 & 0 & 181 & 252 & 245 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 18 & 248 & 255 & 255 & 255 & 255 & 219 & 1 & 129 & 255 & 206 & 106 & 236 & 255 & 247 & 18 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 19 & 246 & 110 & 94 & 101 & 105 & 83 & 0 & 49 & 105 & 103 & 111 & 98 & 109 & 247 & 19 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 19 & 246 & 30 & 0 & 0 & 0 & 2 & 17 & 8 & 0 & 0 & 0 & 30 & 246 & 19 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 19 & 251 & 231 & 235 & 241 & 244 & 244 & 242 & 244 & 246 & 245 & 243 & 236 & 232 & 251 & 19 & 31 & 252 & 255 & 255 \\ 255 & 255 & 252 & 31 & 17 & 237 & 251 & 249 & 249 & 249 & 248 & 248 & 248 & 248 & 248 & 249 & 249 & 251 & 237 & 17 & 31 & 252 & 255 & 255 \\ 255 & 255 & 248 & 35 & 1 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 4 & 3 & 36 & 248 & 255 & 255 \\ 255 & 255 & 242 & 22 & 5 & 87 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 89 & 87 & 0 & 6 & 237 & 255 & 255 \\ 255 & 255 & 230 & 16 & 33 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 255 & 89 & 74 & 234 & 255 & 255 \\ 255 & 255 & 249 & 219 & 223 & 250 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 & 252 & 255 & 255 & 255 & 255 \\ 255 & 255 \end{pmatrix}$$

计算可得 C 的秩为 21, 前 12 个奇异值约为

$$4542, 1186, 730, 504, 378, 257, 211, 71, 67, 38, 32, 19.$$

与“中”相比,“国”除了外框之外还有内部结构,因而奇异值衰减更慢一些.例如

- $k = 1$: 保留 89.3% 的能量, 相对误差约 32.6%;
- $k = 2$: 保留 95.4% 的能量, 相对误差约 21.4%;
- $k = 4$: 保留 98.85% 的能量, 相对误差约 10.7%;
- $k = 8$: 保留 99.968% 的能量, 相对误差约 1.80%.

这说明字形内部层次越丰富,需要保留的奇异值通常也越多.

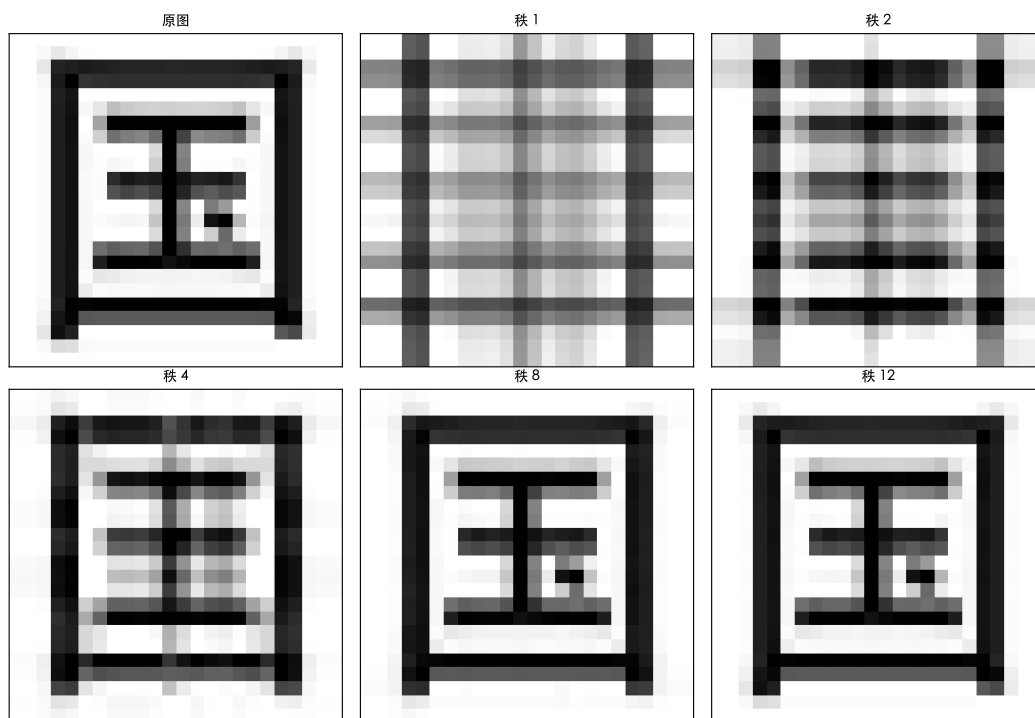


图 17: 汉字“国”灰度矩阵 (24×24 , 秩 21) 的低秩逼近: 它比“中”包含更多内部结构, 因而在同样的秩下恢复得略慢; 秩 8 后主要笔画才基本稳定.

为了更清楚地比较两个汉字的差异, 我们列出它们在不同秩下的能量保留比例和相对误差:

字符与指标	$k = 1$	$k = 2$	$k = 4$	$k = 8$
“中” 能量保留	93.1%	97.0%	99.979%	99.999%
“中” 相对误差	26.2%	17.2%	1.45%	0.28%
“国” 能量保留	89.3%	95.4%	98.85%	99.968%
“国” 相对误差	32.6%	21.4%	10.7%	1.80%

可以看到, “中” 的奇异值衰减更快, 因而更接近低秩结构; “国” 由于存在外框和内部部件的双重结构, 需要更多奇异值才能达到与“中”相当的恢复精度.

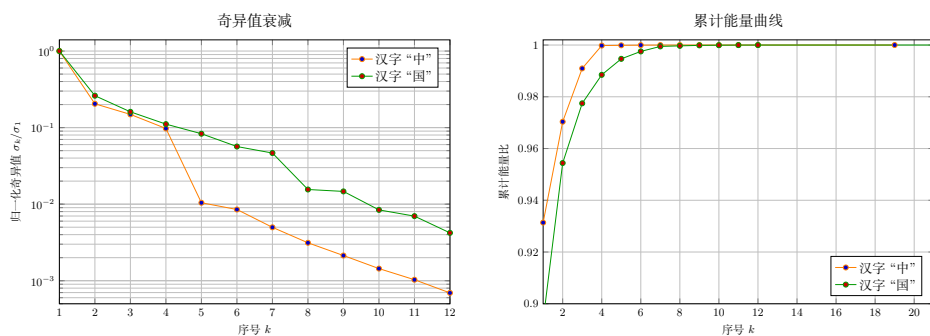


图 18: 汉字“中”与“国”的奇异值衰减和累计能量比较。“中”的曲线下降更快, 对应其更强的低秩结构; “国”的内部结构更多, 因而需要保留更多奇异值。

生成这些矩阵和图片的程序核心流程如下。

- 完整脚本保存在 `tools/generate_svd_zhong_example.py`。
- 运行时需要 `numpy`、`Pillow` 与 `matplotlib`。
- 脚本生成 `pics/svd_zhong.pdf`、`pics/svd_guo.pdf`、`pics/svd_decay_compare.pdf`，以及对应的矩阵 `.tex` 文件和统计文件。

```
for glyph in ["中", "国"]:
    M = render_glyph_as_24_by_24_grayscale_matrix(glyph)
    U, s, Vt = np.linalg.svd(M, full_matrices=False)
    for k in [1, 2, 4, 8, 12]:
        Mk = (U[:, :k] * s[:k]) @ Vt[:k, :]
        save_low_rank_panel(glyph, k, Mk)
    write_matrix_as_latex(glyph, M)
```

```
plot_normalized_singular_values_and_cumulative_energy(["中", "国"])
```

注 11.2. 在实际应用中, 一张 1000×1000 的灰度照片需要存储 10^6 个像素值。若该图片的奇异值快速衰减, 取 $k = 50$ 的低秩逼近仅需存储 $50 \times (1000 + 1000 + 1) = 100,050$ 个数, 压缩比约为 $10:1$, 而人眼几乎无法分辨差异。这正是低秩逼近在图像压缩中的威力。

11.2.2 Eckart–Young 定理

直观上感觉, A_k 应该“很接近” A , 接下来我们严格描述这件事。定义矩阵空间 $M_{m \times n}(\mathbb{R})$ 上的 Frobenius 内积:

$$\langle A, B \rangle_F = \text{tr}(A^T B).$$

则矩阵 A, B 的距离为

$$\sqrt{\langle A - B, A - B \rangle_F} = \sqrt{\sum_{i,j} (a_{ij} - b_{ij})^2}.$$

定理 11.2 (Eckart-Young, Schmidt). A_k 是秩 $\leq k$ 的 $m \times n$ 矩阵中距离 A 最近的矩阵, 即

$$\|A - A_k\|_F = \min_{\text{rank } B \leq k} \|A - B\|_F.$$

推论 11.1. 设 $A = QDP^T$, $D = \text{diag}(\sigma_1, \dots, \sigma_n)$ 是矩阵 A 的奇异值分解, 则

$$\|A\|_F = \sqrt{\sigma_1^2 + \dots + \sigma_n^2},$$

以及

$$\|A - A_k\|_F = \sqrt{\sigma_{k+1}^2 + \dots + \sigma_n^2}.$$

注 11.3 (能量与逼近误差的直观理解). 上述推论给出了低秩逼近误差的精确公式. 我们可以将其理解为一种“能量分配”: 矩阵 A 的“总能量”为

$$\|A\|_F^2 = \sigma_1^2 + \sigma_2^2 + \dots + \sigma_r^2,$$

其中每个奇异值 σ_i 的平方 σ_i^2 恰好是第 i 个秩 1 分量 $\sigma_i \mathbf{w}_i \mathbf{v}_i^T$ 贡献的能量 (因为不同分量在 *Frobenius* 内积下两两正交). 当我们用 A_k 逼近 A 时, 保留的能量为 $\sigma_1^2 + \dots + \sigma_k^2$, 丢弃的能量为 $\sigma_{k+1}^2 + \dots + \sigma_r^2$, 而

$$\frac{\|A - A_k\|_F^2}{\|A\|_F^2} = \frac{\sigma_{k+1}^2 + \dots + \sigma_r^2}{\sigma_1^2 + \dots + \sigma_r^2} = 1 - \frac{\sigma_1^2 + \dots + \sigma_k^2}{\sigma_1^2 + \dots + \sigma_r^2}.$$

因此, “前 k 个奇异值集中了 $p\%$ 的能量”等价于“用 A_k 逼近 A 的相对误差的平方为 $(1 - p\%)$ ”.

回到图 16 中汉字“中”的例子: 前 4 个奇异值已经携带了几乎全部能量, 此时

$$\frac{\sigma_1^2 + \dots + \sigma_4^2}{\sigma_1^2 + \dots + \sigma_{19}^2} \approx 99.979\%,$$

对应的 *Frobenius* 相对误差 $\|B - B_4\|_F / \|B\|_F \approx 1.45\%$. 这就是为什么秩 4 逼近在图 16 中已经能清楚恢复主要笔画.

在给出定理 11.2 的证明之前, 我们先给出一些证明中会用到的重要的性质.

引理 11.1. 给定矩阵 $A, B \in M_{m \times n}(\mathbb{R})$, 任取 $P \in O(n), Q \in O(m)$, 有

$$\langle QAP^T, QBP^T \rangle_F = \langle A, B \rangle_F.$$

引理 11.2. 给定矩阵 $A \in M_{m \times n}(\mathbb{R})$, 则

$$\sigma_1(A) = \max_{0 \neq v \in \mathbb{R}^n} \frac{|Av|_{\mathbb{R}^m}}{|v|_{\mathbb{R}^n}}.$$

证明. 考虑对称矩阵 $M = A^T A$, 则根据对称矩阵特征值的最大最小原理有

$$\lambda_1(A^T A) = \max_{0 \neq v \in \mathbb{R}^n} \frac{\langle v, A^T A v \rangle_{\mathbb{R}^n}}{\langle v, v \rangle_{\mathbb{R}^n}} = \max_{0 \neq v \in \mathbb{R}^n} \frac{\langle Av, Av \rangle_{\mathbb{R}^m}}{\langle v, v \rangle_{\mathbb{R}^n}},$$

从而有

$$\sigma_1(A) = \sqrt{\lambda_1(A^T A)} = \max_{0 \neq v \in \mathbb{R}^n} \frac{|Av|_{\mathbb{R}^m}}{|v|_{\mathbb{R}^n}}.$$

□

引理 11.3.

(1) 任取矩阵 $A \in M_{m \times n}(\mathbb{R})$, 有

$$\sigma_\ell(A - A_k) = \sigma_{k+\ell}(A)$$

(2) 任取矩阵 $A, B \in M_{m \times n}(\mathbb{R})$, 其中 $\text{rank } B \leq k$, 则

$$\sigma_\ell(A - B) \geq \sigma_{k+\ell}(A)$$

证明. (1): 假设 A 的奇异值分解记为

$$A = \sum_{i=1}^{\min\{m,n\}} \sigma_i w_i v_i^T,$$

则

$$A - A_k = \sum_{i=k+1}^{\min\{m,n\}} \sigma_i w_i v_i^T,$$

从而 $\sigma_\ell(A - A_k) = \sigma_{k+\ell}(A)$.

(2): 假设 A 的奇异值分解记为

$$A = \sum_{i=1}^{\min\{m,n\}} \sigma_i w_i v_i^T.$$

我们先证明 $\ell = 1$ 的情况: 取 $W = \text{span}_{\mathbb{R}}\{v_1, \dots, v_{k+1}\}$. 由于 $\text{rank } B \leq k$, 从而 $\dim \ker B \geq n - k$, 因此 $\ker B \cap W \neq \emptyset$. 取 $0 \neq v \in \ker B \cap W$, 不妨假设 $v = \sum_{i=1}^{k+1} a_i v_i$, 根据引理 11.2 有

$$\sigma_1(A - B) \geq \frac{|(A - B)v|_{\mathbb{R}^m}}{|v|_{\mathbb{R}^n}} = \frac{|Av|_{\mathbb{R}^m}}{|v|_{\mathbb{R}^n}} = \frac{\sqrt{\sum_{i=1}^{k+1} \sigma_i^2 a_i^2}}{\sqrt{\sum_{i=1}^{k+1} a_i^2}} \geq \sigma_{k+1}(A).$$

下面我们证明一般的情况: 根据 (1) 有

$$\begin{aligned} \sigma_\ell(A - B) &= \sigma_1((A - B) - (A - B)_{\ell-1}) \\ &= \sigma_1(A - (B + (A - B)_{\ell-1})) \end{aligned}$$

由于 $\text{rank } B \leq k, \text{rank}(A - B)_{\ell-1} \leq \ell - 1$, 从而

$$\text{rank}(B + (A - B)_{\ell-1}) \leq k + \ell - 1,$$

根据之前的情形有

$$\sigma_1(A - (B + (A - B)_{\ell-1})) \geq \sigma_{k+\ell}(A).$$

□

下面给出定理11.2的证明:

证明.

$$\begin{aligned} \|A - B\|_F^2 &= \sum_{i=1}^n \sigma_i^2(A - B) \\ &\geq \sum_{i=1}^n \sigma_{i+k}^2(A) \\ &= \sum_{i=1}^n \sigma_i^2(A - A_k) \\ &= \|A - A_k\|_F^2. \end{aligned}$$

其中第二个不等号用了引理的 (2), 第三个等号用了引理的 (1).

□

11.3 应用: 低维拟合与主成分分析 (PCA)

在许多实际问题中, 我们采集到的数据虽然形式上是高维的, 但其“本质维度”往往远低于观测维度. 例如:

- **经济学:** 一个国家的多项经济指标 (GDP 增长率、失业率、通胀率、利率等) 往往受到少数几个“隐藏因子” (如总需求、货币政策等) 的共同驱动, 并非独立变化;
- **生物信息学:** 在基因表达分析中, 成百上千个基因的表达水平看似高维, 但可能被少数几条信号通路所调控, 呈现出低维结构;
- **图像识别:** 一张 100×100 像素的人脸图片名义上是 10000 维空间中的一个点, 但所有人脸图片实际上只分布在一个很低维的“人脸流形”附近——光照、表情、角度等几个参数就能决定图片的大致形态.

在这些场景中, 我们需要从高维数据中找到最能代表数据变化的低维方向. 这就是**主成分分析**(principal component analysis, PCA) 的核心问题: 给定 m 个 n 维数据点, 找一个 k 维子空间 ($k \ll n$), 使得数据投影到该子空间后, 损失的信息尽可能少.

我们将看到, 这个问题可以用奇异值分解完美地回答.

11.3.1 最佳低维拟合

思考 11.1. 给定 m 次实验, 每次实验得到一个 n 维数据, 不妨假设 $m \gg n$, 则我们得到如下矩阵

$$A = \begin{pmatrix} \alpha_1^T \\ \alpha_2^T \\ \vdots \\ \alpha_m^T \end{pmatrix}.$$

如何判断 $\alpha_1, \dots, \alpha_m$ 是否落在某个更低维的线性空间附近?

命题 11.1. 给定矩阵 $A \in M_{m \times n}(\mathbb{R}), m > n$ 的奇异值分解

$$A = \sum_{i=1}^n \sigma_i w_i v_i^T.$$

令 $W_k = \text{span}_{\mathbb{R}}\{v_1, \dots, v_k\}$, 则 W_k 使得如下取值最小

$$\sum_{i=1}^m (\text{dist}(\alpha_i, W))^2,$$

其中 W 是 \mathbb{R}^n 的 k 维子空间.

证明. 对任意的 k 维子空间 W , 取 W 的标准正交基 $\{u_1, \dots, u_k\}$, 则

$$\begin{aligned} (\text{dist}(\alpha_i, W))^2 &= \|\alpha - \text{Proj}_W \alpha\|^2 \\ &= \left\| \alpha - \sum_{i=1}^k \langle \alpha, u_i \rangle u_i \right\|^2 \\ &= \left\| \alpha^T - ((\alpha, u_1), \dots, (\alpha, u_k)) \begin{pmatrix} u_1^T \\ \vdots \\ u_k^T \end{pmatrix} \right\|_F. \end{aligned}$$

从而

$$\sum_{i=1}^m (\text{dist}(\alpha_i, W))^2 = \left\| A - \begin{pmatrix} \langle \alpha_1, u_1 \rangle & \dots & \langle \alpha_1, u_k \rangle \\ \vdots & & \vdots \\ \langle \alpha_n, u_1 \rangle & \dots & \langle \alpha_n, u_k \rangle \end{pmatrix} \begin{pmatrix} u_1^T \\ \vdots \\ u_k^T \end{pmatrix} \right\|_F^2.$$

另一方面, 由于 $\alpha = \sum_{i=1}^n \langle \alpha, v_i \rangle v_i$, 故我们可以写成

$$\alpha^T = (\langle \alpha, v_1 \rangle, \dots, \langle \alpha, v_n \rangle) P,$$

其中 $P = (v_1, \dots, v_n)$, 从而

$$A = QDP^T,$$

其中 QD 的第 i 行为 $(\langle \alpha_i, v_1 \rangle, \dots, \langle \alpha_i, v_n \rangle)$, 所以

$$QD \begin{pmatrix} v_1^T \\ \vdots \\ v_k^T \\ 0 \\ \vdots \\ 0 \end{pmatrix} = A_k.$$

根据定理11.2可知 W_k 实现了 $\sum_{i=1}^m (\text{dist}(\alpha_i, W))^2$ 的最小值. \square

11.3.2 去中心化与主成分

在上面的例子中, 我们将数据矩阵 A 减去了行均值 μ 后再做奇异值分解. 这一步**去中心化** (centering) 操作在统计学中是自然的: 数据的均值 μ 反映的是“数据集中在哪里”, 而我们关心的是“数据如何散布”. 去掉均值后, 数据的散布完全由**协方差矩阵**

$$\Sigma = \frac{1}{m-1} B^T B$$

描述, 其中 $B = A - \bar{\mu}$ 是中心化后的数据矩阵. 如果 B 的奇异值分解为 $B = QDP^T$, 则

$$\Sigma = \frac{1}{m-1} P D^2 P^T,$$

即协方差矩阵的特征向量恰好是 B 的右奇异向量 v_1, \dots, v_n , 对应的特征值为 $\lambda_i = \sigma_i^2 / (m-1)$.

定义 11.1 (主成分). 设 $B = A - \bar{\mu}$ 是中心化后的 $m \times n$ 数据矩阵, $B = QDP^T$ 是其奇异值分解, $P = (v_1, \dots, v_n)$. 则称 v_i 为数据的**第 i 主成分方向** (the i -th principal component direction), $\sigma_i^2 / (m-1)$ 为第 i 主成分的**方差**. 称 $\sigma_i^2 / \sum_j \sigma_j^2$ 为第 i 主成分的**方差解释比** (variance explained ratio).

例 11.2 (二维数据的主成分). 考虑 $m = 20$ 个二维数据点 $\alpha_1, \dots, \alpha_{20} \in \mathbb{R}^2$ (例如, 某地 20 天的最高温度和日照时长). 将这些数据排成 20×2 矩阵 A , 减去均值 μ 得到中心化数据矩阵 $B = A - \bar{\mu}$. 对 B 做奇异值分解, 得到两个奇异值

$$\sigma_1 \approx 8.72, \quad \sigma_2 \approx 1.76.$$

对应的方差解释比为

$$\frac{\sigma_1^2}{\sigma_1^2 + \sigma_2^2} \approx 96.1\%, \quad \frac{\sigma_2^2}{\sigma_1^2 + \sigma_2^2} \approx 3.9\%.$$

这说明数据的变化几乎完全集中在第一主成分方向 v_1 上——数据点近似分布在一条过均值 μ 的直线上. 图 19 的左图显示了数据点 (蓝色)、两个主成分方向 v_1 (红色, 数据主要变化方向) 和 v_2 (橙色, 次要方向), 以及每个点到 v_1 方向的投影 (灰色虚线); 右图是“碎石图”(scree plot), 直观展示了各主成分解释的方差比例.

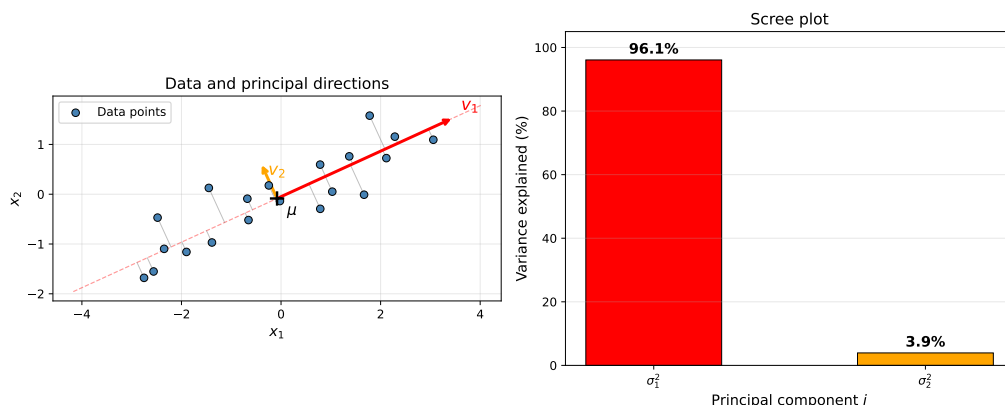


图 19: 二维数据的主成分分析. 左图: 数据散点与两个主成分方向 v_1, v_2 , 灰色线段为数据到第一主成分方向的投影残差. 右图: 碎石图, 第一主成分解释了 96.1% 的方差.

主成分分析的基本思路是: 若前 k 个主成分的方差解释比之和已经很接近 1, 则将 n 维数据投影到 k 维子空间 $\text{span}\{v_1, \dots, v_k\}$ 上, 就能用远少于 n 个坐标来近似表示原始数据, 同时保留绝大部分信息. 下面的命题说明, 经过去中心化后, 最佳的 k 维仿射拟合就是 $\mu + \text{span}\{v_1, \dots, v_k\}$. 为此我们先证明一个引理.

引理 11.4. 设 W 是 \mathbb{R}^n 的一个 k 维子空间, $\alpha_1, \dots, \alpha_m \in \mathbb{R}^n$. 在所有形如 $\beta + W$ ($\beta \in \mathbb{R}^n$) 的 k 维仿射子空间中, 使得

$$\sum_{i=1}^m \text{dist}(\alpha_i, \beta + W)^2$$

最小的平移向量为 $\beta = \text{Proj}_{W^\perp} \mu$, 其中 $\mu = \frac{1}{m} \sum_{i=1}^m \alpha_i$ 是数据的均值. 等价地, 最佳仿射子空间为 $\mu + W$.

证明. 注意到 $\text{dist}(\alpha_i, \beta + W) = \text{dist}(\alpha_i - \beta, W) = \|\text{Proj}_{W^\perp}(\alpha_i - \beta)\|$. 因此

$$\sum_{i=1}^m \text{dist}(\alpha_i, \beta + W)^2 = \sum_{i=1}^m \|\text{Proj}_{W^\perp}(\alpha_i - \beta)\|^2.$$

将 β 分解为 $\beta = \beta_W + \beta_{W^\perp}$, 其中 $\beta_W \in W, \beta_{W^\perp} \in W^\perp$, 则

$$\text{Proj}_{W^\perp}(\alpha_i - \beta) = \text{Proj}_{W^\perp} \alpha_i - \beta_{W^\perp}.$$

记 $\gamma_i = \text{Proj}_{W^\perp} \alpha_i \in W^\perp$, 上式变为

$$\sum_{i=1}^m \|\gamma_i - \beta_{W^\perp}\|^2.$$

这是 W^\perp 中 m 个点 $\gamma_1, \dots, \gamma_m$ 到定点 β_{W^\perp} 的距离平方和. 由初等不等式可知, 当 $\beta_{W^\perp} = \frac{1}{m} \sum_{i=1}^m \gamma_i = \text{Proj}_{W^\perp} \mu$ 时此式取最小值. 此时 $\beta + W = \text{Proj}_{W^\perp} \mu + W = \mu + W$ (因为 $\mu - \text{Proj}_{W^\perp} \mu = \text{Proj}_W \mu \in W$). \square

命题 11.2. 令 $\mu = \frac{1}{m} \sum_{i=1}^m (\alpha_i^T)$, 以及 $\bar{\mu} = (1, \dots, 1)^T \cdot \mu$. 对 $B = A - \bar{\mu}$ 做奇异值分解得到 $B = QDP^T$, 其中 $P = (v_1, \dots, v_n)$, 则

$$\mu + \text{span}_{\mathbb{R}}(v_1, \dots, v_k)$$

是 k 维仿射平面中与 $\alpha_1, \dots, \alpha_m$ 距离平方和最小的.

证明. 设 $\beta + W$ 是任意一个 k 维仿射子空间. 由引理 11.4, 对于固定的 W , 最佳平移 β 使得 $\beta + W = \mu + W$. 因此问题化为: 在所有 k 维子空间 W 中, 最小化

$$\sum_{i=1}^m \text{dist}(\alpha_i, \mu + W)^2 = \sum_{i=1}^m \text{dist}(\alpha_i - \mu, W)^2.$$

记 $\beta_i = \alpha_i - \mu$ 为中心化后的数据, 即矩阵 $B = A - \bar{\mu}$ 的第 i 行. 由命题 11.1, 使 $\sum_{i=1}^m \text{dist}(\beta_i, W)^2$ 最小的 k 维子空间恰好是 $W_k = \text{span}\{v_1, \dots, v_k\}$, 其中 v_1, \dots, v_k 是 B 的前 k 个右奇异向量. 因此最佳 k 维仿射子空间为 $\mu + W_k = \mu + \text{span}\{v_1, \dots, v_k\}$. \square

注 11.4 (历史注记). 主成分分析的思想最早可以追溯到 *Karl Pearson* 在 1901 年的工作¹⁰: 他从几何角度提出了“寻找与数据点距离平方和最小的直线 (或平面)”这一问题, 本质上就是上面的命题. 1933 年, *Harold Hotelling*¹¹ 从统计学角度重新发现了这一方法, 并正式引入了“主成分”(principal components) 这一术语, 将其与协方差矩阵的特征值问题联系起来. 主成分分析与奇异值分解之间的深层关系, 则是在此后数十年间逐渐被数学家和统计学家所认识和系统化的.

如今, 主成分分析已成为数据科学中最基础也最广泛使用的降维工具之一. 例如, *Turk* 和 *Pentland* 在 1991 年提出的“特征脸”(Eigenface)方法, 就是将 PCA 应用于人脸图像: 将每张 $m \times n$ 的人脸图片展平为一个 mn 维向量, 对大量人脸图片构成的数据矩阵做主成分分析, 前几个主成分方向 (即“特征脸”) 捕捉了人脸变化的主要模式 (如光照、表情、脸型等), 仅用 20–50 个主成分就能较好地重建任意一张人脸.

¹⁰K. Pearson, *On lines and planes of closest fit to systems of points in space*, Philosophical Magazine, 1901.

¹¹H. Hotelling, *Analysis of a complex of statistical variables into principal components*, Journal of Educational Psychology, 1933.

11.4 应用场景: 最小二乘法

11.4.1 历史背景

最小二乘法是数学史上最富传奇色彩的方法之一. 1801 年 1 月 1 日, 意大利天文学家皮亚齐(Giuseppe Piazzi) 在西西里岛发现了第一颗小行星谷神星(Ceres). 他在接下来 41 天里观测到谷神星在天球上的 24 个位置, 但此后谷神星运行到太阳背后, 消失在天文学家的视野中. 如何根据这 24 个观测数据预测谷神星再次出现时的位置? 这一挑战吸引了当时欧洲最杰出的数学家.

24 岁的高斯(Carl Friedrich Gauss) 利用他发明的最小二乘法, 成功预测了谷神星的轨道. 1801 年 12 月 31 日, 天文学家齐亚尼 (Franz Xaver von Zach) 在高斯预测的位置附近重新发现了谷神星, 与预测仅相差不到 1 度. 这一壮举使高斯一举成名.

高斯在 1809 年出版的天体运动论(*Theoria Motus Corporum Coelestium*) 中系统阐述了最小二乘法, 声称自己从 1795 年起就已经在使用这一方法. 然而, 法国数学家勒让德(Adrien-Marie Legendre) 在 1805 年的著作中率先公开发表了最小二乘法, 并给出了这一名称 (“méthode des moindres carrés”). 两人之间关于优先权的争论持续了多年, 但无论如何, 最小二乘法迅速成为科学中最基本的数据拟合工具.

11.4.2 问题的提出与几何解释

最小二乘法的核心问题可以描述如下: 假设我们有 n 个可控变量 a_1, \dots, a_n 和一个待预测的响应变量 y , 我们相信 y 与 a_i 之间存在近似的线性关系

$$y \approx x_1 a_1 + x_2 a_2 + \cdots + x_n a_n,$$

其中 x_1, \dots, x_n 是待确定的参数. 进行 m 次独立实验后, 我们得到 m 组数据 (α_i, b_i) ($i = 1, \dots, m$), 其中 $\alpha_i = (a_{i1}, \dots, a_{in})^T \in \mathbb{R}^n$ 是第 i 次实验的自变量取值, $b_i \in \mathbb{R}$ 是对应的观测值. 将所有数据写成矩阵形式:

$$\begin{pmatrix} \alpha_1^T \\ \alpha_2^T \\ \vdots \\ \alpha_m^T \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

即 $Ax = b$, 其中 $A \in M_{m \times n}(\mathbb{R})$, $b \in \mathbb{R}^m$.

当 $m \gg n$ 时 (实验次数远多于参数个数), 方程组 $Ax = b$ 通常是超定的 (overdetermined), 即无精确解. 此时我们退而求其次, 寻找使**残差平方和** (residual sum of squares)

$$\|Ax - b\|^2 = \sum_{i=1}^m (\alpha_i^T x - b_i)^2$$

最小的 x , 这就是**最小二乘问题**(least squares problem).

这个问题有一个优美的几何解释. 记 $W = \text{im } A$ 为 A 的列空间, 则当 x 取遍 \mathbb{R}^n 时, Ax 取遍 W . 因此最小二乘问题等价于: 在子空间 W 中找到与 b 距离最近的点. 由正交投影的理论 (命题 10.4), 这个最近点恰好是 b 在 W 上的正交投影 $\text{Proj}_W b$, 最小残差为

$$\|b - \text{Proj}_W b\|.$$

因此, 最小二乘解 \hat{x} 满足 $A\hat{x} = \text{Proj}_W b$, 等价于残差 $b - A\hat{x}$ 正交于 W 的每个向量, 即

$$A^T(A\hat{x} - b) = 0 \iff A^T A\hat{x} = A^T b.$$

上式称为**正规方程**(normal equation). 当 A 列满秩时, $A^T A$ 可逆, 最小二乘解唯一: $\hat{x} = (A^T A)^{-1} A^T b$. 当 A 不列满秩时, 解不唯一, 各解之间相差 $\ker A$ 中的元素. 通常我们要求在所有最小二乘解中选取范数最小的那个, 称为**最优最小二乘解**(minimum norm least squares solution).

11.4.3 伪逆与最小二乘定理

正规方程给出了最小二乘解的一种求法, 但当 $A^T A$ 不可逆 (即 A 不列满秩) 时就失效了. 奇异值分解提供了一种统一的、对任意矩阵都适用的方法. 给定矩阵 $A \in M_{m \times n}(\mathbb{R})$ 以及其奇异值分解

$$A = QDP^T,$$

其中

$$D = \begin{pmatrix} \sigma_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

令

$$A^\dagger = PD^\dagger Q^T,$$

其中

$$D^\dagger = \begin{pmatrix} \sigma_1^{-1} & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \sigma_2^{-1} & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r^{-1} & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}_{n \times m}.$$

矩阵 A^\dagger 称为 A 的 **Moore-Penrose 伪逆**(pseudoinverse). 则有如下定理:

定理 11.3 (最小二乘解). 对于 $Ax = b$, 则 $\hat{x} = A^\dagger b$ 是最优最小二乘解, 即在所有使 $\|Ax - b\|$ 最小的 x 中, \hat{x} 的范数最小.

证明. 首先证明 $A\hat{x} - b \perp \text{im } A$, 即验证

$$A^T(A(A^\dagger b) - b) = 0.$$

直接计算有

$$\begin{aligned} PD^T Q^T (QDP^T PD^\dagger Q^T - I_m)b &= (PD^T DD^\dagger Q^T - PD^T Q^T)b \\ &= (PD^T Q^T - PD^T Q^T)b \\ &= 0. \end{aligned}$$

再验证 $\ker A \perp A^\dagger b$: 由于 $\ker A = \ker(QDP^T) = \ker D$, 以及 $A^\dagger b = PD^\dagger Q^T b$, 即验证

$$D^\dagger Q^T b \perp \ker D,$$

而由 D 以及 D^\dagger 的表达式是显然的. □

注 11.5. 如果想用

$$y = x_1 a_1 + \cdots + x_n a_n + c$$

去拟合数据, 则考虑

$$\begin{pmatrix} \alpha_1^T, 1 \\ \alpha_2^T, 1 \\ \vdots \\ \alpha_m^T, 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ c \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

令

$$\tilde{A} = \begin{pmatrix} \alpha_1^T, 1 \\ \alpha_2^T, 1 \\ \vdots \\ \alpha_m^T, 1 \end{pmatrix},$$

考虑 \tilde{A}^i 即可.

11.4.4 例子: 直线拟合

例 11.3. 假设有 4 个数据点 $(1, 2), (2, 3), (3, 5), (4, 4)$, 我们希望找到一条直线 $y = kx + c$ 最好地拟合这些数据. 将数据写成矩阵形式

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{pmatrix}}_A \begin{pmatrix} k \\ c \end{pmatrix} = \underbrace{\begin{pmatrix} 2 \\ 3 \\ 5 \\ 4 \end{pmatrix}}_b.$$

此方程组无精确解. 由正规方程 $A^T A \hat{x} = A^T b$, 计算

$$A^T A = \begin{pmatrix} 30 & 10 \\ 10 & 4 \end{pmatrix}, \quad A^T b = \begin{pmatrix} 39 \\ 14 \end{pmatrix}.$$

解得 $\hat{x} = (A^T A)^{-1} A^T b$. 由 $\det(A^T A) = 120 - 100 = 20$, 有

$$(A^T A)^{-1} = \frac{1}{20} \begin{pmatrix} 4 & -10 \\ -10 & 30 \end{pmatrix},$$

从而

$$\hat{x} = \frac{1}{20} \begin{pmatrix} 4 & -10 \\ -10 & 30 \end{pmatrix} \begin{pmatrix} 39 \\ 14 \end{pmatrix} = \frac{1}{20} \begin{pmatrix} 16 \\ 30 \end{pmatrix} = \begin{pmatrix} 0.8 \\ 1.5 \end{pmatrix}.$$

因此最佳拟合直线为 $y = 0.8x + 1.5$. 四个数据点的预测值分别为 2.3, 3.1, 3.9, 4.7, 残差分别为 0.3, 0.1, -1.1, 0.7, 残差平方和为 $0.09 + 0.01 + 1.21 + 0.49 = 1.8$.

11.4.5 最小二乘与主成分分析的比较

最小二乘法 and 主成分分析 (PCA) 都是数据分析中最基本的工具, 它们的目标看似相似——“用低维结构拟合高维数据”——但在几何上有本质的区别.

注 11.6 (最小二乘与 PCA 的区别). 考虑平面上 m 个数据点 $(\alpha_1, b_1), \dots, (\alpha_m, b_m)$.

- (1) **最小二乘法**寻找直线 $y = kx + c$ 使得**竖直**方向的误差平方和 $\sum_i (k\alpha_i + c - b_i)^2$ 最小. 这里有一个不对称性: x 是自变量 (已知), y 是因变量 (待预测), 我们只度量 y 方向的偏差. 几何上, 最小二乘法最小化的是数据点到拟合直线的**竖直距离**的平方和.
- (2) **主成分分析**寻找通过数据中心的直线, 使得数据点到该直线的**正交距离** (即垂直距离) 的平方和最小. *PCA* 不区分自变量和因变量, 各坐标地位平等. 由命题 11.1, 这等价于最大化数据在该方向上的投影方差.

特别地, 当自变量和因变量的地位相同 (例如寻找数据的主要变化方向) 时, 应使用 *PCA*; 当目标是用一组已知变量预测另一个变量时, 应使用最小二乘回归.

尽管出发点不同, 两者在数学上有深刻的联系: 它们都可以通过奇异值分解来统一求解. 给定中心化的数据矩阵 A , *PCA* 提取的是 $A^T A$ 的特征向量 (主成分方向), 而最小二乘法利用的是 A 的伪逆 A^\dagger (通过奇异值的倒数构造). 可以说, *SVD* 为理解线性数据分析提供了一个统一的代数框架.

11.5 习题

11.5.1 练习题

习题 11.1 (一个几乎不用计算的 *SVD*). 设

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

1. 直接观察 A 把 \mathbb{R}^2 的单位圆映到 \mathbb{R}^3 中什么图形.
2. 写出 $A^T A$, 求其特征值.
3. 写出 A 的奇异值.
4. 给出一个 $A = U\Sigma V^T$ 的奇异值分解.

习题 11.2. 设 A 是可逆实方阵, 奇异值为 $\sigma_1, \dots, \sigma_n$. 求 A^{-1} 的奇异值.

习题 11.3 (极分解). (1) 陈述复矩阵的奇异值分解定理 (类似于实矩阵的版本).

- (2) 设 $A \in \text{GL}_n(\mathbb{C})$. 利用奇异值分解证明: 存在酉矩阵 $U \in \text{U}(n)$ 和正定厄米特矩阵 P , 使得 $A = UP$. 这称为 A 的**极分解** (*polar decomposition*).
- (3) 证明极分解的唯一性. (这说明 $\text{GL}_n(\mathbb{C})$ 同胚于 $\text{U}(n) \times \mathcal{H}_n^+$, 其中 \mathcal{H}_n^+ 是所有正定厄米特矩阵的集合.)

习题 11.4 (奇异值刻画正规矩阵). 设 A 是 n 阶复方阵, 奇异值为 $\sigma_1(A) \geq \cdots \geq \sigma_n(A) \geq 0$, 特征值为 $\lambda_1, \dots, \lambda_n$ (按代数重数计). 证明:

$$\sum_{i=1}^n \sigma_i(A)^2 \geq \sum_{i=1}^n |\lambda_i|^2,$$

等号成立当且仅当 A 是正规矩阵.

(提示: 先证任意复方阵可酉相似于上三角阵, 然后比较两边的 Frobenius 范数.)

习题 11.5. 设

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

直接写出 A 的奇异值, 并说明它对单位圆的拉伸效果.

习题 11.6. 计算

$$A^T A, \quad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

习题 11.7. 设

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

求 A 的秩和奇异值.

习题 11.8. 解释为什么奇异值一定是非负数. 请从 $A^T A$ 的特征值角度说明.

习题 11.9. 一个 3×2 矩阵 A 的奇异值为 5, 2. 求 $A^T A$ 的特征值.

习题 11.10. 给定矩阵

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

写出它的一个奇异值分解.

11.5.2 思考题

习题 11.11 (奇异值不等式). 设 A, B 是两个 $m \times n$ 实矩阵. 证明:

$$\sigma_{k+l-1}(A+B) \leq \sigma_k(A) + \sigma_l(B), \quad k+l-1 \leq \min(m, n).$$

习题 11.12 (奇异值-特征值乘积不等式). 设 A 是 n 阶复方阵, 特征值为 $\lambda_1, \dots, \lambda_n$ (按模从大到小排列), 奇异值为 $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_n \geq 0$. 证明对任意 $k = 1, \dots, n$:

$$|\lambda_1 \lambda_2 \cdots \lambda_k| \leq \sigma_1 \sigma_2 \cdots \sigma_k.$$

习题 11.13. 假设平面 \mathbb{R}^2 上有三个点的坐标为 $\alpha_1 = (1, 0)$, $\alpha_2 = (-1, -1)$, $\alpha_3 = (0, 1)$. 以 α_i 做成第 i 行的行向量的 3×2 矩阵记为 A .

- (1) 请写出矩阵 A 的一个奇异值分解.
- (2) 在标准内积和距离下, 找到平面上哪一条直线 (一维仿射空间) 到这三个点的距离平方之和最小.

习题 11.14. 对形如 $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ 的矩阵写下一个极分解.

习题 11.15. 证明第一个奇异值不等式, 假设 A 是 n -阶实方阵, 且有实特征值 λ , 证明 $\sigma_1(A) \geq |\lambda|$.

习题 11.16. 假设 A 是 n 阶实方阵. 判断题: 证明或举出反例.

- (1) n 阶方阵 A 为正交矩阵当且仅当它有 n 个奇异值, 值都是 1.
- (2) 如果 n 阶方阵有 n 个奇异值, 则所有奇异值的乘积等于所有特征值的模的乘积.
- (3) 假设 n 阶方阵 A 的奇异值分解为 $A = QDP^T$, 而 $A + I_n$ 的奇异值分解为 $A + I_n = Q(D + I_n)P^T$, 则 A 是对称矩阵.
- (4) 如果 n 阶方阵 A 的 n 个奇异值就是它的 n 个特征值的绝对值, 则 A 是否一定是对称矩阵?

习题 11.17. 请证明 $m \times n$ 实矩阵 A 的第 k 个奇异值的 *Min-Max* 描述.

$$\sigma_k = \min \{ \max \{ |A(x)| : x \perp W_k, |x| = 1 \} : W_k \subset V \text{ 子空间, } \dim W_k = k - 1 \}$$

这里先固定 $k - 1$ 维子空间 W_k , 取出对应的最大值 $\max \{ |A(x)| : x \perp W_k, |x| = 1 \}$. 然后让 W_k 取遍 $k - 1$ 维子空间, 取出这些值中的最小值.

证明实矩阵 A 的第 k 个奇异值的 *Max-Min* 描述.

$$\sigma_k = \max \{ \min \{ |A(x)| : x \in W_k, |x| = 1 \} : W_k \subset V \text{ 子空间, } \dim W_k = k \}$$

习题 11.18. 设 A 为 $m \times n$ 实矩阵, 则存在唯一的 $n \times m$ 实矩阵 A^\dagger , 满足以下条件: $AA^\dagger A = A$; $A^\dagger AA^\dagger = A^\dagger$; AA^\dagger 和 $A^\dagger A$ 都是实对称矩阵. 上述矩阵 A^\dagger 称为 A 的 *Moore-Penrose* 广义逆. 特别地, A 是方阵且可逆时, 这就是通常的逆矩阵.

习题 11.19 (Frobenius 范数与奇异值). 设 $A \in M_n(\mathbb{R})$, 奇异值为 $\sigma_1 \geq \cdots \geq \sigma_n \geq 0$.

1. 证明 $\|A\|_F^2 = \text{tr}(A^T A) = \sum_{i=1}^n \sigma_i^2$.

2. 证明奇异值 Weyl 不等式:

$$|\sigma_k(A) - \sigma_k(B)| \leq \|A - B\|,$$

其中右侧为算子范数。

习题 11.20 (条件数与最近奇异矩阵). 设 A 是 n 阶可逆实矩阵, 使用算子 2-范数定义条件数

$$\kappa(A) = \|A\| \cdot \|A^{-1}\|.$$

1. 证明 $\kappa(A) = \sigma_1(A)/\sigma_n(A)$ 。

2. 证明

$$\kappa(A)^{-1} = \min \left\{ \frac{\|A - B\|}{\|A\|} : B \text{ 是奇异矩阵} \right\}.$$

习题 11.21 (列 Gram 矩阵与左正交因子分解). 设 $A, B \in M_n(\mathbb{R})$. 证明以下两个条件等价:

1. $A^T A = B^T B$;

2. 存在正交矩阵 Q , 使得 $B = QA$ 。

复矩阵情形中, 把 \mathbb{R}, T 、正交矩阵分别改成 $\mathbb{C}, *$ 、酉矩阵, 结论仍然成立。

习题 11.22 (实正交投影差的秩公式). 设 $P, Q \in M_n(\mathbb{R})$ 是两个正交投影, 即

$$P^2 = P = P^T, \quad Q^2 = Q = Q^T.$$

证明:

$$\text{rank}(P - Q) = \text{rank}P + \text{rank}Q - 2 \dim(\text{im}(P) \cap \text{im}(Q)).$$

习题 11.23 (奇异值的最大最小伸缩). 在 \mathbb{R}^n 中, 记标准内积下向量 v 的长度为 $\|v\|$ 。设

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \\ 1 & -1 & -1 \end{bmatrix}.$$

1. 对 $x \in \mathbb{R}^3 \setminus \{0\}$, 求 $\|Ax\|/\|x\|$ 的最大可能值和最小可能值。

2. 求使得 $\|Ax\|/\|x\|$ 取到最大值的一个向量 x 。

习题 11.24 (显式奇异值分解). 设

$$A = \begin{bmatrix} 3 & -3 & 3 \\ -1 & 5 & -1 \end{bmatrix}.$$

求一个奇异值分解

$$A = UDV,$$

使得 U 为 2 阶正交矩阵, V 为 3 阶正交矩阵,

$$D = \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \sigma_2 & 0 \end{bmatrix}, \quad \sigma_1 \geq \sigma_2 > 0.$$

习题 11.25 (到酉群的最小秩距离). 设 $A \in M_n(\mathbb{C})$. 定义

$$d(A) = \min_{U \in U(n)} \text{rank}(A - U).$$

令 A 的奇异值为 $\sigma_1, \dots, \sigma_n$, 并记

$$p_+ = \#\{j : \sigma_j > 1\}, \quad p_- = \#\{j : \sigma_j < 1\}.$$

证明:

$$d(A) = \max\{p_+, p_-\}.$$

习题 11.26 (压缩算子的最小酉扩张维数). 设 $A \in M_n(\mathbb{C})$ 满足 $\|A\| \leq 1$. 称酉矩阵

$$W = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_{n+s}(\mathbb{C})$$

是 A 的酉扩张。证明: 存在这样的酉扩张当且仅当

$$s \geq \text{rank}(I - A^*A).$$

因此 A 的最小酉扩张维数为

$$n + \text{rank}(I - A^*A).$$

12 应用选读: Transformer: 从内积、矩阵乘法到语言生成

选学背景

本章展示线性代数在大语言模型中的用法, 其中训练梯度和反向传播需要微积分背景, 可作为进阶选读内容.

2017 年, Vaswani 等人在论文 *Attention Is All You Need* 中提出了 Transformer 架构. 此后, Transformer 成为自然语言处理、大语言模型、计算机视觉和科学计算中的重要基础模型之一. 从线性代数的角度看, Transformer 并不是一个完全陌生的对象: 它的核心计算反复使用我们已经学习过的标准基、矩阵乘法、内积、行随机矩阵、仿射变换、投影、矩阵分块和矩阵参数优化.

注 12.1 (本节与原始 Transformer 的关系). 原始 *Transformer* 论文主要为机器翻译提出了 *encoder-decoder* 架构; 现代大语言模型中常见的是只保留 *decoder* 侧思想的**因果语言模型**, 即每个位置只能使用它左边和当前位置的信息来预测下一个词元. 本节为了突出线性代数主线, 主要讲 *decoder-only / causal self-attention* 的核心计算.

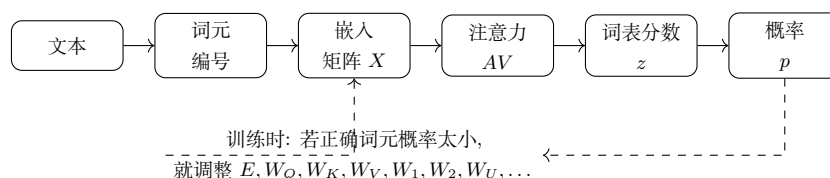
本节内容可分为两层. 第一层是不涉及微积分的“前向计算”:

文本 \rightarrow 词元编号 \rightarrow 向量矩阵 \rightarrow 注意力加权平均 \rightarrow 下一个词元概率.

第二层是训练时才需要的“参数学习”:

预测概率 \rightarrow 损失函数 \rightarrow 计算梯度 \rightarrow 更新参数矩阵.

初读时可先掌握第一层; 第二层可暂时理解为“参数矩阵通过训练逐步调整”.



我们不会讨论工程实现中的全部细节, 而是集中解释三个问题:

1. Transformer 怎样把一段文字表示成矩阵;
2. 注意力机制怎样用内积和矩阵乘法汇总上下文信息;
3. 语言模型怎样通过预测下一个词元来训练, 又怎样逐步生成文本.

12.1 Transformer 模型的训练过程概览

本节先从整体上说明 Transformer 模型是如何被训练成大语言模型的. 后面的小节再分别介绍其中涉及的线性代数结构.

大语言模型的训练首先需要大量文本数据. 原始文本不能直接输入模型, 而要先经过分词器切分成词元, 再把词元转换成编号序列, 构成词表, 其大小记为 m . 例如一段文本可以被表示为

$$i_1, i_2, \dots, i_n,$$

其中每个 i_t 是词表中的一个编号. 这些编号再通过嵌入矩阵变成向量, 从而得到输入矩阵

$$X \in M_{n \times d}(\mathbb{R}).$$

这里 n 是输入序列长度, d 是模型的隐藏维度, X 的第 t 行是词元 i_t 的表示向量. 因此, 在进入 Transformer 之后, 模型处理的对象已经不再是原始文字, 而是一个由词元向量排成的矩阵.

大语言模型最常见的预训练任务是预测下一个词元. 也就是说, 模型看到前面的词元

$$i_1, i_2, \dots, i_t,$$

要预测下一个词元 i_{t+1} 是什么. 例如给定句子前半部分

“小明把奖杯放进箱子, 因为它太”,

模型需要判断下一个词元更可能是“大”、“小”还是其他词元. 从数学上看, 模型最终会在整个词表上输出一个概率分布

$$p = (p_1, \dots, p_m),$$

其中 m 是词表大小, p_j 表示下一个词元是第 j 个词元的概率. 训练的目标就是让正确词元对应的概率尽可能大.

输入矩阵 X 会依次经过许多层 Transformer. 每一层大致由多头注意力、残差连接、层归一化和前馈网络组成. 多头注意力让每个位置根据上下文更新自己的表示; 前馈网络对每个位置的表示进一步做非线性变换; 残差连接帮助保留原有信息; 层归一化则使每一层的表示更加稳定. 经过多层叠加后, 第 t 个位置的向量不再只是第 t 个词元本身的表示, 而是融合了前后上下文信息的表示.

最后, 模型用某个位置的输出向量来预测下一个词元. 这个向量通常先经过一个线性变换, 从 d 维空间映射到 m 维空间:

$$\mathbb{R}^d \longrightarrow \mathbb{R}^m.$$

得到的 m 个数可以理解为模型给词表中每个词元打的分数. 这些分数通常称为 logits. 再经过 softmax 函数之后, 它们变成词表上的概率分布. 概率越大的词元, 模型认为越可能作为下一个词元出现.

训练时,模型的预测通常不会一开始就正确.因此需要定义损失函数来衡量预测结果和正确答案之间的差距.对下一个词元预测任务,常用的是交叉熵损失.它的基本作用是:如果模型给正确词元的概率很高,损失就小;如果模型给正确词元的概率很低,损失就大.然后通过反向传播计算各个参数应该如何调整,再用优化算法更新这些参数.

在 Transformer 中,需要学习的参数包括嵌入矩阵,注意力机制中的查询、键、值和输出矩阵,前馈网络中的权重矩阵和偏置向量,层归一化中的缩放和平移参数,以及最后把隐藏向量映射到词表概率分布的输出矩阵.因此,从线性代数角度看,训练过程就是不断调整一大批矩阵和向量,使模型在预测下一个词元时越来越准确.

整个预训练过程可以概括为

读入文本 \rightarrow 切分词元 \rightarrow 变成向量矩阵 \rightarrow 经过多层 Transformer
 \rightarrow 预测下一个词元 \rightarrow 计算损失 \rightarrow 更新参数.

这个过程在海量文本上反复进行.随着训练推进,模型逐渐学到词元之间的统计关系、语法结构、语义联系,以及更复杂的上下文模式.

所谓大模型,主要体现在三个方面.第一,模型参数很多,例如隐藏维度更大、层数更多、注意力头更多、前馈网络更宽.第二,训练数据很多,模型需要在大量文本上学习语言和知识结构.第三,训练计算量很大,通常需要大量专门的计算设备.因此,“大”不只是指词表大,更主要是指参数规模、数据规模和计算规模都很大.

预训练得到的模型本质上学会的是根据上下文续写文本.为了让它更适合回答问题、遵循指令和进行对话,通常还会进行后续训练,例如监督微调和偏好优化.监督微调用人工整理的问答或指令数据训练模型,使它学会按照任务要求作答;偏好优化则进一步让模型的回答更符合人类偏好.经过这些步骤后,预训练模型才逐渐变成我们熟悉的对话式大语言模型.

12.2 神经网络的基础结构

在机器学习中,一个模型可以看成带有许多可调参数的函数.在线性代数语言中,这些参数常常就是矩阵和向量中的元素.假设我们有一个输入数据矩阵

$$X = \begin{pmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_n^T \end{pmatrix} \in M_{n \times d}(\mathbb{R}),$$

最基本的一层神经网络常写成

$$Y = XW + \mathbf{1}b^T,$$

其中

$$W \in M_{d \times r}(\mathbb{R}), \quad b \in \mathbb{R}^r,$$

$\mathbf{1}$ 是长度为 n 的全 1 列向量. 第 i 行满足

$$y_i^T = x_i^T W + b^T.$$

也就是说, 每个输入向量先和若干权重向量做内积, 再加上偏置.

在实际的神经网络中, 通常还会对这些结果再施加一个非线性函数 ϕ , 得到

$$Z = \phi(Y) = \phi(XW + \mathbf{1}b^T).$$

这里的 ϕ 对矩阵中的每个分量分别作用. 对应到单个神经元, 就是

$$\text{输出} = \phi(x^T w + b),$$

也就是说, 单个神经元先计算一个线性表达式 $x^T w + b \in \mathbb{R}$, 再通过非线性函数 ϕ 得到最终输出. 这个非线性步骤是神经网络能够表示复杂函数的关键; 如果没有非线性函数, 多层线性变换复合起来仍然只是一个线性变换.

注 12.2 (非线性函数的作用). 如果连续做两层但不加非线性函数, 那么

$$(XW_1 + \mathbf{1}b_1^T)W_2 + \mathbf{1}b_2^T = X(W_1W_2) + \mathbf{1}(b_1^T W_2 + b_2^T),$$

仍然只是一个仿射变换. 换句话说, 多层仿射变换的复合仍等价于一层仿射变换. 为了让模型表达更复杂的关系, 需要在矩阵乘法之间加入非线性函数, 例如

$$\text{ReLU}(x) = \max\{0, x\}.$$

对矩阵使用 ReLU 时, 通常是对每个元素分别作用.

训练神经网络可以粗略看成如下循环:

输入 → 前向计算 → 预测 → 计算损失 → 调整参数 → 更新模型.

在 Transformer 中, 嵌入矩阵 E , 注意力中的 W_Q, W_K, W_V, W_O , 前馈网络中的 W_1, W_2 , 输出层中的 W_U , 都属于可以训练的参数矩阵.

神经网络说法	线性代数写法	直观含义
权重	矩阵 W 或向量 w	可调的系数
偏置	向量 b	整体平移或默认倾向
一层网络	$XW + \mathbf{1}b^T$	批量做内积与加权求和
激活函数	ϕ	加入非线性, 避免多层塌缩
训练	更新 W, b 等参数	提高正确答案概率

12.3 注意力机制：从整句编码到选择性读取

早期处理句子的模型常采用递推方式：从左到右逐个词元更新状态。这样做有一个直观问题：如果一个词需要参考很远处的信息，那么信息要经过很多步才能传递到当前位置，中间过程越长，信息越容易衰减。

注意力机制换了一种思路：在更新某个位置时，不必只依赖上一步传来的信息，而是直接给序列中每个位置分配一个权重，再做加权平均。也就是说，第 i 个位置需要确定：

第 $1, 2, \dots, n$ 个位置中哪些对当前位置最有参考价值？

这些权重排成矩阵 $A = (a_{ij})$ 。第 i 行就是第 i 个位置看向所有位置的权重：

$$\tilde{x}_i = \sum_{j=1}^n a_{ij} v_j, \quad a_{ij} \geq 0, \quad \sum_{j=1}^n a_{ij} = 1.$$

因此在 Transformer 中，注意力指的是

根据相关程度，对若干值向量做加权平均。

例 12.1 (一句话中的“它”)。考虑句子：

“小明把奖杯放进箱子，因为它太大了。”

这里“它”究竟更像指“奖杯”还是“箱子”，需要参考前面的词。注意力矩阵中，“它”所在那一行可以理解为：这个位置在更新自己的表示时，分别给“小明”“奖杯”“箱子”等位置多少权重。

注意：这只是一个帮助理解的图像。真实模型中的每一层、每一个注意力头都有自己的注意力权重；这些权重可以画成热力图，并反映某些词之间的信息交互强弱，但不能简单等同于模型做出判断的全部理由。

12.4 从词元到矩阵：语言如何进入向量空间

计算机不能直接处理自然语言中的汉字、单词或标点。在输入模型之前，一段文本首先要被切分成若干个词元。词元可以是一个字、一个词、一个词的一部分，也可以是标点或特殊符号。

设词表大小为 m 。词表可以理解为一个固定的编号表：

$$1, 2, \dots, m.$$

每个编号对应一个词元。例如，第 i 个编号对应第 i 个词元。在通常的训练过程中，词表本身是固定的：哪些词元被收入词表，以及它们的编号，一般不会随着训练改变。

为了把词元输入模型, 我们可以先用标准基向量表示它. 对 $1 \leq i \leq m$, 令

$$e_i = (0, \dots, 0, 1, 0, \dots, 0)^T \in \mathbb{R}^m,$$

其中只有第 i 个分量为 1, 其余分量为 0. 这称为第 i 个词元的 **one-hot 表示**. 它也是一个特殊的概率向量: 所有分量非负, 分量和为 1, 并且全部概率集中在第 i 个位置. 更一般地, 词表上的一个概率分布可以写成

$$p = (p_1, \dots, p_m)^T,$$

其中

$$p_r \geq 0, \quad \sum_{r=1}^m p_r = 1.$$

如果输入序列对应的词元编号为

$$i_1, i_2, \dots, i_n,$$

则它的 one-hot 矩阵为

$$O = \begin{pmatrix} e_{i_1}^T \\ e_{i_2}^T \\ \vdots \\ e_{i_n}^T \end{pmatrix} \in M_{n \times m}(\mathbb{R}).$$

这里 n 是输入序列的长度, 而 m 是词表大小.

one-hot 向量虽然简单, 但维度 m 很高, 也没有直接反映词元之间的语义关系. 因此模型引入一个**嵌入矩阵**

$$E \in M_{m \times d}(\mathbb{R}),$$

其中 d 称为**嵌入维度**, 通常远小于 m . 矩阵 E 的第 i 行

$$e_i^T E \in \mathbb{R}^d$$

就是第 i 个词元的嵌入向量. 因此, 嵌入矩阵可以看成一张“词元向量表”: 每一行对应词表中的一个词元, 每个词元被表示成一个 d 维行向量.

需要注意的是, 词表的大小 m 以及词元编号通常是固定的, 但嵌入矩阵 E 中的元素是模型参数, 会在训练过程中不断调整. 换句话说, 词表记录“有哪些词元”, 而嵌入矩阵记录“每个词元当前对应什么向量”.

整个输入序列经过嵌入层后得到

$$X = OE = \begin{pmatrix} e_{i_1}^T E \\ e_{i_2}^T E \\ \vdots \\ e_{i_n}^T E \end{pmatrix} \in M_{n \times d}(\mathbb{R}).$$

也就是说, 输入序列中的每个词元都被替换成一个 d 维行向量, 然后按照原来的顺序排成一个 $n \times d$ 矩阵. 经过嵌入层之后, 模型处理的对象不再是原始文字, 而是矩阵 X . 第 t 行 x_t^T 表示第 t 个词元的向量表示.

注 12.3. 从线性代数角度看, 嵌入层就是矩阵乘法. *one-hot* 向量 e_i 是标准基向量, 映射

$$e_i^T \mapsto e_i^T E$$

正好取出了矩阵 E 的第 i 行. 因此, 所谓“查表取词向量”, 本质上就是一次特殊的矩阵乘法.

注 12.4 (词元不一定等于一个字或一个词). 为了让词表大小可控, 实际系统常把文字切成介于“字符”和“词”之间的小片段. 例如一个英文长词可能被切成若干子词, 中文标点、空格、数字也可能成为词元. 本节为了突出线性代数结构, 把词元简化看成已经编号的基本单位.

12.5 位置编码: 矩阵的行还需要顺序信息

矩阵 X 的第 t 行记录第 t 个词元的内容, 但是如果只使用这些内容向量, 模型本身并不知道这一行处在序列中的第几个位置. 自然语言中顺序非常重要: “狗咬人”和“人咬狗”包含同样的词元, 但意思完全不同.

因此, Transformer 通常会在输入嵌入上加入**位置编码**. 设

$$P = \begin{pmatrix} p_1^T \\ p_2^T \\ \vdots \\ p_n^T \end{pmatrix} \in M_{n \times d}(\mathbb{R})$$

是位置编码矩阵, 其中 $p_t \in \mathbb{R}^d$ 表示第 t 个位置的信息. 模型真正输入的矩阵常写为

$$X = OE + P.$$

位置编码可以是固定的, 也可以和嵌入矩阵一样通过训练得到.

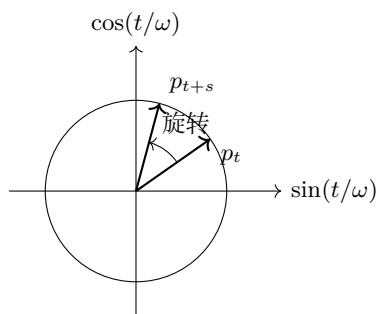
一个经典的固定位置编码使用正弦和余弦函数. 当 d 为偶数时, 可令

$$\text{PE}(t, 2r) = \sin\left(\frac{t}{10000^{2r/d}}\right), \quad \text{PE}(t, 2r+1) = \cos\left(\frac{t}{10000^{2r/d}}\right),$$

其中 $r = 0, 1, \dots, d/2 - 1$. 这种写法看似来自三角函数, 其实也有清楚的线性代数解释. 对固定的频率参数 ω , 有

$$\begin{pmatrix} \sin \frac{t+s}{\omega} \\ \cos \frac{t+s}{\omega} \end{pmatrix} = \begin{pmatrix} \cos \frac{s}{\omega} & \sin \frac{s}{\omega} \\ -\sin \frac{s}{\omega} & \cos \frac{s}{\omega} \end{pmatrix} \begin{pmatrix} \sin \frac{t}{\omega} \\ \cos \frac{t}{\omega} \end{pmatrix}.$$

也就是说, 位置从 t 平移到 $t + s$, 在每个二维频率平面中对应一个正交矩阵. 因此, 正弦位置编码把“相对位移”转化成了若干二维平面中的旋转.



在每个二维频率平面中, 位置平移对应一个旋转矩阵

注 12.5. 如果没有位置编码, 自注意力层对输入行的排列具有等变性: 同时重排输入矩阵的各行, 输出也会以同样方式重排. 这对集合数据是合理的, 但对文本序列不够. 位置编码正是为了打破这种“只看集合、不看顺序”的缺陷.

12.6 从格拉姆矩阵到注意力: 内积一次性计算所有相似度

回顾内积空间中的基本事实: 对标准内积,

$$\langle u, v \rangle = u^T v.$$

当 u 和 v 都是单位向量时, $u^T v = \cos \theta$, 其中 θ 是两者夹角. 因此, 内积可以用来衡量两个向量方向上的相似程度.

设

$$X = \begin{pmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_n^T \end{pmatrix} \in M_{n \times d}(\mathbb{R}).$$

矩阵

$$X X^T = (\langle x_i, x_j \rangle)_{1 \leq i, j \leq n}$$

一次性记录了所有词元两两之间的内积. 这正是向量组 x_1, \dots, x_n 的**格拉姆矩阵**. 如果第 i 行与第 j 行内积较大, 我们可以理解为第 i 个位置与第 j 个位置在当前表示空间中比较相关.

注意力机制的朴素想法是: 更新第 i 个词元的表示时, 不应该只看它自己, 还应该按相关程度参考其他词元. 因此, 我们希望构造权重 a_{ij} , 使得

$$\tilde{x}_i = \sum_{j=1}^n a_{ij} x_j,$$

其中

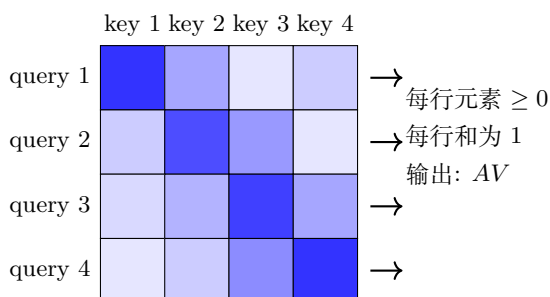
$$a_{ij} \geq 0, \quad \sum_{j=1}^n a_{ij} = 1.$$

于是 \tilde{x}_i 是 x_1, \dots, x_n 的凸组合. 写成矩阵形式, 若 $A = (a_{ij}) \in M_n(\mathbb{R})$, 则

$$\tilde{X} = AX.$$

矩阵 A 的每一行都是概率向量时, 称 A 为**行随机矩阵** (row-stochastic matrix). 注意力矩阵是一个行随机矩阵. 这给出本节最重要的线性代数图像之一:

注意力输出 = 注意力矩阵 \times 值向量矩阵.



注意力矩阵 $A = (a_{ij})$: 第 i 行表示第 i 个位置看向各位置的权重

这里值向量矩阵 $V = XW_V$ 是由 X 出发, 通过一个可训练的权重矩阵 W_V 得到, 后面的小节会更详细地介绍.

12.7 Softmax: 把分数矩阵变成行随机矩阵

内积可以给出相似度分数, 但这些分数可能为负, 也不一定和为 1. 为了把分数转化为权重, Transformer 使用 **softmax 映射**.

定义 12.1 (softmax). 对 $z = (z_1, \dots, z_n)^T \in \mathbb{R}^n$, 定义

$$\text{softmax}(z)_j = \frac{e^{z_j}}{\sum_{r=1}^n e^{z_r}}, \quad j = 1, \dots, n.$$

显然

$$\text{softmax}(z)_j > 0, \quad \sum_{j=1}^n \text{softmax}(z)_j = 1.$$

因此 softmax 把任意实向量变成概率向量.

例 12.2 (softmax 像把分数变成投票比例). 设三个候选词元的分数为

$$z = (2, 1, 0)^T.$$

则

$$\text{softmax}(z) = \frac{(e^2, e, 1)^T}{e^2 + e + 1}.$$

它的三个分量都是正数, 且和为 1, 所以可以看成三个候选词元的概率. 由于

$$e^2 > e > 1,$$

第一个候选的概率最大, 第二个次之, 第三个最小.

直观地说, *softmax* 做了两件事: 先用指数函数把“大分数更大、小分数更小”的差距拉开, 再除以总和, 把结果归一化成概率.

注 12.6 (计算 softmax 时可以整体平移). 对任意常数 c , 有

$$\text{softmax}(z + c\mathbf{1}) = \text{softmax}(z).$$

因此实际计算时常把所有分数同时减去最大值, 以避免 e^x 太大造成数值溢出. 这不改变最后的概率分布.

对矩阵 $S = (s_{ij}) \in M_n(\mathbb{R})$, 我们可以逐行施加 softmax, 定义 **rowsoftmax**

$$\text{rowsoftmax}(S)_{ij} = \frac{e^{s_{ij}}}{\sum_{r=1}^n e^{s_{ir}}}.$$

于是

$$A = \text{rowsoftmax}(S)$$

是一个行随机矩阵, 即每一行的元素均为正且和为 1.

例 12.3 (两个词元). 设

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

即两个词元向量分别是二维标准基. 此时 $XX^T = I_2$, 表示每个词元与自己内积为 1, 与另一个词元内积为 0. 对每一行做 *softmax* 得到

$$A = \text{rowsoftmax}(I_2) = \begin{pmatrix} \frac{e}{e+1} & \frac{1}{e+1} \\ \frac{1}{e+1} & \frac{e}{e+1} \end{pmatrix}.$$

于是

$$AX = \begin{pmatrix} \frac{e}{e+1} & \frac{1}{e+1} \\ \frac{1}{e+1} & \frac{e}{e+1} \end{pmatrix}.$$

这说明第一个词元的新表示主要保留自己, 同时少量参考第二个词元; 第二个词元也同理. 真实 *Transformer* 只是把这种“按相似度加权平均”推广到更高维、更长序列和可训练的 Q - K - V 向量空间.

命题 12.1. 若 $A = \text{rowsoftmax}(S)$, 则对任意 i, j ,

$$a_{ij} > 0,$$

且对任意 i ,

$$\sum_{j=1}^n a_{ij} = 1.$$

因此 AX 的第 i 行是 X 的各行的凸组合.

softmax 不是线性映射. 它的作用是把相似度分数变成可解释的权重分布: 分数越大的位置获得越大的权重, 但所有权重仍然归一化为和为 1.

12.8 查询、键、值向量: 为什么不是直接使用 XX^T

如果直接用 XX^T 计算相似度, 那么每个词元在“寻找信息”和“提供信息”时使用的是同一个向量 x_i . 实际上, 一个词元在不同角色下需要呈现不同特征. 例如, 在句子中某个词可能用某些特征去寻找修饰它的词, 又用另一些特征向其他词提供语义信息.

因此, *Transformer* 为每个输入向量构造三个向量:

- **查询向量** (query vector): 表示当前位置想寻找什么信息;
- **键向量** (key vector): 表示当前位置提供给别人匹配的索引特征;
- **值向量** (value vector): 表示当前位置真正传递出去的信息.

图书馆类比

可以把注意力想成一次“软检索”. 查询向量像读者的问题: “我现在想找什么信息?” 键向量像每本书贴在书脊上的索引标签: “我能被什么问题找到?” 值向量像书中的真正内容: “如果你选中了我, 我要贡献什么信息?”

第 i 个位置的查询向量与第 j 个位置的键向量做内积, 得到匹配分数 $q_i^T k_j$; softmax 把这些分数变成权重; 最后对值向量做加权平均. 这里的“软”表示不是只选一本书, 而是按权重同时参考多本书.

在线性代数中, 这三个向量由三个线性变换给出. 设

$$W_Q \in M_{d \times d_k}(\mathbb{R}), \quad W_K \in M_{d \times d_k}(\mathbb{R}), \quad W_V \in M_{d \times d_v}(\mathbb{R}).$$

定义

$$Q = XW_Q, \quad K = XW_K, \quad V = XW_V.$$

其中

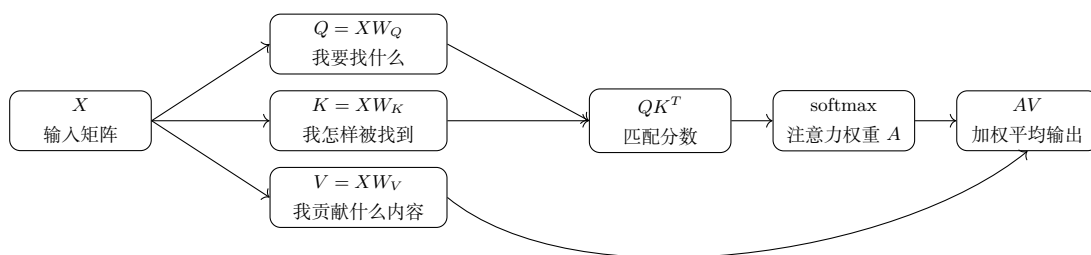
$$Q, K \in M_{n \times d_k}(\mathbb{R}), \quad V \in M_{n \times d_v}(\mathbb{R}).$$

第 i 行 q_i^T 是第 i 个位置的查询向量, 第 j 行 k_j^T 是第 j 个位置的键向量. 二者的内积

$$q_i^T k_j$$

表示第 i 个位置对第 j 个位置的匹配分数. 所有匹配分数同时组成矩阵

$$QK^T = (q_i^T k_j)_{1 \leq i, j \leq n}.$$



定义 12.2. 给定 Q, K, V , 定义注意力输出为

$$\text{Attention}(Q, K, V) = \text{rowsoftmax} \left(\frac{QK^T}{\sqrt{d_k}} \right) V.$$

这里 $\sqrt{d_k}$ 称为缩放因子.

缩放因子 $\sqrt{d_k}$ 的作用是控制内积的大小. 当 d_k 较大时, 未缩放的内积可能变得很大, 从而使 softmax 过于接近某个坐标为 1、其他坐标为 0 的极端分布. 除以 $\sqrt{d_k}$ 后, 分数的尺度更稳定.

注 12.7 (低秩结构). 由于

$$\text{rank}(QK^T) \leq \min\{\text{rank}(Q), \text{rank}(K)\} \leq d_k,$$

softmax 之前的打分矩阵 QK^T 具有低秩约束. 但是 softmax 是非线性映射, 一般不保持矩阵秩. 因此不能简单说“注意力矩阵一定低秩”. 更准确的说法是: 注意力的打分矩阵来自低维投影后的双线性相似度.

12.9 因果遮罩：训练时如何避免使用未来信息

大语言模型通常是自回归模型(autoregressive model): 它根据前面的词元预测下一个词元. 在预测第 $t + 1$ 个词元时, 模型只能使用

$$i_1, i_2, \dots, i_t,$$

不能使用未来的 i_{t+1}, i_{t+2}, \dots . 在矩阵计算中, 这一限制由**因果遮罩**(causal mask) 实现.

位置 t	模型允许看到	要预测的下一个词元
1	i_1	i_2
2	i_1, i_2	i_3
3	i_1, i_2, i_3	i_4
\vdots	\vdots	\vdots

设注意力分数矩阵为

$$S = \frac{QK^T}{\sqrt{d_k}}.$$

定义遮罩矩阵 $M = (m_{ij})$ 为

$$m_{ij} = \begin{cases} 0, & j \leq i, \\ -\infty, & j > i. \end{cases}$$

然后计算

$$A = \text{rowsoftmax}(S + M).$$

因为 $e^{-\infty} = 0$, 所以当 $j > i$ 时,

$$a_{ij} = 0.$$

于是第 i 个位置只能关注第 $1, 2, \dots, i$ 个位置. 从矩阵结构上看, 因果注意力矩阵是下三角形的行随机矩阵.

	$j = 1$	$j = 2$	$j = 3$	$j = 4$	$j = 5$
$i = 1$	0	$-\infty$	$-\infty$	$-\infty$	$-\infty$
$i = 2$	0	0	$-\infty$	$-\infty$	$-\infty$
$i = 3$	0	0	0	$-\infty$	$-\infty$
$i = 4$	0	0	0	0	$-\infty$
$i = 5$	0	0	0	0	0

绿色: 允许看自己和过去; 红色: 未来位置被遮住

注 12.8. 训练时可以把整段文本同时放进模型并行计算, 但因果遮罩保证每个位置只使用它左侧和当前位置的信息. 因此, 并行训练并不意味着模型使用了待预测位置之后的信息.

12.10 多头注意力

单个注意力头只能使用一组 W_Q, W_K, W_V 来计算一种匹配关系. 但语言中的关系是多样的: 有的头可能关注主语和谓语, 有的头可能关注代词和先行词, 有的头可能关注相邻位置或标点. 多头注意力用多组线性映射并行计算这些关系.

设共有 h 个头. 第 r 个头有参数

$$W_Q^{(r)}, \quad W_K^{(r)}, \quad W_V^{(r)}, \quad r = 1, \dots, h.$$

它的输出为

$$H_r = \text{Attention}(XW_Q^{(r)}, XW_K^{(r)}, XW_V^{(r)}).$$

然后把各个头的输出按列拼接:

$$H = \text{Concat}(H_1, \dots, H_h),$$

这一步只是把不同注意力头提取到的信息并排放在一起. 为了让这些信息相互混合, 并把维度变回模型后续层所需要的大小, 还要再乘以一个可训练的输出矩阵 W_O 得到多头注意力输出:

$$\text{MHA}(X) = HW_O.$$

这里 MHA 是 multi-head attention 的缩写.

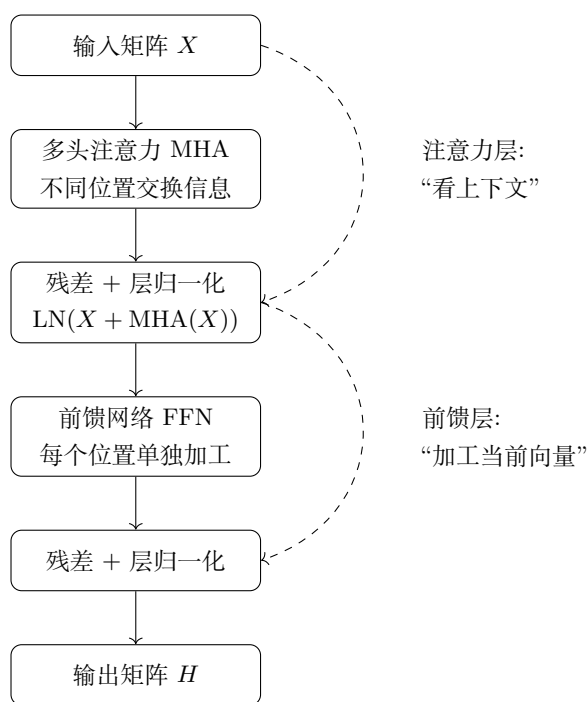
从线性代数角度看, 每个头都先把输入矩阵 X 投影到自己的 Q-K-V 表示空间, 在该空间中计算出注意力输出, 最后再把多个头的信息融合.

12.11 Transformer 块: 残差连接、层归一化和前馈网络

实际模型会把注意力层和前馈网络层堆叠起来. 一个 Transformer 块可以粗略分成两步:

1. **注意力层:** 让不同位置的词元向量彼此交换信息;
2. **前馈网络层:** 对每个位置的向量单独做一次非线性加工.

注意力层负责“看上下文”, 前馈网络层负责“加工当前位置的表示”. 残差连接和层归一化则帮助多层堆叠时保持信息稳定.



一个常见的 Transformer 块可以抽象写成

$$Y = \text{LN}(X + \text{MHA}(X)),$$

$$H = \text{LN}(Y + \text{FFN}(Y)).$$

这里 LN 表示层归一化(layer normalization), FFN 表示逐位置前馈网络(feed-forward network). 下面我们来逐一介绍.

12.11.1 残差连接

在多头注意力之后, Transformer 通常不会直接把 $\text{MHA}(X)$ 作为下一步的输入, 而是把原来的输入 X 加回去, 得到

$$X + \text{MHA}(X).$$

这种结构称为**残差连接**(residual connection).

这里要求 X 和 $\text{MHA}(X)$ 具有相同的形状. 例如若 $X \in M_{n \times d}(\mathbb{R})$, 则多头注意力输出通常也被设计成 $\text{MHA}(X) \in M_{n \times d}(\mathbb{R})$, 于是二者可以逐项相加.

残差连接的直观含义是: 一层网络不必从零开始重新构造一个表示, 而只需要学习如何修正原来的表示. 如果把 $\text{MHA}(X)$ 看成模型从上下文中提取出的新信息, 那么 $X + \text{MHA}(X)$ 就是在保留原有表示 X 的基础上, 加入一个由注意力机制学到的修正项.

换句话说, 这一层学习的不是一个完全新的映射, 而更像是学习一个扰动项 $F(X)$. 当 $F(X)$ 较小时, 输出的 $X + F(X)$ 仍然接近原来的 X ; 当模型认为需要较大修改时, $F(X)$ 可以提供额外的信息.

从深层网络的角度看, 残差连接的一个重要作用是让信息更容易在多层之间保留下来. 如果没有残差连接, 每一层都会把输入完全变换成新的输出, 再交给下一层. 当网络层数很深时, 原来的信息需要连续经过许多次变换, 可能在这个过程中被逐渐削弱或改变.

有了残差连接后, 每一层的输出不只是子层计算出的新信息, 还包含原来的输入. 也就是说, 这一层并不是完全抛弃旧表示, 再重新生成一个新表示, 而是在旧表示的基础上加上一些新的修正. 如果某一层暂时没有学到很有用的变换, 它仍然可以让原来的信息大致传递下去.

反向传播时也有类似现象. 训练深层网络需要把误差信息从后面的层传回前面的层. 如果没有残差连接, 误差信息必须连续穿过许多复杂变换, 可能逐渐变弱, 这就是所谓梯度衰减的问题. 残差连接提供了一条更直接的传递路径, 使误差信息更容易传回前面的层. 因此, 残差连接可以理解为给每一层保留了一条“直通路”. 正向传播时, 原有信息可以更容易保留下来; 反向传播时, 梯度也更容易传回去. 这就是残差连接有助于训练深层网络的原因.

在 Transformer 中, 残差连接不仅用于多头注意力层, 也用于后面的前馈神经网络层. 典型结构可以写成

$$X \mapsto X + \text{MHA}(X),$$

以及

$$Y \mapsto Y + \text{FFN}(Y).$$

也就是说, 每个主要子层都被看成是在当前表示上添加一个可学习的修正项.

12.11.2 前馈网络

前馈网络对矩阵的每一行施加同一个非线性映射. 若 $Y \in M_{n \times d}(\mathbb{R})$, 一个典型前馈网络为

$$\text{FFN}(Y) = \phi(YW_1 + \mathbf{1}b_1^T)W_2 + \mathbf{1}b_2^T.$$

其中 $W_1 \in M_{d \times d_{\text{ff}}}(\mathbb{R})$, $b_1 \in \mathbb{R}^{d_{\text{ff}}}$, $W_2 \in M_{d_{\text{ff}} \times d}(\mathbb{R})$, $b_2 \in \mathbb{R}^d$. 这些 W_1, W_2, b_1, b_2 都是需要通过训练学习的参数.

这里 $\mathbf{1}$ 是长度为 n 的全 1 列向量, 用来把偏置向量加到每一行上; ϕ 是逐坐标作用的非线性函数, 例如 ReLU. 从维度上看, $YW_1 + \mathbf{1}b_1^T \in M_{n \times d_{\text{ff}}}(\mathbb{R})$, 经过 ϕ 后维度不变, 再乘以 W_2 并加上 b_2 , 最终输出仍属于 $M_{n \times d}(\mathbb{R})$.

因此, 前馈网络可以看成先把每个 d 维表示映射到较高维的 d_{ff} 维空间, 在那里施加非线性变换, 再映射回 d 维空间. 如果没有非线性函数 ϕ , 这两次仿射变换合在一起仍然只是一次仿射变换; 正是非线性函数使模型能够表达更复杂的非线性关系.

12.11.3 层归一化

对矩阵中的一行, 我们写成行向量 h^T , 其中 $h \in \mathbb{R}^d$ 是对应的列向量. 它的均值为

$$\mu = \frac{1}{d} \mathbf{1}^T h.$$

中心化就是从每个坐标中减去这个均值, 得到

$$h - \mu \mathbf{1}.$$

中心化后的向量各坐标的平均值为 0.

层归一化对矩阵的每一行独立进行这样的处理. 它先减去这一行的均值, 再除以这一行的标准差 (即平方和开方), 使得每一行都被调整到均值为 0、标准差为 1 的尺度上.

最后, 模型还会引入两个可训练参数

$$\gamma, \beta \in \mathbb{R}^d.$$

其中 γ 用来逐坐标缩放, β 用来逐坐标平移. 对单行来说, 层归一化的输出可以写成

$$\gamma \odot \frac{h - \mu \mathbf{1}}{\sigma} + \beta,$$

其中 σ 是 $h - \mu \mathbf{1}$ 的标准差, \odot 表示逐坐标相乘.

因此, 层归一化可以理解为按行进行的中心化、标准化、再缩放和平移的组合. 中心化使每一行的平均值变为 0, 标准化控制这一行的尺度; 而可训练的 γ 和 β 则允许模型在归一化之后重新调整每个坐标的大小和位置.

12.12 输出层: 隐藏向量如何变成下一个词元概率

经过 L 个 Transformer 块后, 模型得到隐藏状态矩阵

$$H = X^{(L)} \in M_{n \times d}(\mathbb{R}).$$

为了预测下一个词元, 模型要把每个隐藏向量映射到词表空间. 设词表大小为 m , 则需要一个可训练的输出矩阵

$$W_U \in M_{d \times m}(\mathbb{R}),$$

和偏置向量 $b_U \in \mathbb{R}^m$, 从而可定义 logits 矩阵

$$Z = HW_U + \mathbf{1}b_U^T \in M_{n \times m}(\mathbb{R}).$$

第 t 行 z_t^T 给出了第 t 个位置对词表中 m 个词元的未归一化分数. 对第 t 行做 softmax, 得到概率向量

$$p_t = \text{softmax}(z_t).$$

其中 $p_{t,r}$ 表示模型认为“第 t 个位置之后的下一个词元是第 r 个词元”的概率。

设 H 的第 t 行是 h_t^T , W_U 的第 r 列为 u_r . 则 Z 的第 t 行、第 r 列的元素是

$$z_{t,r} = h_t^T u_r + b_{U,r}.$$

也就是说, 模型把当前上下文向量 h_t 与每个候选词元对应的输出向量 u_r 做内积, 再通过 softmax 变成整个词表上的一个概率分布.

12.13 训练: 从下一个词元预测到矩阵参数优化

12.13.1 训练主线: 带监督的下一个词元预测

例 12.4 (由一句话形成多个预测任务). 设词元序列为

$$(i_1, i_2, i_3, i_4) = (\text{我}, \text{爱}, \text{线性}, \text{代数}).$$

训练因果语言模型时, 可以形成三个预测任务:

位置	已知内容	正确下一个词元
1	我	爱
2	我, 爱	线性
3	我, 爱, 线性	代数

模型不是一次性记忆整句, 而是在每个位置上学习给真实的下一个词元更高概率.

设训练文本对应的词元序列为

$$i_1, i_2, \dots, i_T.$$

因果语言模型的训练任务是: 在已经看到前文

$$i_1, i_2, \dots, i_t$$

的情况下, 预测下一个词元

$$i_{t+1}.$$

因此, 第 t 个位置的输出并不是用来预测当前位置的词元 i_t , 而是用来预测下一个词元 i_{t+1} . 换句话说, 输入和标签在位置上错开一位. 这里的标签是指训练时模型应该预测出的正确答案.

如果把

$$i_1, i_2, \dots, i_{T-1}$$

作为输入序列, 那么对应的标签序列就是

$$i_2, i_3, \dots, i_T.$$

也就是说, 输入中的 i_t 对应的训练目标是标签中的 i_{t+1} . 这种做法常称为**标签移位**(shifted labels).

例如, 若训练文本为

“我爱线性代数”,

则模型看到“我”时预测“爱”, 看到“我爱”时预测“线性”, 看到“我爱线性”时预测“代数”. 训练时, 模型实际上是在序列的每个位置同时学习这样的下一个词元预测任务.

因此, 一段长度为 T 的文本并不只提供一次训练样本, 而是几乎每个位置都提供一次下一个词元预测任务. 在 Transformer 中, 这些位置上的预测可以在一次前向传播中同时完成; 因果注意力遮罩保证第 t 个位置只能使用 i_1, \dots, i_t 的信息, 而不能提前看到后面的词元.

12.13.2 交叉熵损失

设模型在第 t 个位置输出概率向量 $p_t \in \mathbb{R}^m$, 正确答案是 $r_t = i_{t+1}$. 用 one-hot 向量

$$y_t = e_{r_t}$$

表示正确标签. 交叉熵损失定义为

$$\ell_t = - \sum_{r=1}^m y_{t,r} \log p_{t,r} = - \log p_{t,r_t}.$$

整个序列上的平均损失为

$$\mathcal{L} = \frac{1}{T-1} \sum_{t=1}^{T-1} \ell_t.$$

因此, 最小化交叉熵就是让模型分配给正确下一个词元的概率尽可能大.

12.13.3 进阶选读: 输出层梯度的矩阵形式

进阶阅读提示

下面的梯度公式说明参数更新的计算来源. 它需要多元微积分和链式法则. 初读时可先理解为: 损失越大, 说明模型给正确词元的概率太小; 训练算法会据此调整参数矩阵, 使后续预测更接近正确答案.

模型在每个位置都会输出一个词表上的概率分布. 设第 t 个位置的预测概率向量为

$$p_t = (p_{t,1}, p_{t,2}, \dots, p_{t,m})^T \in \mathbb{R}^m,$$

其中 $p_{t,j}$ 表示模型认为下一个词元是词表中第 j 个词元的概率. 把所有位置的预测概率按

行排成矩阵, 得到

$$P = \begin{pmatrix} p_1^T \\ p_2^T \\ \vdots \\ p_{T-1}^T \end{pmatrix} \in M_{(T-1) \times m}(\mathbb{R}).$$

对应地, 每个位置也有一个正确答案. 如果第 t 个位置的正确下一个词元是第 k_t 个词元, 那么它的标签可以写成 one-hot 向量 $y_t = e_{k_t} \in \mathbb{R}^m$. 把所有位置的 one-hot 标签按行排成矩阵, 得到

$$Y = \begin{pmatrix} y_1^T \\ y_2^T \\ \vdots \\ y_{T-1}^T \end{pmatrix} \in M_{(T-1) \times m}(\mathbb{R}).$$

因此, P 和 Y 具有相同的形状. 第 t 行的 p_t^T 是模型给出的概率分布, 第 t 行的 y_t^T 是正确答案对应的 one-hot 分布.

设模型最后一层在 softmax 之前输出的打分矩阵为

$$Z \in M_{(T-1) \times m}(\mathbb{R}).$$

它的第 t 行记为 z_t^T , 其中

$$z_t = (z_{t,1}, z_{t,2}, \dots, z_{t,m})^T.$$

第 j 个分量 $z_{t,j}$ 是模型在位置 t 给词表中第 j 个词元的原始打分. 对 z_t 施加 softmax 后得到

$$p_{t,j} = \frac{e^{z_{t,j}}}{\sum_{r=1}^m e^{z_{t,r}}}, \quad j = 1, \dots, m.$$

先看单个位置 t 的损失. 因为正确答案是第 k_t 个词元, 所以 one-hot 标签 y_t 只有第 k_t 个分量等于 1. 该位置的交叉熵损失为

$$\ell_t = - \sum_{j=1}^m y_{t,j} \log p_{t,j} = - \log p_{t,k_t}.$$

将 softmax 展开, 得到

$$\ell_t = - \log \frac{e^{z_{t,k_t}}}{\sum_{r=1}^m e^{z_{t,r}}} = -z_{t,k_t} + \log \left(\sum_{r=1}^m e^{z_{t,r}} \right).$$

现在对任意一个打分 $z_{t,j}$ 求偏导. 第一项 $-z_{t,k_t}$ 的偏导为 $-y_{t,j}$; 第二项的偏导为

$$\frac{e^{z_{t,j}}}{\sum_{r=1}^m e^{z_{t,r}}} = p_{t,j}.$$

因此

$$\frac{\partial \ell_t}{\partial z_{t,j}} = p_{t,j} - y_{t,j}.$$

把所有 $j = 1, \dots, m$ 合在一起, 就得到单个位置上的向量公式

$$\frac{\partial \ell_t}{\partial z_t} = p_t - y_t.$$

总损失取所有位置的平均交叉熵:

$$\mathcal{L} = \frac{1}{T-1} \sum_{t=1}^{T-1} \ell_t = -\frac{1}{T-1} \sum_{t=1}^{T-1} \sum_{j=1}^m y_{t,j} \log p_{t,j}.$$

由于每一行 z_t^T 只影响对应位置的损失 ℓ_t , 上面的单位位置公式可以逐行使用. 再加上平均因子 $\frac{1}{T-1}$, 得到矩阵形式

$$\frac{\partial \mathcal{L}}{\partial Z} = \frac{1}{T-1} (P - Y).$$

这个公式的含义很直观. 在第 t 个位置, 若 j 不是正确词元, 则 $y_{t,j} = 0$, 梯度分量为 $p_{t,j} > 0$; 梯度下降会降低这些错误词元的打分. 若 $j = k_t$ 是正确词元, 则 $y_{t,j} = 1$, 梯度分量为 $p_{t,j} - 1 < 0$; 梯度下降会提高正确词元的打分. 因此, 参数更新会推动预测分布 p_t 向正确的 one-hot 分布 y_t 靠近.

现在设最后的输出层为

$$Z = HW_U + \mathbf{1}b_U^T.$$

这里 $H \in M_{(T-1) \times d}(\mathbb{R})$ 是 Transformer 最后一层给出的隐藏表示, $W_U \in M_{d \times m}(\mathbb{R})$ 是把隐藏向量映射到词表打分的输出矩阵, $b_U \in \mathbb{R}^m$ 是输出偏置, $\mathbf{1}$ 是长度为 $T-1$ 的全 1 列向量. 其中 W_U 和 b_U 都是需要学习的参数.

记

$$G = \frac{\partial \mathcal{L}}{\partial Z}.$$

由于 $Z = HW_U + \mathbf{1}b_U^T$, 矩阵求导给出

$$\frac{\partial \mathcal{L}}{\partial W_U} = H^T G, \quad \frac{\partial \mathcal{L}}{\partial b_U} = G^T \mathbf{1}.$$

也就是

$$\frac{\partial \mathcal{L}}{\partial W_U} = H^T \frac{\partial \mathcal{L}}{\partial Z}, \quad \frac{\partial \mathcal{L}}{\partial b_U} = \left(\frac{\partial \mathcal{L}}{\partial Z} \right)^T \mathbf{1}.$$

第一个公式表示: 输出矩阵 W_U 的梯度由隐藏表示 H 和输出误差 G 相乘得到. 第二个公式表示: 偏置 b_U 的梯度就是把所有位置上的输出误差沿着序列方向加起来.

更一般地, Transformer 中的其他参数也都通过类似方式获得梯度. 关键原则是: 只要一个参数参与了前向计算, 并且前向计算的结果最终影响损失函数, 那么反向传播就可以通过链式法则计算出损失函数对这个参数的梯度.

先看一个最基本的线性层. 若

$$U = XW + \mathbf{1}b^T,$$

并且已经从后面的网络得到

$$G = \frac{\partial \mathcal{L}}{\partial U},$$

则矩阵求导给出

$$\frac{\partial \mathcal{L}}{\partial W} = X^T G, \quad \frac{\partial \mathcal{L}}{\partial b} = G^T \mathbf{1}, \quad \frac{\partial \mathcal{L}}{\partial X} = GW^T.$$

前两个公式说明 W 和 b 可以被更新; 第三个公式说明误差信息还可以继续向前传给 X . 因此, 一个线性层不仅能更新自己的参数, 也能把梯度继续传递给更早的层.

例如输出层

$$Z = HW_U + \mathbf{1}b_U^T$$

就是这种形式. 若记

$$G_Z = \frac{\partial \mathcal{L}}{\partial Z},$$

则

$$\frac{\partial \mathcal{L}}{\partial W_U} = H^T G_Z, \quad \frac{\partial \mathcal{L}}{\partial b_U} = G_Z^T \mathbf{1}.$$

同时, 梯度还会传回隐藏表示 H :

$$\frac{\partial \mathcal{L}}{\partial H} = G_Z W_U^T.$$

这一步很重要: 它说明损失函数不仅能更新最后的输出矩阵 W_U , 还会把误差信息继续传回 Transformer 的内部层.

前馈网络中的参数也是如此. 设

$$\text{FFN}(Y) = \phi(YW_1 + \mathbf{1}b_1^T)W_2 + \mathbf{1}b_2^T.$$

令 $S = YW_1 + \mathbf{1}b_1^T$, $R = \phi(S)$, 则前馈网络可以分成

$$S = YW_1 + \mathbf{1}b_1^T, \quad R = \phi(S), \quad U = RW_2 + \mathbf{1}b_2^T.$$

如果从后面传回来的梯度是 $G_U = \partial \mathcal{L} / \partial U$, 那么先由最后一个线性层得到

$$\frac{\partial \mathcal{L}}{\partial W_2} = R^T G_U, \quad \frac{\partial \mathcal{L}}{\partial b_2} = G_U^T \mathbf{1}.$$

再把梯度传回 R , 经过非线性函数 ϕ 后, 又能得到对 S 的梯度. 记这个梯度为 $G_S = \partial \mathcal{L} / \partial S$, 则第一层线性变换给出

$$\frac{\partial \mathcal{L}}{\partial W_1} = Y^T G_S, \quad \frac{\partial \mathcal{L}}{\partial b_1} = G_S^T \mathbf{1}.$$

因此, 前馈网络中的 W_1, W_2, b_1, b_2 都能通过反向传播得到梯度.

注意力层中的参数也类似. 为了说明主要结构, 先看单个注意力头. 它先由输入矩阵 X 生成查询、键和值矩阵:

$$Q = XW_Q, \quad K = XW_K, \quad V = XW_V.$$

然后用 Q 和 K 计算注意力权重, 再对 V 做加权平均. 简化地写,

$$A = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right), \quad O = AV.$$

如果后面的网络传回了对 O 的梯度, 那么由于 $O = AV$, 梯度会分别传给 A 和 V . 其中传给 V 的部分再经过

$$V = XW_V$$

给出 W_V 的梯度. 同理, 传给 A 的梯度会经过 softmax 传给

$$\frac{QK^T}{\sqrt{d_k}},$$

再分别传给 Q 和 K . 由于

$$Q = XW_Q, \quad K = XW_K,$$

于是也得到 W_Q 和 W_K 的梯度.

更具体地说, 若记 $G_Q = \partial\mathcal{L}/\partial Q$, $G_K = \partial\mathcal{L}/\partial K$, $G_V = \partial\mathcal{L}/\partial V$, 则由线性层求导公式得到

$$\frac{\partial\mathcal{L}}{\partial W_Q} = X^T G_Q, \quad \frac{\partial\mathcal{L}}{\partial W_K} = X^T G_K, \quad \frac{\partial\mathcal{L}}{\partial W_V} = X^T G_V.$$

多头注意力只是把这个过程对每个头分别做一遍. 各个头的输出拼接后再乘以输出矩阵 W_O , 所以 W_O 也通过同样的线性层求导公式获得梯度.

嵌入矩阵 E 也可以这样理解. 输入的 one-hot 矩阵为 O , 嵌入层输出为

$$X = OE.$$

如果从后面的 Transformer 层传回

$$G_X = \frac{\partial\mathcal{L}}{\partial X},$$

那么

$$\frac{\partial\mathcal{L}}{\partial E} = O^T G_X.$$

由于 O 的每一行都是 one-hot 向量, 这个公式的含义很直观: 某个词元在训练文本中出现时, 它对应的嵌入向量那一行就会收到梯度并被更新. 没有在当前批次中出现的词元, 对应行在这一步通常不会更新, 但在后续包含该词元的数据中仍然可以被更新.

层归一化中的参数 γ, β 也是可训练参数. 层归一化对每一行先做归一化, 再逐坐标乘以 γ 、加上 β . 因此, 后面传回来的梯度可以直接计算出每个坐标上应该如何调整 γ 和 β .

综上, 训练并不是只更新最后的输出矩阵 W_U . 损失函数先给出对输出打分 Z 的梯度, 然后这个梯度沿着计算图逐层向前传播. 每当遇到一个由可训练矩阵或向量参与的运算, 就用链式法则计算该参数的梯度. 因此,

$$E, W_Q, W_K, W_V, W_O, W_1, W_2, W_U, \dots$$

这些参数都可以被优化. 实际训练时, 梯度下降及其变体会反复执行类似

$$\theta \mapsto \theta - \eta \frac{\partial \mathcal{L}}{\partial \theta}$$

的更新, 其中 θ 表示任意一个可训练参数, η 是学习率. 通过大量文本上的反复更新, 模型逐渐调整这些矩阵和向量, 使正确词元的概率越来越大.

注 12.9. 最小二乘法通过最小化平方误差来拟合线性模型; 语言模型训练通过最小化交叉熵来拟合下一个词元的概率分布. 二者的损失函数不同, 但共同点是: 都是在参数空间中寻找使损失函数尽可能小的参数.

12.14 生成: 模型如何一个词元一个词元输出文本

训练完成后, 给定提示词序列

$$i_1, i_2, \dots, i_n,$$

模型计算最后一个位置的概率分布

$$p_n = \text{softmax}(z_n).$$

然后从这个分布中选择下一个词元 i_{n+1} , 再把它接回原序列:

$$i_1, i_2, \dots, i_n, i_{n+1}.$$

重复这一过程, 就得到一段文本. 这就是**自回归生成**. 从概率论角度看, 模型把一个序列的概率分解为

$$\mathbb{P}(i_1, \dots, i_T) = \prod_{t=1}^{T-1} \mathbb{P}(i_{t+1} | i_1, \dots, i_t).$$

从概率分布中选择词元可以有不同方式:

- **贪心选择:** 每次选概率最大的词元;
- **温度采样:** 使用 $\text{softmax}(z/\tau)$, 其中 $\tau > 0$ 控制分布的尖锐程度;
- **top- k 采样:** 只在概率最大的 k 个词元中重新归一化并采样;
- **top- p 采样:** 选择累计概率达到 p 的一小组词元, 再在其中采样.

这些策略不改变 Transformer 的矩阵计算本质, 只是改变从概率分布中选取下一个词元的规则.

12.15 KV 缓存: 自回归生成中的矩阵分块复用

在训练时, 模型可以同时处理一整段序列. 但在生成时, 词元必须一个一个产生. 如果每生成一个新词元都重新计算所有历史词元的键向量和值向量, 会造成大量重复计算.

注意到在第 $n+1$ 步生成时, 旧词元的键向量和值向量不会改变. 因此可以把它们缓存起来. 对某一层某一头, 假设已经有

$$K_{1:n} = \begin{pmatrix} k_1^T \\ \vdots \\ k_n^T \end{pmatrix}, \quad V_{1:n} = \begin{pmatrix} v_1^T \\ \vdots \\ v_n^T \end{pmatrix}.$$

新词元到来后, 只需计算

$$q_{n+1}, \quad k_{n+1}, \quad v_{n+1},$$

并把新的键向量和值向量追加为

$$K_{1:n+1} = \begin{pmatrix} K_{1:n} \\ k_{n+1}^T \end{pmatrix}, \quad V_{1:n+1} = \begin{pmatrix} V_{1:n} \\ v_{n+1}^T \end{pmatrix}.$$

新位置的注意力输出为

$$a_{n+1} = \text{softmax} \left(\frac{q_{n+1}^T K_{1:n+1}^T}{\sqrt{d_k}} \right),$$

$$o_{n+1} = a_{n+1} V_{1:n+1}.$$

KV 缓存的本质是矩阵分块和矩阵行的复用: 已经计算过的块保留下来, 新一步只追加新行.

例 12.5 (只检查矩阵大小). 设词表大小 $m = 6$, 序列长度 $n = 4$, 嵌入维度 $d = 5$, 注意力头维度 $d_k = 3, d_v = 5$. 则

$$O \in M_{4 \times 6}(\mathbb{R}), \quad E \in M_{6 \times 5}(\mathbb{R}),$$

所以

$$X = OE \in M_{4 \times 5}(\mathbb{R}).$$

若

$$W_Q, W_K \in M_{5 \times 3}(\mathbb{R}), \quad W_V \in M_{5 \times 5}(\mathbb{R}),$$

则

$$Q, K \in M_{4 \times 3}(\mathbb{R}), \quad V \in M_{4 \times 5}(\mathbb{R}).$$

于是

$$QK^T \in M_{4 \times 4}(\mathbb{R}), \quad A = \text{rowsoftmax}(QK^T/\sqrt{3}) \in M_{4 \times 4}(\mathbb{R}),$$

并且

$$AV \in M_{4 \times 5}(\mathbb{R}).$$

注意力输出仍然有 4 行, 因为序列长度没有改变; 仍然有 5 列, 是因为每个词元的表示维度仍为 5.

12.16 一个小型语言模型的完整数学流程

我们用一个只看矩阵形状的小例子串起整章. 设词表大小 $m = 5$, 嵌入维度 $d = 3$, 序列长度 $n = 4$, 输入词元为

$$(2, 4, 1, 3).$$

对应 one-hot 矩阵为

$$O = \begin{pmatrix} e_2^T \\ e_4^T \\ e_1^T \\ e_3^T \end{pmatrix} \in M_{4 \times 5}(\mathbb{R}).$$

若嵌入矩阵 $E \in M_{5 \times 3}(\mathbb{R})$, 位置编码矩阵 $P \in M_{4 \times 3}(\mathbb{R})$, 则

$$X = OE + P \in M_{4 \times 3}(\mathbb{R}).$$

设单头注意力中 $d_k = 2, d_v = 3$, 则

$$W_Q, W_K \in M_{3 \times 2}(\mathbb{R}), \quad W_V \in M_{3 \times 3}(\mathbb{R}),$$

$$Q = XW_Q \in M_{4 \times 2}(\mathbb{R}), \quad K = XW_K \in M_{4 \times 2}(\mathbb{R}), \quad V = XW_V \in M_{4 \times 3}(\mathbb{R}).$$

分数矩阵为

$$S = \frac{QK^T}{\sqrt{2}} \in M_4(\mathbb{R}).$$

若使用因果遮罩, 则

$$A = \text{rowsoftmax}(S + M)$$

是一个下三角行随机矩阵. 注意力输出为

$$AV \in M_{4 \times 3}(\mathbb{R}).$$

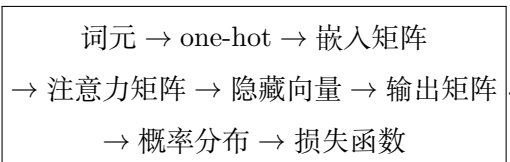
经过若干 Transformer 块后得到隐藏矩阵 $H \in M_{4 \times 3}(\mathbb{R})$. 输出矩阵 $W_U \in M_{3 \times 5}(\mathbb{R})$ 给出

$$Z = HW_U + \mathbf{1}b_U^T \in M_{4 \times 5}(\mathbb{R}).$$

第 t 行 softmax 后得到 $p_t \in \mathbb{R}^5$, 表示词表中五个词元分别作为下一个词元的概率. 如果第 t 个位置的正确答案是 r_t , 则该位置损失为

$$\ell_t = -\log p_{t,r_t}.$$

整个过程可以概括为



12.17 Transformer 模型的主要特点

Transformer 之所以在自然语言处理中非常有效,一个重要原因是它改变了模型处理序列的方式. 在较早的循环神经网络中,文本通常要按照从左到右的顺序逐步处理. 第 t 个位置的表示依赖于前一个位置传来的隐藏状态. 这种结构很自然,但也有明显限制:信息需要一步一步向后传递,距离较远的词元之间不容易直接建立联系;同时,由于后一步依赖前一步,训练和计算也不容易充分并行.

Transformer 的核心机制是自注意力. 在自注意力中,每个位置都可以直接参考序列中的其他位置. 例如理解一个代词时,模型可以直接关注它前面可能作为先行词的词元;理解一个动词时,模型也可以关注与它相关的主语、宾语或修饰成分. 这种机制使得远距离词元之间可以在同一层中发生直接的信息交互,不必完全依靠逐步传递.

与卷积神经网络相比,Transformer 的注意力关系也更加灵活. 卷积通常在固定大小的局部窗口中提取信息,要捕捉远距离关系往往需要堆叠许多层. 而注意力机制不是预先规定只看附近几个位置,而是根据当前输入动态地决定每个位置应该关注哪些位置. 因此,Transformer 更适合处理自然语言中复杂而多变的依赖关系.

多头注意力进一步增强了这种能力. 一个注意力头只能学习一种匹配方式,而语言中的关系有很多种:有的关系来自语法结构,有的关系来自指代,有的关系来自相邻词元,有的关系来自整句的语义. 多头注意力让模型可以用多组不同的线性变换同时观察同一段文本,从而在不同表示空间中捕捉不同类型的关系.

Transformer 的另一个重要优点是容易扩大规模. 它主要由矩阵乘法、逐坐标非线性函数、归一化和 softmax 等运算组成. 这些运算非常适合在现代计算设备上并行执行. 因此,当数据量、参数量和计算资源增加时,Transformer 可以比较自然地扩展成更深、更宽的模型. 这也是它能够训练出大语言模型的重要原因之一.

从表示学习的角度看,Transformer 的每一层都在不断更新词元表示. 初始时,每个词元只有自己的嵌入向量;经过多层自注意力和前馈网络之后,每个位置的向量逐渐融合上下文信息. 因而同一个词元在不同句子中可以获得不同的表示. 例如“苹果”在水果语境和科技公司语境中,经过上下文更新后可以对应不同的向量表示.

残差连接和层归一化也使深层 Transformer 更容易训练. 残差连接帮助原有信息在多层之间保留下来,层归一化则让每一层的数值尺度更加稳定. 这些结构本身不直接产生语言理解能力,但它们使得模型可以堆叠很多层,从而获得更强的表达能力.

概括来说,Transformer 的主要特点有以下几方面:

- 通过自注意力机制,不同位置之间可以直接交换信息;
- 通过多头注意力,模型可以同时捕捉多种不同类型的关系;
- 通过矩阵化计算,训练过程更容易并行化;
- 通过残差连接和层归一化,深层模型更容易优化;

- 通过大规模预训练, 模型可以从海量文本中学习语言规律和知识结构.

当然, Transformer 并不是在所有方面都没有代价. 标准自注意力需要比较序列中所有位置之间的关系, 因而当序列很长时, 计算量和显存开销会明显增加. 但在自然语言建模中, 它在表达能力、并行计算和规模扩展之间取得了非常好的平衡, 因此成为现代大语言模型的基础结构.

基础版总结

如果暂时不讨论微积分和训练细节, 本节的核心可以概括为四点:

1. 文本先被切成词元, 每个词元变成一个向量, 整段文本变成一个矩阵 X ;
2. QK^T 用矩阵乘法一次性计算所有位置之间的匹配分数;
3. softmax 把每一行分数变成概率权重, 注意力输出 AV 是 value 向量的加权平均;
4. 输出层把隐藏向量变成词表上的概率分布, 模型据此预测下一个词元.

因此, Transformer 的核心计算可以理解为若干线性代数对象的组合: 矩阵乘法、内积、行随机矩阵、仿射变换、分块矩阵和参数优化.

12.18 习题

12.18.1 练习题

习题 12.1 (词元与词表). 设词表为

{我, 爱, 线性, 代数, 。}.

若按这个顺序编号为 1, 2, 3, 4, 5, 写出词元“线性”和“。”的 *one-hot* 向量.

习题 12.2 (从编号到矩阵). 设输入词元编号为 (2, 4, 1), 词表大小为 5. 写出对应的 *one-hot* 矩阵 $O \in M_{3 \times 5}(\mathbb{R})$.

习题 12.3 (嵌入就是取行). 设

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 1 \\ -1 & 3 \end{pmatrix}.$$

求 $(0, 0, 1, 0)E$, 并说明它取出了 E 的哪一行.

习题 12.4. 设词表中有 4 个词, 词“线性”的 *one-hot* 行向量为

$$e_2^T = (0, 1, 0, 0).$$

若嵌入矩阵 E 是 4×3 矩阵, 说明 $e_2^T E$ 表示什么. 若 E 的第二行为 $(2, -1, 3)$, 求 $e_2^T E$.

习题 12.5. 一个序列长度为 5, 每个词元的向量维度为 8. 若把整个序列记为矩阵 X , 写出 X 的大小. 若线性层矩阵 W 为 8×6 , 写出 XW 的大小.

习题 12.6 (注意力机制中的矩阵形状). 设序列长度为 $n = 4$, 嵌入维度为 $d = 6$, 单头注意力中 $d_k = d_v = 3$. 令输入矩阵 $X \in \mathbb{R}^{4 \times 6}$, 权重矩阵

$$W_Q, W_K \in \mathbb{R}^{6 \times 3}, \quad W_V \in \mathbb{R}^{6 \times 3}.$$

1. 写出 $Q = XW_Q$ 、 $K = XW_K$ 、 $V = XW_V$ 的矩阵大小.
2. 写出打分矩阵 QK^T 的大小.
3. *softmax* 后得到的注意力矩阵每一行为什么可以看作概率分布?
4. 最终输出 $\text{softmax}(QK^T/\sqrt{d_k})V$ 的大小是多少?

习题 12.7 (形状检查). 设 $X \in M_{5 \times 8}(\mathbb{R})$, $W_Q, W_K \in M_{8 \times 3}(\mathbb{R})$, $W_V \in M_{8 \times 6}(\mathbb{R})$. 写出 $Q = XW_Q$ 、 $K = XW_K$ 、 $V = XW_V$ 、 QK^T 和 $\text{rowsoftmax}(QK^T)V$ 的大小.

习题 12.8. 设

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

计算 QK^T , 并说明每个元素可以看成哪两个向量的相似度.

习题 12.9. 对分数 $(2, 1, 0)$ 计算 *softmax* 的形式:

$$\frac{(e^2, e^1, e^0)}{e^2 + e^1 + e^0}.$$

不必求小数值, 只需说明三个权重的大小顺序.

习题 12.10 (注意力权重是否合法). 判断下列向量能否作为某一行注意力权重, 并说明理由:

$$(0.2, 0.3, 0.5), \quad (1, -1, 1), \quad (0.4, 0.4, 0.4), \quad (0, 0.7, 0.3).$$

习题 12.11 (加权平均). 设注意力权重为 $(0.1, 0.6, 0.3)$, 三个 *value* 向量为

$$v_1 = (1, 0), \quad v_2 = (0, 1), \quad v_3 = (2, 2).$$

求输出向量 $0.1v_1 + 0.6v_2 + 0.3v_3$.

习题 12.12 (看懂注意力矩阵). 设

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0.2 & 0.8 & 0 \\ 0.1 & 0.3 & 0.6 \end{pmatrix}.$$

证明 A 是行随机矩阵. 解释第 3 行 $(0.1, 0.3, 0.6)$ 的含义.

习题 12.13 (因果遮罩). 写出长度为 4 的因果遮罩矩阵 $M = (m_{ij})$, 其中 $j \leq i$ 时 $m_{ij} = 0$, $j > i$ 时 $m_{ij} = -\infty$. 哪些位置被禁止关注?

习题 12.14. 证明对任意 $z \in \mathbb{R}^n$, 向量 $\text{softmax}(z)$ 的所有分量均为正且和为 1.

习题 12.15. 设 $S \in M_n(\mathbb{R})$, $A = \text{rowsoftmax}(S)$. 证明 A 是行随机矩阵, 并证明 AX 的每一行都是 X 各行的凸组合.

习题 12.16. 设因果遮罩矩阵 M 满足 $m_{ij} = 0$ 当 $j \leq i$, $m_{ij} = -\infty$ 当 $j > i$. 证明

$$\text{rowsoftmax}(S + M)_{ij} = 0, \quad j > i.$$

12.18.2 思考题

习题 12.17 (Q/K/V 类比). 用“图书馆检索”的类比解释查询、键、值向量三者的不同作用. 为什么值向量不一定要和键向量是同一个?

习题 12.18 (注意力不是简单复制). 若某一行注意力权重为 $(0, 1, 0)$, 输出只复制第二个值向量. 若权重为 $(0.2, 0.5, 0.3)$, 输出是什么类型的向量? 这两种情况有什么不同?

习题 12.19 (多头注意力的直觉). 一个句子中可能同时存在“相邻词关系”“主谓关系”“代词指代关系”. 解释为什么多个注意力头可能比单个注意力头更灵活.

习题 12.20 (训练与生成的区别). 训练时, 模型可以对一句话中的许多位置同时计算损失; 生成时, 模型必须一个词元一个词元地追加. 解释这两种说法如何同时成立.

习题 12.21 (softmax 平移不变性). 证明对任意 $z \in \mathbb{R}^n$ 和常数 $c \in \mathbb{R}$, 有

$$\text{softmax}(z + c\mathbf{1}) = \text{softmax}(z).$$

这个性质为什么有助于数值计算?

习题 12.22 (温度采样的定性分析). 设 $z = (2, 1, 0)$, 比较

$$\text{softmax}(z), \quad \text{softmax}(z/2), \quad \text{softmax}(2z)$$

的分布尖锐程度. 不要求算小数, 只需比较哪个更接近平均分布, 哪个更偏向最大分数.

习题 12.23 (不用微积分理解非线性). 证明如果 $F(X) = XW_1 + \mathbf{1}b_1^T$, $G(Y) = YW_2 + \mathbf{1}b_2^T$, 则 $G(F(X))$ 仍是 X 的仿射函数. 由此解释为什么前馈网络中需要 *ReLU* 或其他非线性函数.

习题 12.24. 设 $Q, K \in M_{n \times d_k}(\mathbb{R})$. 证明

$$\text{rank}(QK^T) \leq d_k.$$

进一步思考: 为什么不能由此推出 $\text{rowsoftmax}(QK^T)$ 也一定低秩?

习题 12.25. 设 $p = \text{softmax}(z)$, 正确标签为 *one-hot* 向量 $y = e_r$. 令

$$\ell(z) = - \sum_{j=1}^m y_j \log p_j.$$

证明

$$\frac{\partial \ell}{\partial z} = p - y.$$

习题 12.26. 设 $Z = HW + \mathbf{1}b^T$, 损失函数 \mathcal{L} 对 Z 的梯度为 $G = \partial \mathcal{L} / \partial Z$. 证明

$$\frac{\partial \mathcal{L}}{\partial W} = H^T G, \quad \frac{\partial \mathcal{L}}{\partial b} = G^T \mathbf{1}.$$

习题 12.27. 设 $C = I_d - \frac{1}{d} \mathbf{1}\mathbf{1}^T$. 证明 $C^2 = C$, $C\mathbf{1} = 0$, 并解释为什么 Ch 是 h 去均值后的向量.

习题 12.28. 对正弦位置编码, 证明位置平移 $t \mapsto t + s$ 在每个二维频率平面对应一个正交矩阵. 这个结论怎样说明位置编码保留了相对位移信息?

习题 12.29. 在 *KV* 缓存中, 设已有 $K_{1:n}, V_{1:n}$, 新增一行 k_{n+1}^T, v_{n+1}^T . 写出 $K_{1:n+1}$ 和 $V_{1:n+1}$ 的分块形式, 并解释为什么旧的键向量和值向量不需要重新计算.

习题 12.30. 考虑一个词表大小 $m = 6$, 序列长度 $n = 3$, 嵌入维度 $d = 4$, 注意力头维度 $d_k = 2, d_v = 4$ 的单头模型. 写出 $O, E, X, W_Q, W_K, W_V, Q, K, V, QK^T, A, AV, W_U, Z$ 的矩阵形状.

13 挑战选读: 若尔当标准型

选学背景

若尔当标准型回答“不可对角化时还能怎样化简矩阵”的问题, 是特征值理论的高阶部分. 对高中生友好的主线可以先掌握二阶、三阶矩阵的特征值和对角化; 本章适合作为挑战章, 或在学习线性递推通项公式时选择性阅读应用部分.

在第8中, 我们研究了线性变换的特征值与对角化问题. 对角化给出了最简洁的标准型, 但并非所有线性变换都可对角化. 本章的核心目标是: 对于代数闭域 (特别是 \mathbb{C}) 上的线性变换, 找到一种最精细的标准型——若尔当标准型 (Jordan normal form), 它完全确定了线性变换的相似类.

为什么已经有了特征值和特征向量, 仍然还不够? 根本原因是: 重复特征值并不保证能找到足够多的线性无关特征向量. 在常系数微分方程中, 这会表现为除了 $e^{\lambda t}$ 之外还会出现 $te^{\lambda t}, t^2e^{\lambda t}, \dots$ 这样的解; 在离散系统中, 若尔当块

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

满足

$$J^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix},$$

因此矩阵高次幂里会冒出额外的多项式因子. 这些看似分散的现象, 本质上都在说明: 当特征向量不够用时, 我们需要一种比对角化更细致的标准型.

从历史上看, 若尔当标准型也不是凭空降下来的技术. Jordan 在 19 世纪提出了通过标准块分类线性变换的思想, 后来的 Weierstrass、Frobenius 等人则从更严密的代数视角完善了相关理论. 因而本章讨论的不是孤立技巧, 而是分类问题逼出来的自然答案.

整体思路分为两步. 第一步是**广义特征子空间分解**: 利用 Cayley-Hamilton 定理和核分解 (推论7.1), 将问题约化为特征多项式只有一个根 $(\lambda - \lambda_0)^n$ 的情形. 第二步是**幂零变换的若尔当分解**: 令 $N = T - \lambda_0 I$, 则 N 是幂零变换, 通过分析 $\ker N \subset \ker N^2 \subset \dots$ 的递增链, 构造若尔当基, 最终得到若尔当块的直和分解. 在 §8.8中, 我们已经处理了极小多项式等于特征多项式这一最简情形 (定理8.6); 本章将处理一般情形.

本章约定: 除非特别说明, \mathbb{F} 表示一个域, V 是有限维 \mathbb{F} -线性空间, $T: V \rightarrow V$ 是 \mathbb{F} -线性变换. 在涉及若尔当标准型的存在性时, 我们要求 T 的特征多项式 χ_T 在 $\mathbb{F}[\lambda]$ 中完全分裂 (即所有根都在 \mathbb{F} 中). 特别地, 当 $\mathbb{F} = \mathbb{C}$ 时此条件自动满足.

13.1 广义特征子空间分解

给定 \mathbb{F} -线性空间 V 以及 \mathbb{F} -线性变换 $T: V \rightarrow V$, 在 §8.8 中我们知道, 当 T 的极小多项式等于特征多项式时, T 在适当基下的矩阵为友阵 $C(\chi_T)$ (定理 8.6). 对于一般的线性变换, 我们希望找到 T -不变子空间 W_1, \dots, W_k 使得

$$V = W_1 \oplus \cdots \oplus W_k,$$

以及每个 W_i 的基 B_i , 使得矩阵 $[T|_{W_i}]_{B_i}$ 具有简洁的标准型, 且这些标准型完全决定 T 的相似类.

回顾 Cayley-Hamilton 定理 (定理 8.4) 和多元裴蜀恒等式的核分解 (推论 7.1): 若 $h(T) = 0$ 且 $h = h_1 h_2$, $\gcd(h_1, h_2) = 1$, 则 $V = \ker h_1(T) \oplus \ker h_2(T)$, 且 $h_i(T|_{\ker h_i(T)}) = 0$. 将这一结论应用到特征多项式上, 我们得到如下定理 (参见 §8.5 中关于矩阵情形的讨论; 这里给出线性变换的完整叙述和证明).

定理 13.1 (广义特征子空间分解). 设 χ_T 完全分解为

$$\chi_T(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_s)^{n_s},$$

其中 $\lambda_1, \dots, \lambda_s$ 各不相同. 定义广义特征子空间为

$$V[\lambda_i] := \ker(T - \lambda_i I)^{n_i}.$$

则每个 $V[\lambda_i]$ 都是 T -不变子空间, 且有直和分解

$$V = V[\lambda_1] \oplus \cdots \oplus V[\lambda_s].$$

并且 $T|_{V[\lambda_i]}$ 的特征多项式为 $(\lambda - \lambda_i)^{n_i}$, $\dim V[\lambda_i] = n_i$.

证明. 由 Cayley-Hamilton 定理, $\chi_T(T) = 0$. 由于 $(\lambda - \lambda_1)^{n_1}, \dots, (\lambda - \lambda_s)^{n_s}$ 两两互素, 反复应用核分解 (推论 7.1) 得到 $V = \bigoplus_{i=1}^s V[\lambda_i]$, 且每个 $V[\lambda_i]$ 是 T -不变子空间.

记 f_i 为 $T_i = T|_{V[\lambda_i]}$ 的特征多项式. 由于

$$(T_i - \lambda_i I)^{n_i} = 0,$$

可知 T_i 等于标量变换 $\lambda_i I$ 加上幂零变换. 因而 T_i 的唯一特征值是 λ_i , 其特征多项式必为

$$f_i(\lambda) = (\lambda - \lambda_i)^{d_i},$$

其中 $d_i = \dim V[\lambda_i]$. 又直和分解下特征多项式相乘, 即

$$\chi_T = f_1 f_2 \cdots f_s.$$

与

$$\chi_T(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_s)^{n_s}$$

比较各个互异一次因子的幂次, 得 $d_i = n_i$. 因此 $f_i = (\lambda - \lambda_i)^{n_i}$, 且 $\dim V[\lambda_i] = n_i$. \square

习题 13.1. 广义特征子空间也可以定义为

$$V[\lambda_i] := \{v \in V \mid \text{存在 } k \text{ 使得 } (T - \lambda_i I)^k v = 0\}.$$

验证这两种定义是等价的.

注 13.1. 这里的记号 $V[\lambda_i]$ 与 §8.5 中的 V'_{λ_i} 表示同一对象——特征值 λ_i 对应的广义特征子空间. 在后续讨论中我们统一使用 $V[\lambda_i]$ 这一记号.

注 13.2. 由于 $V[\lambda_i] = \ker(T - \lambda_i I)^{n_i}$ 的定义方式不依赖于基的选取, 若 $F: V \rightarrow W$ 给出 (V, T) 到 (W, S) 的同构 (即 $FT = SF$), 则 F 把 T 的 λ_i 广义特征子空间同构到 S 的 λ_i 广义特征子空间. 所以 (V, T) 和 (W, S) 同构当且仅当在调整广义特征子空间的顺序后, 有

$$(V[\lambda_i], T|_{V[\lambda_i]}) \cong (W[\lambda_i], S|_{W[\lambda_i]}).$$

我们对矩阵 $A \in M_n(\mathbb{C})$ 有相应的结论, A 视作 $\mathbb{C}^n \rightarrow \mathbb{C}^n$ 的线性变换, 有对应的广义特征子空间 $W[\lambda_i] \subset \mathbb{C}^n$, 且 $\mathbb{C}^n = \bigoplus W[\lambda_i]$. 即存在可逆矩阵 $P \in \text{GL}(n, \mathbb{C})$ 使得

$$P^{-1}AP = \text{diag}\{A_1, \dots, A_s\},$$

其中 A_i 的特征多项式为 $(\lambda - \lambda_i)^{n_i}$. 且 A 和 B 相似当且仅当在调整顺序后对应的对角块相似.

13.2 幂零变换的若尔当标准型

由定理 13.1, 问题约化为对每个广义特征子空间 $(V[\lambda_i], T|_{V[\lambda_i]})$ 的同构分类. 我们假设 $(V, T: V \rightarrow V)$ 满足 $\chi_T = (\lambda - \lambda_0)^n$, 令 $N = T - \lambda_0 I$, 则 N 与 T 有相同的不变子空间, 且 (V, T) 同构于 (W, S) 当且仅当 $(V, N) \cong (W, S - \lambda_0 I)$. 因此可以约化为幂零变换 (V, N) 的分解以及对应的同构类分类.

定义 13.1. 设 $N: V \rightarrow V$ 是线性变换, 若存在正整数 k 使得 $N^k = 0$, 则称 N 为**幂零变换** (*nilpotent*). 矩阵 A 称为**幂零矩阵**, 如果 $A^k = 0$ 对某个正整数 k 成立.

由 Cayley-Hamilton 定理以及极小多项式的性质, N 的幂零指数 k 不超过 $\dim V$, 且 $\chi_N = \lambda^{\dim V}$. 由上三角化定理, 存在 V 的一组基 B 使得 $[N]_B$ 是严格上三角阵.

定义 13.2 (若尔当块). n 阶**若尔当块** (*Jordan block*) 定义为

$$J_n(\lambda) := \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}_{n \times n} = \lambda I_n + J_n(0),$$

其中 $J_n(0)$ 称为**幂零若尔当块**. 特别地, $J_1(\lambda) = (\lambda)$.

注 13.3. 回顾 §8.8 中友阵的定义 (定义 8.15), 多项式 λ^n 的友阵 $C(\lambda^n)$ 经过基的反转 (将 e_1, \dots, e_n 调整为 e_n, \dots, e_1) 后恰好变为 $J_n(0)$. 事实上, 友阵 $C(\lambda^n)$ 的极小多项式和特征多项式都等于 λ^n (命题 8.10 和 8.11), 这说明 $J_n(0)$ 也满足同样的性质.

命题 13.1. 若尔当块 $J_n(\lambda)$ 具有以下性质:

1. $\chi_{J_n(\lambda)}(\mu) = (\mu - \lambda)^n$, 即 $J_n(\lambda)$ 的唯一特征值为 λ , 代数重数为 n ;
2. $m_{J_n(\lambda)}(\mu) = (\mu - \lambda)^n$, 即极小多项式等于特征多项式;
3. $\dim \ker(J_n(\lambda) - \lambda I_n) = 1$, 即几何重数为 1;
4. $J_n(\lambda)$ 可对角化当且仅当 $n = 1$.

证明. 由 $J_n(\lambda) = \lambda I_n + J_n(0)$, 可知 $J_n(\lambda) - \lambda I_n = J_n(0)$. 由于 $J_n(0)^{n-1} \neq 0$ 且 $J_n(0)^n = 0$, 得 (1) 和 (2). 直接计算 $\ker J_n(0) = \text{span}\{e_1\}$ 得 (3). (4) 由 (1) 和 (3) 立即得到: 可对角化要求几何重数等于代数重数, 即 $1 = n$. \square

定理 13.2 (幂零变换的若尔当标准型). 设 N 是有限维线性空间 V 上的幂零变换, 则存在 N -不变子空间 W_1, \dots, W_s 使得 $V = W_1 \oplus \dots \oplus W_s$, 且存在 W_i 的基 B_i 使得

$$[N|_{W_i}]_{B_i} = J_{k_i}(0).$$

并且 $(V, N) \cong (V', N')$ 当且仅当对应的 k_1, \dots, k_s 和 k'_1, \dots, k'_s 在不计顺序下相同.

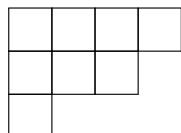
在给出证明之前, 我们先用 Young 图 (Young diagram) 的语言来直观地描述幂零变换的若尔当标准型以及证明策略.

$$v_4 \xrightarrow{N} v_3 \xrightarrow{N} v_2 \xrightarrow{N} v_1 \xrightarrow{N} 0$$

$$Nv_1 = 0, \quad Nv_{i+1} = v_i, \quad \text{一条链对应一个若尔当块}$$

图 20: 幂零变换的若尔当链. 一般情形中 $N = T - \lambda I$.

注 13.4 (Young 图与若尔当型). 设 $\dim V = n$, N 的极小多项式为 λ^{k_1} . 幂零变换 N 的若尔当标准型由一组若尔当块 $J_{k_1}(0), \dots, J_{k_s}(0)$ 构成 (允许重复), 满足 $k_1 \geq k_2 \geq \dots \geq k_s \geq 1$ 且 $k_1 + \dots + k_s = n$. 这样的数据恰好对应 n 的一个分拆 (partition) $\lambda = (k_1 \geq k_2 \geq \dots \geq k_s)$, 也可用一个 Young 图来表示: 共 s 行, 第 i 行有 k_i 个格子, 左对齐. 例如, 8 维空间上若尔当块为 $J_4(0) \oplus J_3(0) \oplus J_1(0)$ 时, 对应分拆 $(4, 3, 1)$ 和 Young 图



Young 图的行对应若尔当块: 第 i 行有 k_i 个格子, 对应一个 $J_{k_i}(0)$ 块. Young 图的列对应核链 $\ker N^j$ 的递增: 第 j 列的格子数等于 $\dim \ker N^j - \dim \ker N^{j-1}$, 即从 $\ker N^{j-1}$ 到 $\ker N^j$ 新增的维数. 记 $\ell_j = \dim \ker N^j$, 则第 j 列的格子数为 $\ell_j - \ell_{j-1}$.

在定理 13.2 的证明中, 基的构造过程可以用 Young 图来理解. 考虑如下从左到右填入的过程:

1. 令 $d_j = \ell_j - \ell_{j-1}$ 为 Young 图第 j 列的格子数. 由引理 13.1 的 (4), $d_1 \geq d_2 \geq \dots \geq d_{k_1}$, 从而确实构成 Young 图的列长度.
2. **第一步:** 取 V_0/V_1 的一组基 (共 d_{k_1} 个向量), 每个向量生成一条长度为 k_1 的 “ N -链”, 填入 Young 图最长的那些行.
3. **第二步:** 在 V_1/V_2 中, 前一步通过 N 映射已贡献了 d_{k_1} 个线性无关向量. 扩充 V_1/V_2 的基还需添加 $d_{k_1-1} - d_{k_1}$ 个新向量, 每个新向量生成一条长度为 $k_1 - 1$ 的 N -链, 填入次长的那些行.
4. 以此类推: 第 t 步在 V_{t-1}/V_t 中扩充基, 新添加的向量生成长度为 $k_1 - t + 1$ 的 N -链.

以分拆 $(4, 3, 1)$ 为例, Young 图的填表过程为:

$N^3 u$	$N^2 v$	$N v_1$	v_1
$N^2 u$	$N w_1$	w_1	
u_1			

其中 v_1 在第一步选取 (从 V_0/V_1), w_1 在第二步选取 (在 V_1/V_2 中扩充基), u_1 在第三步选取 (在 V_2/V_3 中扩充基). 每一行给出一个若尔当块的基, 但写成矩阵基时采用反向链顺序: 从被 N 最终送到 0 的向量开始, 依次写到链的起点. 这样 N 把每个基向量送到前一个基向量, 与定义 13.2 中第一上副对角线为 1 的若尔当块一致.

定理 13.2 的证明. 先假设极小多项式等于特征多项式, 即 $N^n = 0$ 但 $N^{n-1} \neq 0$, 则存在 $v_n \neq 0$ 使得 $N^{n-1}v_n \neq 0$. 定义 $v_{i-1} = Nv_i$, 断言 v_1, \dots, v_n 组成了 V 的一组基: 若 $\sum_i a_i v_i = 0$, 则

$$N^{n-1}(\sum_i a_i v_i) = a_n N^{n-1}v_n = 0,$$

即 $a_n = 0$; 同样有

$$N^{n-2}(\sum_i a_i v_i) = a_{n-1} N^{n-2}v_{n-1} = 0,$$

即 $a_{n-1} = 0$, 同理以此类推有 $a_1 = \dots = a_n = 0$. 因此 v_1, \dots, v_n 是 V 的一组基. 注意这里的顺序已经是反向链顺序: $v_1 = N^{n-1}v_n$ 先被 N 送到 0, 而 v_n 是链的起点. 在此基下 $Nv_i = v_{i-1}$ (约定 $v_0 = 0$), 即 $[N]_B = J_n(0)$.

现在处理一般情形. 假设 N 的极小多项式为 λ^{k_1} , 则 $N^{k_1-1} \neq 0$. 考虑 $\ker N^k$ 构成的递增链, 令

$$V_0 = \ker N^{k_1} = V, V_1 = \ker N^{k_1-1}, \dots, V_i = \ker N^{k_1-i}, \dots, V_{k_1} = \ker N^0 = \{0\}.$$

引理 13.1. 上述子空间具有以下性质:

1. $V_i \supset V_{i+1}$;
2. $N(V_i) \subset V_{i+1}$;
3. N 诱导了映射 $\tilde{N}: V_i/V_{i+1} \rightarrow V_{i+1}/V_{i+2}$;
4. \tilde{N} 是单射;
5. 若对每个 $0 \leq i \leq k_1 - 1$, 取 $v_i^1, \dots, v_i^{m_i} \in V_i$ 满足 $\overline{v_i^1}, \dots, \overline{v_i^{m_i}} \in V_i/V_{i+1}$ 中线性无关, 则全体 v_i^j 在 V 中线性无关.

证明. (1). 由于 $N^k(v) = 0$ 推出 $N^{k+1}(v) = 0$, 故 $V_i \supset V_{i+1}$.

(2). 任取 $w \in V_i = \ker N^{k_1-i}$, 则 $N^{k_1-i-1}(Nw) = N^{k_1-i}w = 0$, 即 $Nw \in \ker N^{k_1-i-1} = V_{i+1}$. 因此 $N(V_i) \subset V_{i+1}$.

(3). 由 (1) 和 (2) 可知 \tilde{N} 良定义.

(4). 假设 $\tilde{N}(\bar{v}) = 0$, 则 $N(v) \in V_{i+2}$, 等价于 $N(v) \in \ker N^{k_1-i-2}$, 等价于 $v \in \ker N^{k_1-i-1}$, 等价于 $v \in V_{i+1}$, 即 $\bar{v} = 0$.

(5). 假设 $\sum_{i,j} a_{ij}v_j^i = 0$. 将等式在商空间 V_0/V_1 中取像: 由于 $v_i^j \in V_i \subset V_0$ 且对 $i \geq 1$ 有 $v_i^j \in V_1$, 故 $\overline{v_i^j} = 0 \in V_0/V_1$ 对所有 $i \geq 1$ 成立. 因此 $\sum_j a_{0j}\overline{v_0^j} = 0$, 由 $\overline{v_0^1}, \dots, \overline{v_0^{m_0}}$ 在 V_0/V_1 中线性无关, 得 $a_{0j} = 0$ 对所有 j 成立. 此时等式化为 $\sum_{i \geq 1, j} a_{ij}v_j^i = 0$. 再在 V_1/V_2 中取像, 类似地得到 $a_{1j} = 0$ 对所有 j 成立. 以此类推, 得到 $a_{ij} = 0$ 对所有 i, j 成立. \square

取 $v_1, \dots, v_{m_0} \in V$, 满足 $\tilde{v}_1, \dots, \tilde{v}_{m_0}$ 是 V_0/V_1 的一组基, 考虑每条链按反向顺序排列得到的向量组

$$N^{k_1-1}v_1, \dots, Nv_1, v_1, N^{k_1-1}v_2, \dots, Nv_2, v_2, \dots, N^{k_1-1}v_{m_0}, \dots, Nv_{m_0}, v_{m_0}.$$

由引理 13.1 的 (4) 可知 $\overline{N^i(v_1)}, \dots, \overline{N^i(v_{m_0})}$ 在 V_i/V_{i+1} 中线性无关, 从而根据 (5) 可知

$$N^{k_1-1}v_1, \dots, Nv_1, v_1, N^{k_1-1}v_2, \dots, Nv_2, v_2, \dots, N^{k_1-1}v_{m_0}, \dots, Nv_{m_0}, v_{m_0}$$

在 V 中线性无关. 将以上这些向量记做 B_1 , 生成的 N -线性子空间记为 W , 则 $[N|_W]_{B_1}$ 是分块对角矩阵, 且每一个对角块是 $J_{k_1}(0)$, 共有 m_0 块.

若 $\overline{Nv_1}, \dots, \overline{Nv_{m_0}}$ 不是 V_1/V_2 的基, 则添加 $w_1, \dots, w_m \in V_1$, 使得 $\overline{w_1}, \dots, \overline{w_{m_1}}$ 和 $\overline{Nv_1}, \dots, \overline{Nv_{m_0}}$ 构成了 V_1/V_2 的一组基, 则

$$\overline{N^i v_1}, \dots, \overline{N^i v_{m_0}}, \overline{N^{i-1} w_1}, \dots, \overline{N^{i-1} w_{m_1}}$$

在 V_i/V_{i+1} 中线性无关, 所以

$$B_2 = \{N^{k_1-2}w_1, \dots, w_1, N^{k_1-2}w_2, \dots, w_2, \dots, N^{k_1-2}w_{m_1}, \dots, w_{m_1}\}$$

线性无关, 也与 B_1 中的向量线性无关, 并且 $[N|_{\text{span}\{B_2\}}]_{B_2}$ 是分块对角矩阵, 每一个对角块为 $J_{k_1-1}(0)$, 共 m_1 个.

一般地, 对 $0 \leq t \leq k_1 - 1$, 归纳地进行如下构造. 假设已选取了

$$B_1, \dots, B_t$$

使得 B_j 中的向量来源于在 V_j/V_{j+1} 中扩充基的过程. 若 $\overline{N^t v_1}, \dots, \overline{N^t v_{m_0}}, \overline{N^{t-1} w_1}, \dots, \overline{N^{t-1} w_{m_1}}, \dots$ 不构成 V_t/V_{t+1} 的基, 则在 V_t 中添加向量 u_1, \dots, u_{m_t} 来扩充. 对每个 u_ℓ , 令

$$B_{t+1, \ell} = \{N^{k_1-t-1}u_\ell, \dots, Nu_\ell, u_\ell\},$$

则 $B_{t+1} = \bigcup_\ell B_{t+1, \ell}$ 中的向量 (连同 B_1, \dots, B_t) 在 V 中线性无关 (由引理13.1的 (4) 和 (5)), 且 $[N|_{\text{span} B_{t+1, \ell}}]$ 在基 $B_{t+1, \ell}$ 下的矩阵为 $J_{k_1-t}(0)$.

记 $\ell_i = \dim V_i/V_{i+1}$, 则 $\sum_{i=0}^{k_1-1} \ell_i = \dim V$. 在上述过程中, 第 t 步扩充了 $m_t = \ell_t - \ell_{t-1}$ 个向量 (约定 $\ell_{-1} = 0$), 每个贡献一个 $J_{k_1-t}(0)$ 若尔当块. 合并所有已构造的反向 N -链向量为 B , 则

$$|B| = m_0 \cdot k_1 + m_1 \cdot (k_1 - 1) + \dots + m_{k_1-1} \cdot 1 = \sum_{i=0}^{k_1-1} (k_1 - i)m_i.$$

由 $\sum_{i=0}^{k_1-1} \ell_i = \dim V$ 以及 $m_i = \ell_i - \ell_{i-1}$ 可验证 $|B| = \dim V$, 因此 B 是 V 的一组基, 且 $[N]_B$ 是分块对角矩阵, 对角线上有 m_t 个 $J_{k_1-t}(0)$ 若尔当块.

关于唯一性: 若 N 在某组基下的矩阵是若尔当块的直和, 则 $\dim \ker N^j$ 是相似不变量 (即不依赖于基的选取), 从而 $\ell_i = \dim \ker N^{k_1-i} - \dim \ker N^{k_1-i-1}$ 唯一确定, 进而 $J_{k_1-i}(0)$ 的个数 $m_i = \ell_i - \ell_{i-1}$ 也唯一确定. \square

下面通过一个完整的计算实例, 展示定理13.2的证明如何具体地操作, 以找到若尔当基.

例 13.1. 设 $V = \mathbb{C}^6$, 线性变换 N 在标准基 e_1, \dots, e_6 下的矩阵为

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

我们按照证明中的步骤, 逐步求出 A 的若尔当标准型和若尔当基.

第一步：计算核链. 直接计算得

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad A^3 = 0.$$

因此 A 的幂零指数为 $k = 3$ (因为 $A^2 \neq 0$ 而 $A^3 = 0$).

第二步：确定核链的维数. 逐次解齐次线性方程组：

- $\ker A$: 方程 $Ax = 0$ 的解空间. 由 A 的非零行为第 1, 3, 5 行, 得约束 $x_4 = 0, x_1 = 0, x_2 + x_6 = 0$. 因此

$$\ker A = \text{span}\{e_2 - e_6, e_3, e_5\}, \quad \dim \ker A = 3.$$

- $\ker A^2$: 方程 $A^2x = 0$ 等价于 $x_4 = 0$ (因为 A^2 仅第 (3, 4) 元素非零). 因此

$$\ker A^2 = \text{span}\{e_1, e_2, e_3, e_5, e_6\}, \quad \dim \ker A^2 = 5.$$

- $\ker A^3 = \mathbb{C}^6, \dim \ker A^3 = 6$.

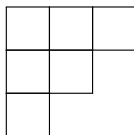
第三步：确定若尔当型 (Young 图). 令 $d_j = \dim \ker A^j - \dim \ker A^{j-1}$ (约定 $\dim \ker A^0 = 0$):

$$d_1 = 3, \quad d_2 = 5 - 3 = 2, \quad d_3 = 6 - 5 = 1.$$

这是 Young 图的列长度序列, 满足 $d_1 \geq d_2 \geq d_3$. 对偶 (转置) 分拆给出行长度: 第 1 行长 3 (因为 d_1, d_2, d_3 均 ≥ 1), 第 2 行长 2 (因为 $d_1, d_2 \geq 2$ 但 $d_3 < 2$), 第 3 行长 1 (因为 $d_1 \geq 3$ 但 $d_2 < 3$). 因此若尔当标准型为

$$J_3(0) \oplus J_2(0) \oplus J_1(0),$$

对应分拆 (3, 2, 1) 和 Young 图:



第四步：逐列构造若尔当基. 令 $V_0 = V = \mathbb{C}^6, V_1 = \ker A^2, V_2 = \ker A, V_3 = \{0\}$.

- 第一列: 取 V_0/V_1 的基. $\dim V_0/V_1 = 6 - 5 = 1$. 需选取 $v_1 \notin \ker A^2$, 即 v_1 的第 4 分量非零. 取 $v_1 = e_4$. 由 v_1 生成长度为 3 的 N -链:

$$v_1 = e_4, \quad Av_1 = Ae_4 = e_1, \quad A^2v_1 = A^2e_4 = e_3.$$

验证: $A^2v_1 = e_3 \neq 0$ (确认 $v_1 \notin \ker A^2$), $A^3v_1 = 0$.

• 第二列: 在 V_1/V_2 中扩充基. $\dim V_1/V_2 = 5 - 3 = 2$. 在 V_1/V_2 中, $Av_1 = e_1$ 的像 \bar{e}_1 已贡献 1 个非零向量 (因为 $e_1 \in V_1 = \ker A^2$ 但 $Ae_1 = e_3 \neq 0$, 故 $e_1 \notin V_2 = \ker A$). 由于 V_1/V_2 是 2 维的, 需再添加 1 个新向量 $w_1 \in V_1 \setminus V_2$ 使得 \bar{w}_1 与 \bar{e}_1 在 V_1/V_2 中线性无关.

注意 $V_1 = \text{span}\{e_1, e_2, e_3, e_5, e_6\}$, $V_2 = \ker A = \text{span}\{e_2 - e_6, e_3, e_5\}$. 取 $w_1 = e_2$ (因为 $Ae_2 = e_5 \neq 0$, 故 $e_2 \notin \ker A$; 且若 $ae_1 + be_2 \in \ker A$ 则 $A(ae_1 + be_2) = ae_3 + be_5 = 0$ 推出 $a = b = 0$, 故 \bar{e}_1 与 \bar{e}_2 在 V_1/V_2 中线性无关).

由 $w_1 = e_2$ 生成长度为 2 的 N -链: $w_1 = e_2, Aw_1 = Ae_2 = e_5$.

• 第三列: 在 V_2/V_3 中扩充基. $\dim V_2/V_3 = 3 - 0 = 3$. 已有的向量: $A^2v_1 = e_3$ 和 $Aw_1 = e_5$, 它们的像 \bar{e}_3, \bar{e}_5 在 $V_2/V_3 \cong \ker A$ 中贡献 2 维. 需添加 1 个新向量 $u_1 \in \ker A$ 使其与 e_3, e_5 在 $\ker A$ 中线性无关. 由 $\ker A = \text{span}\{e_2 - e_6, e_3, e_5\}$, 取 $u_1 = e_2 - e_6$ (它在 $\ker A$ 中且与 e_3, e_5 无关). 这个 u_1 生成长度 1 的链 (因 $Au_1 = 0$).

第五步: 写出若尔当基并验证. 合并所有 N -链, 得到 Young 图的填表:

$$\begin{array}{|c|c|c|} \hline A^2v_1 & Av_1 & v_1 \\ \hline Aw_1 & w_1 & \\ \hline u_1 & & \\ \hline \end{array} = \begin{array}{|c|c|c|} \hline e_3 & e_1 & e_4 \\ \hline e_5 & e_2 & \\ \hline e_2 - e_6 & & \\ \hline \end{array}$$

每一行构成一个若尔当块的基 (按反向 N -链顺序排列). 若尔当基为

$$\mathcal{B} = (\underbrace{e_3, e_1, e_4}_{J_3(0)}, \underbrace{e_5, e_2}_{J_2(0)}, \underbrace{e_2 - e_6}_{J_1(0)}).$$

记过渡矩阵 $P = (e_3 \ e_1 \ e_4 \ e_5 \ e_2 \ e_2 - e_6)$, 读者可直接验证

$$P^{-1}AP = J_3(0) \oplus J_2(0) \oplus J_1(0) = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & & & \\ & & & 0 & 1 & \\ & & & & 0 & \\ & & & & & 0 \end{pmatrix}.$$

注 13.5 (若尔当基构造的算法总结). 由上例可总结出对幂零矩阵 $A \in M_n(\mathbb{F})$ (幂零指数为 k) 求若尔当基的算法:

1. 计算 A, A^2, \dots, A^k , 确定 $\ker A \subset \ker A^2 \subset \dots \subset \ker A^k = \mathbb{F}^n$;
2. 令 $d_j = \dim \ker A^j - \dim \ker A^{j-1}$, 列长度序列 (d_1, d_2, \dots, d_k) 确定 Young 图的形状, 即确定了各若尔当块的大小;
3. 取 $V_0/V_1 (= \mathbb{F}^n / \ker A^{k-1})$ 的一组基 $\bar{v}_1, \dots, \bar{v}_{d_k}$, 由 v_i 生成长度为 k 的 N -链;

4. 对 $t = 1, \dots, k-1$, 在 V_t/V_{t+1} 中将已有向量 $N^t v_1, \dots$ 扩充为基, 新向量生成长度为 $k-t$ 的 N -链;

5. 将每条 N -链按反向链顺序合并, 即得若尔当基.

对一般的 (非幂零) 矩阵, 先做广义特征子空间分解 (定理13.1), 再对每个广义特征子空间上的幂零部分 $N_i = T - \lambda_i I$ 执行上述算法.

13.3 若尔当标准型定理

将广义特征子空间分解 (定理13.1) 与幂零变换的若尔当标准型 (定理13.2) 组合, 我们得到若尔当标准型定理.

定理 13.3 (若尔当标准型). 设 V 是 \mathbb{C} 上的 n 维线性空间, $T: V \rightarrow V$ 是线性变换. 则存在 V 的一组基 B , 使得

$$[T]_B = \text{diag}\{J_{k_1}(\lambda_1), J_{k_2}(\lambda_2), \dots, J_{k_r}(\lambda_r)\},$$

其中 $J_{k_i}(\lambda_i)$ 是 k_i 阶若尔当块 (定义13.2), $\lambda_1, \dots, \lambda_r$ 为 T 的特征值 (允许重复). 上述分解在不计若尔当块顺序下是唯一的, 即若尔当块的集合 $\{J_{k_1}(\lambda_1), \dots, J_{k_r}(\lambda_r)\}$ 是 T 的完全相似不变量.

等价地, 对于矩阵 $A \in M_n(\mathbb{C})$, 存在可逆矩阵 $P \in \text{GL}(n, \mathbb{C})$ 使得

$$P^{-1}AP = \text{diag}\{J_{k_1}(\lambda_1), \dots, J_{k_r}(\lambda_r)\}.$$

右端称为 A 的若尔当标准型 (Jordan normal form). 两个复方阵 $A, B \in M_n(\mathbb{C})$ 相似当且仅当它们有相同的若尔当标准型 (不计若尔当块顺序).

证明. 存在性. 由定理13.1, 设 $\chi_T(\lambda) = \prod_{i=1}^s (\lambda - \lambda_i)^{n_i}$, 则 $V = \bigoplus_{i=1}^s V[\lambda_i]$. 对每个 $V[\lambda_i]$, 令 $N_i = T|_{V[\lambda_i]} - \lambda_i I$, 则 N_i 是幂零变换. 由定理13.2, 存在 $V[\lambda_i]$ 的基使得 N_i 的矩阵为 $\text{diag}\{J_{k_{i,1}}(0), \dots, J_{k_{i,s_i}}(0)\}$, 从而 $T|_{V[\lambda_i]}$ 在此基下的矩阵为 $\text{diag}\{J_{k_{i,1}}(\lambda_i), \dots, J_{k_{i,s_i}}(\lambda_i)\}$. 将各广义特征子空间的基合并即得.

唯一性. 由广义特征子空间分解的唯一性 (特征值及其代数重数由 χ_T 唯一确定), 问题约化为每个广义特征子空间上幂零部分的唯一性, 而这由定理13.2保证. \square

注 13.6. 若尔当标准型定理要求底域为代数闭域 (例如 \mathbb{C}). 对于一般域 \mathbb{F} , 如果 χ_T 在 $\mathbb{F}[\lambda]$ 中完全分裂, 则同样的结论成立. 对于 χ_T 不完全分裂的情形, 需要使用有理标准型, 这将在后续章节中讨论.

13.4 矩阵次幂的计算和应用：递推数列的通项公式

在第8.3节中, 我们看到当矩阵可对角化时, 其幂次 A^n 可以通过 $A^n = P\Lambda^n P^{-1}$ 方便地计算. 这在处理 Markov 链 (如例8.3) 和线性递推数列时具有重要作用. 然而, 对角化方法要求矩阵的几何重数等于代数重数. 当遇到不可对角化矩阵时, 我们便需要借助若尔当标准型来计算矩阵的次幂. 本节我们将展示如何利用若尔当标准型系统地求解任意常系数线性递推数列的通项公式.

13.4.1 若尔当块的次幂

为了计算一般矩阵的幂, 我们首先考察单个若尔当块 $J_k(\lambda)$ 的幂. 注意到 $J_k(\lambda) = \lambda I_k + J_k(0)$, 其中 $J_k(0)$ 是对应于特征值 0 的若尔当块, 即在第一上副对角线上全为 1, 其余为 0 的幂零矩阵. 由于标量矩阵 λI_k 与任何矩阵可交换, 我们可以利用二项式定理对 $J_k(\lambda)^n$ 进行展开.

命题 13.2 (若尔当块的次幂). 设 $J_k(\lambda)$ 是大小为 k 的属于特征值 λ 的若尔当块. 那么对于任意非负整数 n , 当 $\lambda \neq 0$ 或 $\lambda = 0, n \geq k$ 时,

$$J_k(\lambda)^n = \begin{pmatrix} \lambda^n & \binom{n}{1}\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \cdots & \binom{n}{k-1}\lambda^{n-k+1} \\ 0 & \lambda^n & \binom{n}{1}\lambda^{n-1} & \cdots & \binom{n}{k-2}\lambda^{n-k+2} \\ 0 & 0 & \lambda^n & \cdots & \binom{n}{k-3}\lambda^{n-k+3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^n \end{pmatrix}. \quad (11)$$

这里约定当 $j > n$ 时, 二项式系数 $\binom{n}{j} = 0$.

证明. 记 $N = J_k(0)$, 即 N 的第 $(i, i+1)$ 个元素为 1, 其余均为 0. 容易算出 N^j 的非零元素位于第 j 条上副对角线, 它的第 $(i, i+j)$ 个元素为 1. 特别地, 由于它的大小是 k , $N^k = 0$, 这是一个幂零指数为 k 的幂零矩阵. 将 $J_k(\lambda)$ 分解为 $\lambda I_k + N$. 由于 λI_k 与 N 可交换, 根据二项式定理,

$$J_k(\lambda)^n = (\lambda I_k + N)^n = \sum_{j=0}^n \binom{n}{j} \lambda^{n-j} N^j.$$

由于当 $j \geq k$ 时 $N^j = 0$, 级数实际上只求和到 $\min(n, k-1)$. 将 N^j 的显式结构代入求和, 在第 i 行第 j 列 (其中 $j \geq i$, 对应向上平移 $j-i$ 次), 元素的值即为所乘常数 $\binom{n}{j-i} \lambda^{n-(j-i)}$, 这恰好是公式(11)中对应位置的元素. \square

注 13.7. 上式的结果也可以用形式导数优雅地表达. 注意到 $(J_k(\lambda)^n)_{ij}$ 在 $j \geq i$ 时等于 $\frac{1}{(j-i)!} \frac{d^{j-i}}{d\lambda^{j-i}} (\lambda^n)$. 这反映了在矩阵函数的微积分中 (下一小节), $J_k(\lambda)$ 上的函数作用对应于逐项求导的过程. 当 $\lambda = 0$ 时, 上式中只有 $\binom{n}{j-i} 0^{n-j+i}$ 在 $n = j-i$ 时为 1, 这与 $J_k(0)^n$ 平移 n 步是一致的.

对于一般的方阵 A , 设其可化为若尔当标准型 $A = PJP^{-1}$, 其中 $J = \text{diag}(J_{k_1}(\lambda_1), \dots, J_{k_m}(\lambda_m))$. 根据矩阵乘法的结合律,

$$A^n = (PJP^{-1})^n = PJ^nP^{-1} = P \text{diag}(J_{k_1}(\lambda_1)^n, \dots, J_{k_m}(\lambda_m)^n) P^{-1}.$$

如此, 我们只需求出过渡矩阵 P 及其逆 P^{-1} , 并代入命题13.2的公式计算各个块的次幂, 即可得到任意矩阵 A^n 的显式表达式. 一些元素可能不可避免地含有组合数与多项式的混合项.

13.4.2 线性常系数递推数列通项的一般理论

作为对角化和若尔当次幂计算的绝佳应用, 我们现在解决代数学中经典的一类结构分析问题.

定义 13.3 (常系数线性递推). 设数列 $(a_n)_{n=0}^{\infty}$ 满足 k 阶齐次常系数线性递推关系:

$$a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \dots + c_1a_{n+1} + c_0a_n \quad (n \geq 0), \quad (12)$$

其中 c_0, c_1, \dots, c_{k-1} 为常数, 且 $c_0 \neq 0$, 给定初值约束 a_0, a_1, \dots, a_{k-1} .

数列在第 $n+k$ 项的值由前面 k 项组合决定. 我们引入一个 k 维“状态向量” $\mathbf{x}_n = (a_n, a_{n+1}, \dots, a_{n+k-1})^T$. 那么, 递推关系(12)可以表示为一阶向量差分方程:

$$\begin{pmatrix} a_{n+1} \\ a_{n+2} \\ \vdots \\ a_{n+k-1} \\ a_{n+k} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{k-1} \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-2} \\ a_{n+k-1} \end{pmatrix},$$

即 $\mathbf{x}_{n+1} = C\mathbf{x}_n$. 我们发现, 转移矩阵 C 恰好是多项式

$$f(\lambda) = \lambda^k - c_{k-1}\lambda^{k-1} - \dots - c_1\lambda - c_0$$

的友阵 (见定义8.15的转置形式). 这是非常深刻的联系. 方程 $f(\lambda) = 0$ 不仅是 C 的特征多项式, 它更被直接称作该递推关系的**特征方程**. 因为 $\mathbf{x}_n = C^n\mathbf{x}_0$, 求数列的通项公式就完全等同于计算 C^n .

(一) 特征根互不相同的情形 (可对角化)

若特征方程 $f(\lambda) = 0$ 的 k 个根 $\lambda_1, \lambda_2, \dots, \lambda_k$ 在复数域中互不相同, 那么代数重数均为 1. 因为 C 特征值皆单根, C 是可对角化的.

定理 13.4 (互异特征根的通项). 若齐次线性递推项方程互不相同的复非零根为 $\lambda_1, \dots, \lambda_k$, 那么任何满足该递推式的数列必定具有如下形式:

$$a_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n + \dots + \alpha_k \lambda_k^n,$$

其中常数 $\alpha_1, \dots, \alpha_k$ 完全由初值约束 a_0, \dots, a_{k-1} 唯一确定.

证明. 因为 C 互不相同特征值为 λ_i , 故有非奇异矩阵 P 使得 $C = P \operatorname{diag}(\lambda_1, \dots, \lambda_k) P^{-1}$. 于是 $\mathbf{x}_n = C^n \mathbf{x}_0 = P \operatorname{diag}(\lambda_1^n, \dots, \lambda_k^n) P^{-1} \mathbf{x}_0$. 如果设列向量 $P^{-1} \mathbf{x}_0 = (\alpha_1, \dots, \alpha_k)^T$, 那么将其乘回来之后, \mathbf{x}_n 的第一个元素 (即 a_n) 刚好是所有 λ_i^n 以 P 的第一行元素乘以 α_i 后的线性组合. 即 a_n 必定是 λ_i^n 的线性组合. 为了求特解, 将 $n = 0, 1, \dots, k-1$ 代入即可解出一个范德蒙德 (Vandermonde) 方程组确定 α_i . \square

例 13.2 (Fibonacci 数列的 Binet 公式). 众所周知的 Fibonacci 数列递推定义为 $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. 其特征方程为:

$$\lambda^2 - \lambda - 1 = 0 \implies \lambda_1 = \frac{1 + \sqrt{5}}{2} = \phi, \quad \lambda_2 = \frac{1 - \sqrt{5}}{2} = \hat{\phi},$$

由定理 13.4, $F_n = c_1 \phi^n + c_2 \hat{\phi}^n$. 代入 $n = 0$ 得 $c_1 + c_2 = 0$, $n = 1$ 得 $c_1 \phi + c_2 \hat{\phi} = 1$. 解得 $c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}}$. 这便给出著名的 Binet 公式:

$$F_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}}.$$

(二) 有重根的情形 (不可对角化)

当特征根有重根时, C 一般不能对角化 (事实上, 友阵是**不可减损**的, 它的每个特征值的几何重数必然等于 1, 只要有重根它就一定不可对角化, 见命题 8.11). 这就是必须引入若尔当块(11)的时机.

定理 13.5 (任意常系数线性递推的通项). 设递推方程(12)的特征方程具有 s 个不同的根 $\lambda_1, \dots, \lambda_s$, 其代数重数分别为 m_1, \dots, m_s (从而 $\sum m_i = k$). 那么任何满足该递推式的数列必然呈现如下形式:

$$a_n = P_1(n) \lambda_1^n + P_2(n) \lambda_2^n + \dots + P_s(n) \lambda_s^n, \quad (13)$$

其中每个 $P_i(n)$ 常系数的并且是关于 n 的不超过 $m_i - 1$ 次的多项式. 等价地, 上述通项式展开包含了 k 个独立基函数 $n^j \lambda_i^n$ (其中 $0 \leq j < m_i$).

证明. 根据若尔当标准型定理, $C = PJP^{-1}$, 其中 J 的构成为关于各个 λ_i 的若尔当块组成的块对角或分块矩阵. 因为代数重数为 m_i , 这些块在次幂 J^n 下按命题 13.2 会产生出包含 $\binom{n}{j} \lambda_i^{n-j}$ 项的矩阵元, 此处的 j 最大取到 $m_i - 1$. 这是 n 的一个最高不超过 $m_i - 1$ 次的多项式. 与 P 和 $P^{-1} \mathbf{x}_0$ 的常数项作用即得线性组合的结构. \square

例 13.3 (带重根的递推数列解法). 已知数列初值为 $a_0 = 1, a_1 = 4, a_2 = 20$, 并满足如下递推关系 (由于含有三项前面依赖项是 3 阶递推):

$$a_{n+3} = 5a_{n+2} - 8a_{n+1} + 4a_n.$$

其对应的特征方程为

$$\lambda^3 - 5\lambda^2 + 8\lambda - 4 = 0.$$

对其进行因式分解: $\lambda = 1$ 是显然的一个根 $1 - 5 + 8 - 4 = 0$. 提出 $(\lambda - 1)$ 得到 $\lambda^2 - 4\lambda + 4 = (\lambda - 2)^2$. 因此方程有单根 $\lambda_1 = 1$ 以及二重根 $\lambda_2 = 2 (m_2 = 2)$.

根据结构定理 13.5, 通项必然可用如下基函数表示 (由于重数分别为 1 和 2):

$$a_n = C_1 \cdot 1^n + (C_2 + C_3 n) \cdot 2^n = C_1 + (C_2 + C_3 n) 2^n.$$

利用初值反解多项式系数:

$$n = 0: C_1 + C_2 = 1$$

$$n = 1: C_1 + (C_2 + C_3)2 = 4$$

$$n = 2: C_1 + (C_2 + 2C_3)4 = 20$$

解该三元一次方程组, 得 $C_1 = 4, C_2 = -3, C_3 = 2$. 从而推导出显式通项为

$$a_n = 4 + (2n - 3)2^n.$$

使用若尔当型给出来的理论指导极大简化了原本需求特征空间计算高阶过渡矩阵的流程。这也是结构定理“先定架子后解参”之所以优越直白的原因。

注 13.8 (与生成函数的联系). 熟悉离散数学和组合计数的读者可能会发现, 求解递推数列和离散系统的另一种强大技术是**生成函数法** (*Generating Functions*). 如果将数列作形式幂级数 $G(x) = \sum_{n=0}^{\infty} a_n x^n$, 递推关系就等价于说 $G(x)$ 是有理函数 $P(x)/Q(x)$. 对具有重根的 $Q(x)$ 进行部分分式展开 (*Partial Fraction Decomposition*) 也会得到形如 $1/(1 - \lambda x)^m$ 的项, 利用二项式广义展开就可以产生带多项式的系数 $\binom{n+m-1}{m-1} \lambda^n$. 本质上, 有理分式展开正是代数层面上矩阵按若尔当块进行不变子空间分解的一个解析映射缩影! 线性代数从结构分解出发提供了同一现象更加几何的基底。

13.5 习题

13.5.1 练习题

本节中标注为“有理标准型方向”的题目可以留到第15章之后再处理; 标注为“矩阵函数方向”的题目可以留到第14章之后再处理.

习题 13.2 (二阶若尔当块的幂). 设

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

1. 将 J 写成 $\lambda I + N$, 并验证 $N^2 = 0$.
2. 计算 J^n .
3. 当 $\lambda = 1$ 时, 解释为什么 J^n 不会保持有界.
4. 将结论与递推关系 $x_{n+1} = Jx_n$ 的增长联系起来.

习题 13.3. 设 N 是 n 维 \mathbb{F} -线性空间 V 上的幂零变换, 幂零指数为 k (即 $N^k = 0, N^{k-1} \neq 0$). 证明:

1. $k \leq n$;
2. N 的极小多项式为 λ^k ;
3. N 的特征多项式为 λ^n .

习题 13.4. 设 $A \in M_n(\mathbb{C})$ 是幂零矩阵. 证明 $\text{tr}(A) = 0, \det(A) = 0, I + A$ 可逆.

习题 13.5. 求下列矩阵的若尔当标准型 (不要求过渡矩阵):

1. $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix};$

2. $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix};$

3. $A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix};$

4. $A = \begin{pmatrix} 3 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$

习题 13.6. 求下列矩阵的若尔当标准型, 以及相应的过渡矩阵 P (使得 $P^{-1}AP$ 为若尔当标准型):

$$1. A = \begin{pmatrix} 5 & 4 & 2 \\ -1 & 0 & -1 \\ -2 & -2 & 0 \end{pmatrix};$$

$$2. A = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

习题 13.7. 设 $A \in M_4(\mathbb{C})$ 的特征多项式为 $\chi_A(\lambda) = (\lambda - 1)^2(\lambda - 2)^2$. 列出 A 所有可能的若尔当标准型.

习题 13.8. 设 $A \in M_5(\mathbb{C})$, 特征多项式为 $\chi_A(\lambda) = (\lambda - 2)^5$. 已知 $\text{rank}(A - 2I) = 3$, $\text{rank}(A - 2I)^2 = 1$. 求 A 的若尔当标准型.

习题 13.9. 设 $A \in M_n(\mathbb{C})$, 特征多项式 $\chi_A(\lambda) = (\lambda - \lambda_0)^n$. 证明: A 的若尔当标准型恰好只有一个若尔当块 $J_n(\lambda_0)$ 当且仅当 A 的极小多项式等于特征多项式.

习题 13.10. 设 A 是 n 阶复方阵, 若尔当标准型中特征值 λ 对应的若尔当块为 $J_{k_1}(\lambda), \dots, J_{k_s}(\lambda)$, $k_1 \geq \dots \geq k_s \geq 1$. 证明:

1. λ 的代数重数为 $k_1 + \dots + k_s$;
2. λ 的几何重数为 s (即若尔当块的个数);
3. λ 在极小多项式中的幂次为 k_1 (即最大若尔当块的阶).

习题 13.11. 设 $A \in M_n(\mathbb{C})$ 的若尔当标准型为 J . 求 A^T 的若尔当标准型.
(提示: 考虑 $J_k(\lambda)^T$ 与 $J_k(\lambda)$ 的关系.)

习题 13.12. 设 $A \in M_n(\mathbb{C})$ 可逆, 若尔当标准型为 $\text{diag}\{J_{k_1}(\lambda_1), \dots, J_{k_r}(\lambda_r)\}$. 求 A^{-1} 的若尔当标准型.

(提示: 先对一个若尔当块 $J_k(\lambda)$ ($\lambda \neq 0$) 求逆, 并分析其若尔当型.)

习题 13.13. 设 $N, N' \in M_n(\mathbb{C})$ 都是幂零矩阵. 证明: N 与 N' 相似当且仅当对所有 $k \geq 1$, $\text{rank } N^k = \text{rank } N'^k$.

习题 13.14. 设 $N \in M_6(\mathbb{C})$ 为幂零矩阵, $\text{rank } N = 4$, $\text{rank } N^2 = 2$, $\text{rank } N^3 = 0$. 求 N 的若尔当标准型, 并画出对应的 Young 图.

习题 13.15. 设 $N \in M_n(\mathbb{C})$ 是幂零矩阵, 幂零指数为 k . 证明: $\text{rank } N \geq k - 1$. 何时等号成立?

习题 13.16. 设

$$J = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

求 J 的特征值和特征向量空间维数。

习题 13.17. 设

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

计算 N^2 , 并说明 N 为什么是幂零矩阵。

习题 13.18. 设

$$J = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

计算 $J - 3I$, $(J - 3I)^2$ 和 $(J - 3I)^3$ 。

习题 13.19. 判断矩阵

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

是否可对角化。请从特征向量数量解释。

习题 13.20. 设 A 的若尔当标准型含有一个大小为 3、特征值为 2 的若尔当块。写出这个若尔当块, 并求它的特征多项式。

13.5.2 思考题

习题 13.21 (矩阵函数方向). 设 $A \in M_n(\mathbb{C})$, $f(\lambda) \in \mathbb{C}[\lambda]$. 若 A 的若尔当标准型为 $\text{diag}\{J_{k_1}(\lambda_1), \dots, J_{k_r}(\lambda_r)\}$, 求 $f(A)$ 的若尔当标准型.

(提示: 先计算 $f(J_k(\lambda))$. 注意 $J_k(\lambda) = \lambda I + J_k(0)$, 对 f 做 Taylor 展开.)

习题 13.22 (矩阵函数方向). 设 $A \in M_n(\mathbb{C})$, 证明 $e^A := \sum_{k=0}^{\infty} \frac{A^k}{k!}$ 收敛 (在 $M_n(\mathbb{C})$ 的标准拓扑下), 并证明 $\det(e^A) = e^{\text{tr}(A)}$.

(提示: 利用若尔当标准型, 约化到单个若尔当块 $J_k(\lambda)$ 的情形.)

习题 13.23. 设 $A, B \in M_n(\mathbb{C})$, 若尔当标准型分别为 J_A 和 J_B . 判断以下命题是否正确, 并给出证明或反例:

1. $A + B$ 的若尔当标准型由 J_A 和 J_B 唯一确定;

2. AB 的若尔当标准型由 J_A 和 J_B 唯一确定.

习题 13.24. 求所有与矩阵 $A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$ 可交换的 2×2 复矩阵.

(提示: 设 $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 利用 $AB = BA$ 列出方程.)

习题 13.25. 设 $J = J_n(\lambda) \in M_n(\mathbb{C})$, 求 J 的中心化子 (commutant), 即全体与 J 可交换的 n 阶复方阵构成的集合 $C(J) = \{B \in M_n(\mathbb{C}) \mid BJ = JB\}$. 证明 $C(J)$ 恰好是 $\{f(J) \mid f \in \mathbb{C}[\lambda]\}$, 即 J 的多项式构成的集合.

习题 13.26. 设 $A \in M_n(\mathbb{C})$ 有 n 个不同的特征值. 证明与 A 可交换的矩阵一定是 A 的多项式. 请思考: 若 A 有重复特征值, 该结论是否仍然成立?

习题 13.27 (矩阵开方). 设 $A \in M_n(\mathbb{C})$ 可逆. 利用若尔当标准型, 证明存在 $B \in M_n(\mathbb{C})$ 使得 $B^2 = A$.

(提示: 先对一个可逆若尔当块 $J_k(\lambda) (\lambda \neq 0)$ 找 B , 使得 $B^2 = J_k(\lambda)$.)

习题 13.28 (矩阵对数). 设 $A \in M_n(\mathbb{C})$ 的所有特征值都有正实部. 利用若尔当标准型, 证明存在 $B \in M_n(\mathbb{C})$ 使得 $e^B = A$.

习题 13.29. 设 V 是 n 维复线性空间, $T: V \rightarrow V$ 是线性变换. 证明以下等价:

1. T 是幂零变换;
2. T 的所有特征值为 0;
3. $T^n = 0$;
4. $\text{tr}(T^k) = 0$ 对所有 $k \geq 1$ 成立.

习题 13.30. 设 $T: V \rightarrow V$ 是复线性空间上的线性变换, T 的若尔当标准型已知. 利用 Young 图, 确定以下信息:

1. $\dim \ker T^k$ 对各 $k \geq 0$;
2. $\dim \text{Im } T^k$ 对各 $k \geq 0$;
3. T 的极小多项式的次数.

习题 13.31. 列举 6 的所有分拆, 画出对应的 Young 图, 并写出相应的 6 阶幂零若尔当标准型. 其中哪些满足极小多项式为 λ^3 ?

习题 13.32. 设 $A \in M_n(\mathbb{C})$ 满足 $A^2 = A$ (即 A 为幂等矩阵). 求 A 的若尔当标准型.

(提示: A 的极小多项式整除 $\lambda^2 - \lambda = \lambda(\lambda - 1)$.)

习题 13.33. 设 $A \in M_n(\mathbb{C})$ 满足 $A^3 = I$. 求 A 所有可能的若尔当标准型.

习题 13.34. 计算矩阵 $\begin{pmatrix} 1 & -3 & 4 \\ 0 & 7 & 8 \\ 0 & 0 & 7 \end{pmatrix}$ 的若尔当标准型.

习题 13.35 (矩阵函数方向). 利用二项式展开求若尔当块 $J = J_{\lambda, n}$ 的 k 次方. 比较你的公式和 x^k 的各阶导数的关系, 从而推导出对一般的多项式 f , 矩阵 $f(J)$ 的表达形式.

习题 13.36 (矩阵函数方向). 利用若尔当标准型证明, 如果 $A \in M_n(\mathbb{C})$ 是一个可逆矩阵, 则存在一个复方阵 B 使得 $B^2 = A$. 如果 A 不可逆, 该结论是否依然成立?

习题 13.37 (有理标准型方向). 假设域 F 上的有限维线性空间 V 上的线性变换 T 的特征多项式有某一个不可约因子 $p(\lambda)$, 证明 T 存在维数为 $\deg p$ 的不变子空间.

习题 13.38. 假设 T, S 均为有限维 F -线性空间 V 上的线性变换, 且 $TS = ST$, 证明 T 的广义特征子空间也是 S 的不变子空间.

习题 13.39. 假设 F 是一个域, 且 $\{A_i\}_{i \in I}$ 是一族两两乘法可换的方阵, 且 A_i 均可以对角化. 证明存在同一个可逆方阵 P 使得对任意 $i \in I$, $P^{-1}A_iP$ 都是对角阵.

习题 13.40. 对一般的域 F , 证明如果 $A \in M_n(F)$ 是一个幂零矩阵, 即 $A^m = 0$ 对某一个整数 m 成立, 则 A 在 F 上相似于某一个若尔当标准型.

习题 13.41. 证明任意一个复数域上的 n 阶方阵 A 可以写作两个矩阵 D 和 N 的和, 其中 D 是对角化矩阵, N 是幂零矩阵, 且 $DN = ND$. (进一步思考: 证明这样的分解是唯一的.)

习题 13.42. $A: V \rightarrow V$ 是有限维复线性空间的算子, $m_A(x) \in \mathbb{C}[x]$ 是算子的极小多项式并有素分解 $m_A(x) = \prod_{i=1}^k (x - \lambda_i)^{n_i}$. 令 $V_i = \ker((A - \lambda_i I)^{n_i})$. 证明

$$V = \bigoplus V_i.$$

习题 13.43. 考虑 $N \in M_5(\mathbb{C})$ 满足 $N^3 = 0$. 请问这样的 N 在复数域上的相似类有多少个? 请从中挑一个类描述所有和 N 交换的矩阵的形式.

习题 13.44 (有理标准型方向). 假设域 F 上的有限维线性空间 V 上的线性变换 T 的特征多项式不可约, 找出所有的 T 不变子空间.

习题 13.45. 假设 A 是一个可对角化的 n 阶复方阵, 且 A 的互不相同特征值为 $\lambda_1, \dots, \lambda_k$, 其中每个 λ_i 的代数重数为 m_i , 求与 A 乘法交换的所有 n 阶方阵组成的 $M_n(\mathbb{C})$ 子空间的维数.

习题 13.46. 假设实方阵 A 满足 $A^2 = -I$, 证明 A 的阶数为偶数, 且对每个固定的阶数, 求出这样的 A 的相似类有多少个? 对每一个固定的 $2n$ -阶矩阵 A , 将与 A 乘法交换的实方阵全体 V 和 $M_n(\mathbb{C})$ 建立一个双射, 从而求出 V 的实维数.

习题 13.47 (有理标准型方向). 考虑极小多项式为 $x^2 - x + 1$ 的四阶方阵 $A \in M_4(\mathbb{F}_3)$. 求出这样的 A 的相似类有多少个? 对每一个相似类里的矩阵 A , 求出这样的矩阵的个数.

习题 13.48 (有理标准型方向). 假设 F 是一个域, 考虑 $A \in M_n(F)$ 且 A 的特征多项式在 $F[x]$ 中不可约. 证明所有和 A 交换的 F -方阵都是 A 的多项式.

习题 13.49 (若尔当块平方的反问题). 记

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}.$$

如果复方阵

$$A^2 = \begin{pmatrix} J_2(0) & 0 & 0 & 0 \\ 0 & J_2(0) & 0 & 0 \\ 0 & 0 & J_3(0) & 0 \\ 0 & 0 & 0 & J_3(0) \end{pmatrix},$$

求 A 的若尔当标准型, 并证明你的结论.

习题 13.50 (给定特征多项式与极小多项式的若尔当型). 设 A 是复数域 \mathbb{C} 上的 10×10 矩阵, 已知:

$$f(\lambda) = (\lambda - 1)^6(\lambda + 1)^4, \quad m(\lambda) = (\lambda - 1)^4(\lambda + 1)^2.$$

写出 A 所有可能的复相似类有多少种, 并列出每种相似类的若尔当标准型.

习题 13.51 (参数矩阵的极小多项式、若尔当型与指数). 设

$$A_t = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & t \\ 0 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{C}), \quad t \in \mathbb{C}.$$

- 按 t 的取值分类, 求 A_t 的极小多项式.
- 按 t 的取值分类, 写出 A_t 的若尔当标准型.
- 计算

$$e^{A_t} = \sum_{k=0}^{\infty} \frac{A_t^k}{k!}$$

的显式表达式.

习题 13.52 (极小多项式与特征多项式). 设 A 是 $n \times n$ 复矩阵, $p(x)$ 是 A 的特征多项式, $m(x)$ 是 A 的极小多项式。

1. 证明 $m(x)$ 和 $p(x)$ 有相同的根。
2. 构造一个 4×4 矩阵 A , 使得 $m(x) \neq p(x)$ 且 A 不可对角化。

习题 13.53 (不变子空间有限性与极小多项式). 设 V 是复数域上的有限维线性空间, $T \in \text{End}(V)$ 。判断下列两个陈述是否等价:

1. T 的不变子空间个数只有有限个;
2. T 的极小多项式等于特征多项式。

若等价, 请给出证明; 若不等价, 请给出反例。课后思考: 若把复数域换成有理数域, 结论是否仍然成立?

习题 13.54 (幂零矩阵的最大秩与若尔当型). 设 $A \in M_{2026}(\mathbb{C})$ 满足 $A^3 = 0$ 。

1. 求 $\text{rank}(A)$ 的最大可能值。
2. 当 $\text{rank}(A)$ 达到最大时, 求 A 的可能若尔当标准型。

14 选读：矩阵函数和常微分方程

选学背景

本章需要无穷级数、矩阵指数和常微分方程背景。如果读者还没有学微积分，可以只阅读二阶矩阵指数的直观例子和相图图示；完整的 ODE 理论可在后续课程中再学。

自然界中的许多连续过程——放射性物质的衰变、弹簧振子的振荡、化学反应中浓度的变化、传染病在人群中的传播——都可以用**常微分方程**(Ordinary Differential Equations, 简称 ODE) 来描述。最简单的情形是单变量方程 $x'(t) = ax(t)$ ，其解为 $x(t) = e^{at}x(0)$ 。当系统涉及多个相互耦合的变量时，方程自然地推广为向量形式 $\mathbf{x}'(t) = A\mathbf{x}(t)$ ，其中 A 是一个方阵。要写出这类方程组的解，我们需要赋予“ e 的矩阵次幂”以精确含义——这便引出了**矩阵指数**的概念。

上一节中，我们探讨了**离散**时间的常系数线性递推 $\mathbf{x}_{n+1} = C\mathbf{x}_n$ ，认识到其核心在于计算转移矩阵的次幂 C^n 。现在，我们将视线转向**连续**的对应物。这两者之间的类比极为完美：离散系统的解 $\mathbf{x}_n = C^n\mathbf{x}_0$ 对应于连续系统的解 $\mathbf{x}(t) = e^{tA}\mathbf{x}_0$ ；递推中 λ^n 的角色由指数函数 $e^{\lambda t}$ 接替；而若尔当标准型在两种情形中都扮演着将系统“解耦”为独立子问题的核心角色。

本节的目标是：首先引入矩阵指数和一般矩阵函数的定义，借助若尔当标准型给出显式计算公式；然后用它求解一阶线性 ODE 组和高阶标量 ODE；最后讨论系统的**稳定性**——特征值的实部如何决定解的长期行为——并将这一思想推广到非线性系统的局部分析中。

除了力学、化学和生物模型之外，连续时间 Markov 链也是方程组 $\mathbf{x}'(t) = A\mathbf{x}(t)$ 的重要来源。如果 $\mathbf{x}(t)$ 记录系统在各状态上的概率分布，而 A 是瞬时跃迁速率矩阵，那么系统在时间 t 后的演化正是由 e^{tA} 给出。与此类似，很多非线性传染病模型或生态模型在平衡点附近也会先被线性化为 $\mathbf{x}' = A\mathbf{x}$ 。这说明矩阵指数并不是形式定义，而是连续时间演化的自然语言。

14.1 矩阵的幂级数与矩阵指数

我们已经知道，标量方程 $x'(t) = ax(t)$ 的解是 $x(t) = e^{at}x(0)$ 。如果想把这个公式推广到方程组 $\mathbf{x}'(t) = A\mathbf{x}(t)$ ，最自然的猜测是 $\mathbf{x}(t) = e^{tA}\mathbf{x}(0)$ ——但这要求我们赋予“ e 的矩阵次幂”以严格含义。幸运的是， e^x 的泰勒级数 $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ 对所有 x 绝对收敛，而其中的运算（加法、乘法、数乘）在方阵上同样有意义，于是我们可以通过**代数代入**的方式给出定义：

定义 14.1 (矩阵指数). 对于任意 n 阶实方阵 $A \in M_n(\mathbb{R})$ 或复方阵 $A \in M_n(\mathbb{C})$ ，定义其**矩阵指数** (Matrix Exponential) e^A (或记作 $\exp(A)$) 为如下幂级数：

$$e^A = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!}A^k. \quad (14)$$

任意引入一种矩阵上的范数 (如分量最大值范数) 后, 不难证明上述级数不仅收敛, 且是**绝对收敛**的。我们不在此作深入的分析拓扑探讨, 直接罗列矩阵指数的一些基本代数性质:

命题 14.1 (矩阵指数的基本性质). 设 $A, B \in M_n(\mathbb{C})$,

1. $e^{0_{n \times n}} = I_n$ 。
2. 如果 $AB = BA$, 即矩阵可交换, 则 $e^{A+B} = e^A e^B$ 。
3. e^A 总是可逆矩阵, 且 $(e^A)^{-1} = e^{-A}$ 。(由前两条, 取 $B = -A$ 立得)
4. $\det(e^A) = e^{\text{tr}(A)}$ 。由于 $e^{\text{tr}(A)} \neq 0$, 这也再次验证了 e^A 是可逆的。
5. 若矩阵之间相似 $B = P^{-1}AP$, 则 $e^B = P^{-1}e^A P$ 。也就是说, 求指数可以与对角化或若尔当分解过程结合使用。

注 14.1. 值得极度警惕的是, 当 $AB \neq BA$ 时, $e^{A+B} \neq e^A e^B$ 通常成立。这就使得非交换代数中的指数运算不仅不能简单相加, 反倒由此诞生了著名的 **Baker-Campbell-Hausdorff (BCH) 公式**, 在李理论中至关重要。

在进入更深层的理论之前, 我们先通过最简单的情形建立直觉。

例 14.1 (对角矩阵的矩阵指数). 设 $A = \text{diag}(\lambda_1, \dots, \lambda_n)$ 是对角矩阵。由于 $A^k = \text{diag}(\lambda_1^k, \dots, \lambda_n^k)$, 代入定义得

$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} \text{diag}(\lambda_1^k, \dots, \lambda_n^k) = \text{diag}\left(\sum_{k=0}^{\infty} \frac{\lambda_1^k}{k!}, \dots, \sum_{k=0}^{\infty} \frac{\lambda_n^k}{k!}\right) = \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}).$$

例如, $e^{\begin{pmatrix} 1 & 0 \\ 0 & -3 \end{pmatrix}} = \begin{pmatrix} e & 0 \\ 0 & e^{-3} \end{pmatrix}$ 。对角矩阵的指数就是对每个对角元取标量指数! 这一事实立即验证了命题 14.1(4): $\det(e^A) = e^{\lambda_1} \dots e^{\lambda_n} = e^{\lambda_1 + \dots + \lambda_n} = e^{\text{tr}(A)}$ 。

例 14.2 (可对角化矩阵与幂零矩阵). 设 $A = P \text{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$, 则由命题 14.1(5),

$$e^A = P \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P^{-1}.$$

再看一个不可对角化但很容易计算的幂零例子: 令 $A = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ 。此时可以直接从级数计算: $A^2 = 0$, 故

$$e^A = I + A + \underbrace{\frac{A^2}{2!} + \dots}_{=0} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

级数在有限步内截断! 这一幂零矩阵的情形将在下一小节中系统讨论。

除了指数外, 如果一个幂级数 $\sum_{k=0}^{\infty} a_k z^k$ 在某个圆盘内收敛, 我们同样可以通过 $\sum_{k=0}^{\infty} a_k A^k$ 定义任意**一般矩阵函数** $f(A)$, 如 $\sin(A), \cos(A)$, 只要求 A 的特征值均落在此收敛半径内即可。

14.2 若尔当块上的矩阵函数

对于一般的方阵，直接按定义对级数求和来计算 e^A 几乎是不可能的。但我们手中有一件利器：若尔当标准型。由于 $e^{PJP^{-1}} = Pe^JP^{-1}$ (命题14.1(5))，我们只需将 A 化为若尔当标准型 $J = \text{diag}(J_{k_1}(\lambda_1), \dots)$ ，从而归结于求每个小块 $e^{J_k(\lambda)}$ 的问题。在命题13.2中，我们曾指出若尔当块的次幂具有逐项关于特征值“求导”的优美性质。这一关系其实对一般可微函数也是通用的！

命题 14.2 (若尔当块的矩阵函数公式). 设 $f(z)$ 是在一个包含 λ 的开集上的复解析函数，且 $J_k(\lambda)$ 是一大小为 k 的若尔当块，则：

$$f(J_k(\lambda)) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{f''(\lambda)}{2!} & \cdots & \frac{f^{(k-1)}(\lambda)}{(k-1)!} \\ 0 & f(\lambda) & f'(\lambda) & \cdots & \frac{f^{(k-2)}(\lambda)}{(k-2)!} \\ 0 & 0 & f(\lambda) & \cdots & \frac{f^{(k-3)}(\lambda)}{(k-3)!} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & f(\lambda) \end{pmatrix}. \quad (15)$$

证明. 根据 $J_k(\lambda) = \lambda I + N$ (N 为第一上副对角线为 1 的幂零阵, $N^k = 0$)，我们对 f 在 λ 处进行泰勒展开并代入：

$$f(\lambda I + N) = \sum_{j=0}^{\infty} \frac{f^{(j)}(\lambda)}{j!} N^j.$$

由于 $N^k = 0$ ，级数在 N^{k-1} 处自然截断为有限项求和。将这些项按照 N^j 的非零元素位于第 j 条上副对角线这一结构填入矩阵元中，便得到上式。□

对于矩阵指数函数 $f(z) = e^{tz}$ ， $f^{(j)}(z) = t^j e^{tz}$ 。代入命题14.2，我们得到非常实用的核心推论：

$$e^{tJ_k(\lambda)} = e^{\lambda t} \begin{pmatrix} 1 & t & \frac{t^2}{2!} & \cdots & \frac{t^{k-1}}{(k-1)!} \\ 0 & 1 & t & \cdots & \frac{t^{k-2}}{(k-2)!} \\ 0 & 0 & 1 & \cdots & \frac{t^{k-3}}{(k-3)!} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

14.3 常系数线性常微分方程组

有了若尔当块上矩阵指数的显式公式，我们现在装备齐全，可以攻克本节的核心问题——常系数线性微分方程组的求解了。

矩阵指数在分析中最核心的应用之一是求解一阶常系数线性常微分方程组 (ODE)。在一元微积分中，标量方程 $x'(t) = ax(t)$ 的解为 $x(t) = e^{at}x(0)$ 。矩阵指数使我们能够将这个公式几乎逐字推广到向量情形。

定理 14.1 (常系数线性 ODE 组的解). 设 $A \in M_n(\mathbb{C})$, $\mathbf{x}_0 \in \mathbb{C}^n$. 则初值问题

$$\mathbf{x}'(t) = A\mathbf{x}(t), \quad \mathbf{x}(0) = \mathbf{x}_0 \quad (16)$$

存在唯一解

$$\mathbf{x}(t) = e^{tA}\mathbf{x}_0.$$

注 14.2. 关于解的存在唯一性, 属于常微分方程理论的基本定理 (*Picard-Lindelöf* 定理), 在本课程中我们承认该分析结论. 线性代数的贡献在于**显式给出解的构造**. 下面我们验证 $\mathbf{x}(t) = e^{tA}\mathbf{x}_0$ 确实满足方程(16).

验证. 只需逐项对级数求导. 对 $e^{tA} = \sum_{k=0}^{\infty} \frac{t^k}{k!} A^k$ 关于 t 求导 (逐项求导的合法性由一致收敛保证, 我们在此承认这一分析事实), 得到

$$\frac{d}{dt} e^{tA} = \sum_{k=1}^{\infty} \frac{k t^{k-1}}{k!} A^k = \sum_{k=1}^{\infty} \frac{t^{k-1}}{(k-1)!} A^k = A \sum_{j=0}^{\infty} \frac{t^j}{j!} A^j = A e^{tA}.$$

因此 $\mathbf{x}'(t) = \frac{d}{dt}(e^{tA}\mathbf{x}_0) = A e^{tA}\mathbf{x}_0 = A\mathbf{x}(t)$. 又 $\mathbf{x}(0) = e^{0A}\mathbf{x}_0 = I\mathbf{x}_0 = \mathbf{x}_0$, 初值条件满足. \square

关键观察: 由命题14.1(5), 如果 $A = PJP^{-1}$ 是 A 的若尔当标准型, 则 $e^{tA} = P e^{tJ} P^{-1}$. 令 $\mathbf{y}(t) = P^{-1}\mathbf{x}(t)$, 则原方程化为 $\mathbf{y}'(t) = J\mathbf{y}(t)$. 由于 J 是块对角的, 该系统完全**解耦**为各个若尔当块上的独立小系统, 从而可以逐块求解.

(一) **可对角化情形.** 若 A 可对角化, $A = P \operatorname{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$, 其中 P 的列向量 $\mathbf{v}_1, \dots, \mathbf{v}_n$ 为特征向量. 则 $e^{tA} = P \operatorname{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t}) P^{-1}$, 通解可以显式展开为

$$\mathbf{x}(t) = c_1 e^{\lambda_1 t} \mathbf{v}_1 + c_2 e^{\lambda_2 t} \mathbf{v}_2 + \dots + c_n e^{\lambda_n t} \mathbf{v}_n,$$

其中常数 c_i 由初值 $P^{-1}\mathbf{x}_0 = (c_1, \dots, c_n)^T$ 唯一确定. 每一项 $c_i e^{\lambda_i t} \mathbf{v}_i$ 称为系统的一个**模态** (mode): 沿特征方向 \mathbf{v}_i 的独立指数演化.

(二) **不可对角化情形.** 若 A 不可对角化, 若尔当块 $J_k(\lambda)$ 的矩阵指数 (由命题14.2) 使得解中除了指数项 $e^{\lambda t}$ 外, 还出现 t, t^2, \dots, t^{k-1} 的多项式因子. 具体地, 大小为 k 的若尔当块 $J_k(\lambda)$ 对应的解空间中的 k 个独立解为:

$$e^{\lambda t} \mathbf{e}_1, \quad e^{\lambda t} (t\mathbf{e}_1 + \mathbf{e}_2), \quad e^{\lambda t} \left(\frac{t^2}{2!} \mathbf{e}_1 + t\mathbf{e}_2 + \mathbf{e}_3 \right), \quad \dots$$

其中 \mathbf{e}_i 为标准基. 这就是”重特征值产生多项式乘指数解”这一经典现象的本质代数原因.

例 14.3 (可对角化方程组). 求解方程组的通解:

$$\mathbf{x}' = A\mathbf{x}, \quad A = \begin{pmatrix} -1 & -3 \\ 0 & -4 \end{pmatrix}.$$

第一步：求特征值。 A 是上三角阵，特征值为对角元 $\lambda_1 = -1, \lambda_2 = -4$ ，互不相同。

第二步：求特征向量。 $\lambda_1 = -1$: 解 $(A + I)\mathbf{v} = 0$, 即 $\begin{pmatrix} 0 & -3 \\ 0 & -3 \end{pmatrix} \mathbf{v} = 0$, 取 $\mathbf{v}_1 = (1, 0)^T$ 。

$\lambda_2 = -4$: 解 $(A + 4I)\mathbf{v} = 0$, 即 $\begin{pmatrix} 3 & -3 \\ 0 & 0 \end{pmatrix} \mathbf{v} = 0$, 取 $\mathbf{v}_2 = (1, 1)^T$ 。

第三步：写出通解。 由可对角化情形的公式：

$$\mathbf{x}(t) = c_1 e^{-t} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_2 e^{-4t} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} c_1 e^{-t} + c_2 e^{-4t} \\ c_2 e^{-4t} \end{pmatrix}.$$

两个特征值实部均为负，故当 $t \rightarrow \infty$ 时 $\mathbf{x}(t) \rightarrow \mathbf{0}$ ，系统渐近稳定。

例 14.4 (不可对角化方程组). 求解方程组的通解：

$$\mathbf{x}' = A\mathbf{x}, \quad A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

A 有二重特征值 $\lambda = 2$ ，但几何重数为 1 (A 本身已是若尔当块 $J_2(2)$)。由若尔当块的矩阵指数公式：

$$e^{tA} = e^{2t} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

因此通解为

$$\mathbf{x}(t) = e^{2t} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = c_1 e^{2t} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_2 e^{2t} \begin{pmatrix} t \\ 1 \end{pmatrix}.$$

注意第二个独立解 $e^{2t}(t, 1)^T$ 中出现了多项式因子 t ，这正是不可对角化 (只有一个若尔当块) 的直接后果。尽管 e^{2t} 趋于无穷 (因为 $\operatorname{Re}(\lambda) = 2 > 0$)，多项式因子 t 使其增长更快，系统不稳定。

例 14.5 (复特征值与旋转). 考虑简谐振子的相空间方程：

$$\mathbf{x}' = A\mathbf{x}, \quad A = \begin{pmatrix} 0 & -\omega \\ \omega & 0 \end{pmatrix}, \quad \omega > 0.$$

这是一个实的斜对称矩阵，特征值为 $\pm\omega i$ (纯虚数)。我们直接利用矩阵指数的级数定义来计算 e^{tA} 。

注意 $A^2 = -\omega^2 I$ ，从而 $A^3 = -\omega^2 A$ ， $A^4 = \omega^4 I$ ，依此类推，幂次以周期 4 循环 (类比于 i 的幂次)。按奇偶分类求和：

$$e^{tA} = \underbrace{\sum_{m=0}^{\infty} \frac{(-1)^m (\omega t)^{2m}}{(2m)!} \cdot I}_{\cos(\omega t)} + \underbrace{\sum_{m=0}^{\infty} \frac{(-1)^m (\omega t)^{2m+1}}{(2m+1)!} \cdot \frac{A}{\omega}}_{\sin(\omega t)},$$

这里我们承认了正弦和余弦函数的幂级数展开 (即 Euler 公式的实部与虚部)。代入 A 的具体形式:

$$e^{tA} = \begin{pmatrix} \cos(\omega t) & -\sin(\omega t) \\ \sin(\omega t) & \cos(\omega t) \end{pmatrix}.$$

这正是旋转角为 ωt 的旋转矩阵 $R(\omega t) \in \text{SO}(2)$ 。因此, 解 $\mathbf{x}(t) = R(\omega t) \mathbf{x}_0$ 描述了初始点 \mathbf{x}_0 绕原点以角速度 ω 做匀速圆周运动。特征值为纯虚数, 既不衰减也不增长, 对应于中心型 (center) 的稳定行为。

更一般地, 对于实矩阵有复特征值 $\lambda = a \pm bi$ ($b \neq 0$) 的情形, 对应解中会出现 $e^{at} \cos(bt)$ 和 $e^{at} \sin(bt)$ 的组合, 其中 e^{at} 控制振幅的衰减 ($a < 0$, 螺旋汇) 或增长 ($a > 0$, 螺旋源), 而 $\cos(bt), \sin(bt)$ 控制振荡频率。

下面我们给出一个从物理建模到矩阵求解的完整例子, 展示线性 ODE 理论在物理中的典型应用方式。

例 14.6 (耦合弹簧系统——正则模式分析). 两个质量均为 m 的物体 m_1, m_2 排列在一条直线上, 通过三根弹性系数均为 k 的弹簧依次连接在两面固定墙壁之间 (即“墙—弹簧— m_1 —弹簧— m_2 —弹簧—墙”)。设 $x_1(t), x_2(t)$ 分别为两个物体偏离各自平衡位置的位移。

第一步: 建立方程。 对 m_1 , 左侧弹簧提供回复力 $-kx_1$, 右侧弹簧提供力 $-k(x_1 - x_2)$ (当 $x_1 > x_2$ 时被压缩, 推 m_1 向左)。牛顿第二定律给出

$$m\ddot{x}_1 = -kx_1 - k(x_1 - x_2) = -2kx_1 + kx_2.$$

类似地, 对 m_2 : $m\ddot{x}_2 = -k(x_2 - x_1) - kx_2 = kx_1 - 2kx_2$ 。取 $\omega_0^2 = k/m$, 写成矩阵形式:

$$\begin{pmatrix} \ddot{x}_1 \\ \ddot{x}_2 \end{pmatrix} = -\omega_0^2 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

第二步: 化为一阶系统。 引入 $\mathbf{x} = (x_1, x_2, \dot{x}_1, \dot{x}_2)^T$, 则 $\mathbf{x}' = A\mathbf{x}$, 其中

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -2\omega_0^2 & \omega_0^2 & 0 & 0 \\ \omega_0^2 & -2\omega_0^2 & 0 & 0 \end{pmatrix}.$$

第三步: 对角化求解。 实际上, 更高效的方法是先对角化“刚度矩阵” $K = \omega_0^2 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ 。其特征值为 ω_0^2 和 $3\omega_0^2$, 对应的特征向量分别为 $\mathbf{u}_1 = \frac{1}{\sqrt{2}}(1, 1)^T$ 和 $\mathbf{u}_2 = \frac{1}{\sqrt{2}}(1, -1)^T$ 。

引入正则坐标 $q_1 = \frac{x_1+x_2}{\sqrt{2}}$, $q_2 = \frac{x_1-x_2}{\sqrt{2}}$, 系统完全解耦为两个独立的简谐振子:

$$\ddot{q}_1 = -\omega_0^2 q_1, \quad \ddot{q}_2 = -3\omega_0^2 q_2.$$

因此, $q_1(t) = A_1 \cos(\omega_0 t + \phi_1)$, $q_2(t) = A_2 \cos(\sqrt{3}\omega_0 t + \phi_2)$ 。

第四步: 物理解读。 两个正则模式 (normal modes) 具有清晰的物理含义:

- **低频模式** (频率 ω_0) : q_1 振动而 $q_2 = 0$, 即 $x_1 = x_2$, 两个质量**同向**振动, 中间的弹簧不被压缩。
- **高频模式** (频率 $\sqrt{3}\omega_0$) : q_2 振动而 $q_1 = 0$, 即 $x_1 = -x_2$, 两个质量**反向**振动, 中间的弹簧被额外压缩, 因此等效劲度系数更大, 频率更高。

一般运动是这两个正则模式的线性叠加。这就是**谱分析**思想的物理原型: 对角化将耦合系统分解为独立模态, 而特征值决定了各模态的固有频率。同样的方法在分子振动光谱、固体物理的声子色散关系、以及建筑结构的抗震分析中都有广泛应用。

14.4 高阶标量 ODE 的矩阵降阶法

在物理和工程中, 我们更经常遇到的是**单个高阶微分方程** (如弹簧振子方程 $mx'' + cx' + kx = 0$), 而非直接以方程组的形式出现。好消息是, 任何高阶方程都可以通过引入辅助变量化为一阶方程组——这使得上面的全部理论立刻适用。

正如在上一小节 (递推数列) 中我们利用友阵 (§8.8) 将高次线性递推化作一阶系统, 对于高阶线性齐次常微分方程, 若尔当理论同样提供完全平行的统一框架。

考虑 k 阶常系数齐次标量微分方程:

$$y^{(k)} + c_{k-1}y^{(k-1)} + c_{k-2}y^{(k-2)} + \cdots + c_1y' + c_0y = 0, \quad (17)$$

其中 c_0, c_1, \dots, c_{k-1} 为常数, 初值条件为 $y(0), y'(0), \dots, y^{(k-1)}(0)$ 给定。

引入状态向量 $\mathbf{x}(t) = (y(t), y'(t), \dots, y^{(k-1)}(t))^T \in \mathbb{C}^k$ 。注意到 $\mathbf{x}(t)$ 的前 $k-1$ 个分量的导数恰好是下一个分量本身 (即 $(y^{(j)})' = y^{(j+1)}$), 而最后一个分量的导数 $y^{(k)}$ 则由方程(17)表示为前面各分量的线性组合。因此方程(17)等价于一阶向量 ODE 系统 $\mathbf{x}'(t) = C\mathbf{x}(t)$, 其中转移矩阵为:

$$C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{k-1} \end{pmatrix} \in M_k(\mathbb{C}).$$

这恰好是多项式 $f(\lambda) = \lambda^k + c_{k-1}\lambda^{k-1} + \cdots + c_1\lambda + c_0$ 的**友阵** (见定义8.15的转置形式)。对应的**特征方程**即为 $f(\lambda) = 0$ 。

由命题8.11, 友阵的极小多项式等于特征多项式, 从而每个特征值的几何重数必然为 1。一旦有重根出现, C 就不可对角化, 若尔当标准型中必然出现高阶若尔当块。结合上一小节矩阵指数在若尔当块上的显式公式, 我们可以完整地刻画通解的结构。

定理 14.2 (高阶常系数齐次线性 ODE 的通解). 设方程(17)的特征方程 $f(\lambda) = 0$ 在 \mathbb{C} 中有 s 个不同的根 $\lambda_1, \dots, \lambda_s$, 代数重数分别为 m_1, \dots, m_s ($\sum_{i=1}^s m_i = k$). 则方程(17)的通解空间是一个 k 维 \mathbb{C} -线性空间, 由如下 k 个线性无关的基函数张成:

$$\{t^j e^{\lambda_i t} \mid 1 \leq i \leq s, 0 \leq j \leq m_i - 1\}.$$

因此, 通解为

$$y(t) = \sum_{i=1}^s P_i(t) e^{\lambda_i t}, \quad (18)$$

其中每个 $P_i(t) = \alpha_{i,0} + \alpha_{i,1}t + \dots + \alpha_{i,m_i-1}t^{m_i-1}$ 是关于 t 的次数不超过 $m_i - 1$ 的多项式, 共含 k 个待定常数, 完全由初值条件唯一确定.

证明. 将方程(17)化为一阶系统 $\mathbf{x}' = C\mathbf{x}$ 后, 解为 $\mathbf{x}(t) = e^{tC}\mathbf{x}(0)$. 设 C 的若尔当标准型为 $C = PJP^{-1}$, 其中 $J = \text{diag}(J_{m_1}(\lambda_1), \dots, J_{m_s}(\lambda_s))$ (因为友阵每个特征值几何重数为 1, 所以每个 λ_i 恰好对应一个大小为 m_i 的若尔当块). 那么

$$e^{tC} = P \text{diag}(e^{tJ_{m_1}(\lambda_1)}, \dots, e^{tJ_{m_s}(\lambda_s)}) P^{-1}.$$

由若尔当块的矩阵指数公式 (命题14.2), $e^{tJ_{m_i}(\lambda_i)}$ 的第 (α, β) 元素 (当 $\beta \geq \alpha$) 为 $\frac{t^{\beta-\alpha}}{(\beta-\alpha)!} e^{\lambda_i t}$. 因此 e^{tC} 的每个元素都是形如 $t^j e^{\lambda_i t}$ ($0 \leq j \leq m_i - 1$) 的项的线性组合. $\mathbf{x}(t)$ 的第一个分量即 $y(t)$, 它自然也是这些基函数的线性组合.

反过来, 直接验证 $y(t) = t^j e^{\lambda t}$ ($0 \leq j \leq m - 1$) 确实满足方程(17)(当 λ 是 f 的 m 重根时): 代入方程后, 利用莱布尼兹求导公式 $(t^j e^{\lambda t})^{(n)} = \sum_{l=0}^j \binom{n}{l} \frac{j!}{(j-l)!} t^{j-l} \lambda^{n-l} e^{\lambda t}$, 整理可证所有项恰好在 $(\lambda - \lambda_i)^{m_i} \mid f(\lambda)$ 的条件下消去.

这 k 个函数的线性无关性由 e^{tC} 的可逆性保证 (或等价地, 由不同指数函数和多项式调制函数的线性无关性, 即经典的广义范德蒙行列式非零). 维数等于 k 则由 ODE 理论中初值问题的解的唯一性给出. \square

注 14.3. 将定理 14.2 与离散递推数列的定理 13.5 对比, 可以清晰地看到 "离散 vs 连续" 的完美对偶:

离散递推	连续 ODE
$\mathbf{x}_{n+1} = C\mathbf{x}_n$	$\mathbf{x}'(t) = C\mathbf{x}(t)$
解: $\mathbf{x}_n = C^n \mathbf{x}_0$	解: $\mathbf{x}(t) = e^{tC} \mathbf{x}_0$
基函数: $n^j \lambda_i^n$	基函数: $t^j e^{\lambda_i t}$
稳定性: $ \lambda_i < 1$	稳定性: $\text{Re}(\lambda_i) < 0$

两者共享同一个友阵 C 和同一组特征根, 只是 λ^n 被 $e^{\lambda t}$ 所替换.

例 14.7 (含重根的二阶 ODE). 求解初值问题

$$y'' + 2y' + y = 0, \quad y(0) = 3, \quad y'(0) = 1.$$

特征方程为 $\lambda^2 + 2\lambda + 1 = (\lambda + 1)^2 = 0$, 有二重根 $\lambda = -1$ ($m = 2$)。

方法一 (直接用定理 14.2): 通解为

$$y(t) = (\alpha_0 + \alpha_1 t) e^{-t}.$$

代入初值: $y(0) = \alpha_0 = 3$; $y'(t) = (\alpha_1 - \alpha_0 - \alpha_1 t)e^{-t}$, 故 $y'(0) = \alpha_1 - \alpha_0 = 1$, 解得 $\alpha_1 = 4$ 。

$$y(t) = (3 + 4t) e^{-t}.$$

方法二 (矩阵指数法): 引入 $\mathbf{x} = (y, y')^T$, 友阵为

$$C = \begin{pmatrix} 0 & 1 \\ -1 & -2 \end{pmatrix}.$$

C 的若尔当标准型为 $J_2(-1) = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$, 过渡矩阵 $P = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ (满足 $C = PJ_2(-1)P^{-1}$)。

于是

$$e^{tC} = P \begin{pmatrix} e^{-t} & te^{-t} \\ 0 & e^{-t} \end{pmatrix} P^{-1} = e^{-t} \begin{pmatrix} 1+t & t \\ -t & 1-t \end{pmatrix}.$$

代入 $\mathbf{x}(0) = (3, 1)^T$:

$$\begin{pmatrix} y(t) \\ y'(t) \end{pmatrix} = e^{-t} \begin{pmatrix} 1+t & t \\ -t & 1-t \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = e^{-t} \begin{pmatrix} 3+4t \\ -3t+1-t \end{pmatrix} = e^{-t} \begin{pmatrix} 3+4t \\ 1-4t \end{pmatrix}.$$

因此 $y(t) = (3 + 4t)e^{-t}$, 与方法一完全一致。注意到 $y'(t) = (1 - 4t)e^{-t}$, 亦可直接验证。

14.5 系统的稳定性

求出通解固然重要, 但在许多实际问题中, 我们更关心的是解的**长期行为**: 一座桥梁在风中会不会越摆越大直到垮塌? 一个控制系统受到外界干扰后能否自动回到设定值? 一颗人造卫星的轨道在微小扰动下会不会偏离? 所有这些问题都可以抽象为同一个数学问题: 线性系统 $\mathbf{x}' = A\mathbf{x}$ 的解当 $t \rightarrow \infty$ 时是否趋于零?

在前面的例题中, 我们已经多次非正式地提到“稳定”与“不稳定”: 例 14.3 中两个负实特征值导致解衰减至零 (渐近稳定); 例 14.4 中正实特征值导致解发散 (不稳定); 例 14.5 中纯虚特征值导致解在圆轨道上永续运动 (稳定但不衰减)。这些现象并非巧合, 而是由**特征值的实部**这一统一的代数指标所完全决定的。本小节将系统地阐述这一联系。

动机: 阻尼谐振子。考虑经典的弹簧-阻尼器系统: 质量为 m 的物体连接在弹性系数为 k 的弹簧上, 并受到与速度成正比的阻尼力 (阻尼系数 $c \geq 0$)。牛顿第二定律给出

$$m\ddot{x} + c\dot{x} + kx = 0, \quad m, k > 0, c \geq 0.$$

引入两个无量纲参数：**固有频率** $\omega_n = \sqrt{k/m}$ (无阻尼时系统的振动角频率) 和**阻尼比** $\zeta = \frac{c}{2\sqrt{mk}}$ (衡量阻尼强度相对于临界值的比例)，方程化为标准形式

$$x'' + 2\zeta\omega_n x' + \omega_n^2 x = 0. \quad (19)$$

其特征方程为

$$\lambda^2 + 2\zeta\omega_n \lambda + \omega_n^2 = 0, \quad \lambda = -\zeta\omega_n \pm \omega_n \sqrt{\zeta^2 - 1}.$$

随着阻尼比 ζ 从零到大于1的变化，特征根在复平面上的位置发生质变，对应着截然不同的物理行为：

阻尼比	特征根	物理行为	稳定性
$\zeta = 0$	$\pm\omega_n i$ (纯虚)	无阻尼自由振动	稳定 (非渐近)
$0 < \zeta < 1$	$a \pm bi, a < 0$	欠阻尼振荡衰减	渐近稳定
$\zeta = 1$	$-\omega_n$ (二重根)	临界阻尼	渐近稳定
$\zeta > 1$	两个不等负实根	过阻尼指数衰减	渐近稳定

例 14.8 (阻尼谐振子的四种模式). 取 $\omega_n = 1$ (即 $m = k = 1$), 初值 $x(0) = 1, x'(0) = 0$, 分别考虑以下情形。

(i) **无阻尼** ($\zeta = 0$): 特征根 $\lambda = \pm i$, 通解 $x(t) = \cos t$ 。系统做等幅简谐振动，能量守恒。

(ii) **欠阻尼** ($\zeta = 0.2$): 特征根 $\lambda = -0.2 \pm 0.98i$ (近似), 通解含因子 $e^{-0.2t}(\cos 0.98t + \dots)$ 。系统做振幅指数衰减的振荡，衰减速率由 $|\operatorname{Re}(\lambda)| = 0.2$ 决定。

(iii) **临界阻尼** ($\zeta = 1$): 二重根 $\lambda = -1$, 由定理 14.2, 通解 $x(t) = (1+t)e^{-t}$ 。系统以最快的非振荡方式回到平衡位置——这正是门禁阻尼器、汽车悬挂系统所追求的理想阻尼。

(iv) **过阻尼** ($\zeta = 2$): 特征根 $\lambda_1 = -2 + \sqrt{3} \approx -0.27, \lambda_2 = -2 - \sqrt{3} \approx -3.73$, 通解为两个衰减指数的叠加。系统缓慢回到平衡，不振荡，但比临界阻尼更慢。

上述四种情形的共同特点是：**所有特征值的实部 ≤ 0** 。当且仅当所有特征值实部**严格**小于零时 (即 $\zeta > 0$)，系统才渐近稳定，解最终趋于零。当 $\zeta = 0$ 时，纯虚特征值仅给出有界但不衰减的振荡。这促使我们对一般线性系统的稳定性给出精确的定义和完整的刻画。

稳定性的严格定义。考虑一般的线性系统 $\mathbf{x}'(t) = A\mathbf{x}(t)$ ($A \in M_n(\mathbb{R})$ 或 $M_n(\mathbb{C})$)，其平衡点 (又称**不动点**或**奇点**) 为 $\mathbf{x}_0 = \mathbf{0}$ ¹²。以下定义中 $\|\cdot\|$ 表示 \mathbb{R}^n (或 \mathbb{C}^n) 上的任意范数¹³。

定义 14.2 (平衡点的稳定性). 设 $\mathbf{x}'(t) = A\mathbf{x}(t)$ 是 \mathbb{R}^n (或 \mathbb{C}^n) 上的线性 ODE 系统。

¹²若方程为 $\mathbf{x}' = A\mathbf{x} + \mathbf{b}$ 且 $\mathbf{b} \neq \mathbf{0}$, 平衡点为 $-A^{-1}\mathbf{b}$ (当 A 可逆时), 平移后化为齐次方程即可。

¹³在有限维空间上, 所有范数都是等价的, 因此稳定性的定义不依赖于范数的选取。

1. 原点称为**稳定的** (*Lyapunov stable*), 如果对任意 $\varepsilon > 0$, 存在 $\delta > 0$, 使得只要初值满足 $\|\mathbf{x}(0)\| < \delta$, 则解对所有 $t \geq 0$ 满足 $\|\mathbf{x}(t)\| < \varepsilon$. 直观地说, 初始点足够靠近原点的轨道永远不会远离。
2. 原点称为**渐近稳定的** (*asymptotically stable*), 如果它是稳定的, 且进一步地 $\|\mathbf{x}(t)\| \rightarrow 0$ ($t \rightarrow \infty$)。
3. 原点称为**不稳定的** (*unstable*), 如果它不是稳定的, 即存在某个 $\varepsilon > 0$ 使得无论多么小的初始扰动都有可能使轨道最终偏离原点距离达到 ε 。

注 14.4. 对于线性系统 $\mathbf{x}' = A\mathbf{x}$, 由于解 $\mathbf{x}(t) = e^{tA}\mathbf{x}(0)$ 是关于初值的线性函数, 定义中“局部”的限制 ($\|\mathbf{x}(0)\| < \delta$) 实际上是不必要的——如果一个线性系统渐近稳定, 则任意初值的解都趋于零。这一点与非线性系统截然不同 (参见后文关于非线性系统的讨论)。

例 14.9 (稳定性判据前的三个低阶模型). 在阅读一般判据前, 先看最小的几个模型。

(1) **一维模型.** 若 $x' = \lambda x$, 则 $x(t) = e^{\lambda t}x(0)$. 因此 $\lambda < 0$ 时解趋于 0, $\lambda = 0$ 时解保持常数, $\lambda > 0$ 时除零解外都会指数增长. 这解释了为什么特征值实部的正负是稳定性的核心。

(2) **一个衰减方向和一个不动方向.** 若

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

则

$$e^{tA} = \begin{pmatrix} e^{-t} & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} e^{-t}x_1(0) \\ x_2(0) \end{pmatrix}.$$

轨道不会远离原点, 但一般不会趋于原点. 所以原点稳定, 但不渐近稳定。

(3) **零特征值上的二阶若尔当块.** 若

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

则 $N^2 = 0$, 因而

$$e^{tN} = I + tN = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

此时

$$\begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = \begin{pmatrix} x_1(0) + tx_2(0) \\ x_2(0) \end{pmatrix}.$$

即使初值很小, 只要 $x_2(0) \neq 0$, 第一坐标也会随 t 线性增长. 这说明: 特征值实部等于 0 时, 只有 1×1 的若尔当块才允许稳定; 更大的若尔当块会带来多项式增长。

以下定理将稳定性问题完全归结为特征值的代数计算。

定理 14.3 (线性系统稳定性的特征值判据). 设 $A \in M_n(\mathbb{C})$, $\lambda_1, \dots, \lambda_s$ 为 A 的所有不同特征值. 则线性系统 $\mathbf{x}'(t) = A\mathbf{x}(t)$ 的原点:

1. **渐近稳定** \iff 所有特征值满足 $\operatorname{Re}(\lambda_i) < 0$ ($1 \leq i \leq s$).
2. **稳定 (但不渐近稳定)** \iff 所有特征值满足 $\operatorname{Re}(\lambda_i) \leq 0$, 至少有一个特征值满足 $\operatorname{Re}(\lambda_i) = 0$, 且每个 $\operatorname{Re}(\lambda_i) = 0$ 的特征值对应的若尔当块全部为 1×1 的 (即该特征值的几何重数等于代数重数).
3. **不稳定** \iff 存在某个特征值 $\operatorname{Re}(\lambda_i) > 0$; 或者存在某个 $\operatorname{Re}(\lambda_i) = 0$ 的特征值对应的若尔当块大小 ≥ 2 .

证明. 关键在于利用若尔当标准型将问题分解为逐块分析. 设 $A = PJP^{-1}$, 其中 $J = \operatorname{diag}(J_{k_1}(\lambda_1), \dots, J_{k_r}(\lambda_r))$. 由于 $e^{tA} = P e^{tJ} P^{-1}$, 而 e^{tJ} 是块对角的, 每一块为

$$e^{tJ_k(\lambda)} = e^{\operatorname{Re}(\lambda)t} \cdot \begin{pmatrix} e^{i\operatorname{Im}(\lambda)t} & t e^{i\operatorname{Im}(\lambda)t} & \dots & \frac{t^{k-1}}{(k-1)!} e^{i\operatorname{Im}(\lambda)t} \\ 0 & e^{i\operatorname{Im}(\lambda)t} & \dots & \frac{t^{k-2}}{(k-2)!} e^{i\operatorname{Im}(\lambda)t} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & e^{i\operatorname{Im}(\lambda)t} \end{pmatrix},$$

因此每个矩阵元素的模为 $|(e^{tJ_k(\lambda)})_{\alpha\beta}| = \frac{t^{\beta-\alpha}}{(\beta-\alpha)!} e^{\operatorname{Re}(\lambda)t}$ (当 $\beta \geq \alpha$).

(1) 若 $\operatorname{Re}(\lambda) < 0$, 则对每个多项式次数 j , 有 $t^j e^{\operatorname{Re}(\lambda)t} \rightarrow 0$ ($t \rightarrow \infty$), 因为指数衰减总是压制多项式增长. 因此 $e^{tJ_k(\lambda)} \rightarrow 0$. 若所有块都如此, 则 $e^{tA} \rightarrow 0$, 从而对任意初值 $\mathbf{x}(t) = e^{tA}\mathbf{x}(0) \rightarrow \mathbf{0}$, 即渐近稳定.

反之, 若存在某个 $\operatorname{Re}(\lambda_i) \geq 0$, 取初值沿该若尔当块对应的 (广义) 特征向量方向, 则解中含有 $e^{\operatorname{Re}(\lambda_i)t}$ 因子 (可能乘以多项式), 不趋于零.

(2) 若 $\operatorname{Re}(\lambda) = 0$ 且若尔当块为 1×1 , 则该块的贡献为 $e^{i\operatorname{Im}(\lambda)t}$, 模恒为 1 (纯旋转), 解有界但不衰减. 若所有 $\operatorname{Re}(\lambda) \leq 0$ 的块都满足此条件, 再加上 $\operatorname{Re}(\lambda) < 0$ 的块趋于零, 则整个 e^{tA} 有界, 系统稳定. 若确实存在实部为 0 的特征值, 则这部分的解一般不会趋于 0, 所以系统不是渐近稳定.

反之, 若某个 $\operatorname{Re}(\lambda) = 0$ 的特征值对应大小 $k \geq 2$ 的若尔当块, 则该块中出现 $t^j e^{i\operatorname{Im}(\lambda)t}$ ($j \geq 1$) 项, 其模为 t^j , 随 $t \rightarrow \infty$ 无界增长, 系统不稳定. \square

注 14.5. 在工程控制论中, 满足 $\operatorname{Re}(\lambda) < 0$ 的特征值称为**稳定极点**, 而那些 $\operatorname{Re}(\lambda) \geq 0$ 的称为**不稳定极点**. 定理告诉我们: 一个线性系统渐近稳定当且仅当其所有极点都位于复平面的开左半平面. 这正是经典控制理论中 **Routh-Hurwitz 判据**和 **Nyquist 稳定性判据**所检验的条件.

二维线性系统的典型相图. 定理14.3给出了任意维数下的稳定性判据. 当 $n = 2$ 时, 特征值的可能类型十分有限, 我们可以先列出二维线性系统 $\mathbf{x}' = A\mathbf{x}$ ($A \in M_2(\mathbb{R})$) 最常见的

几类相图。所谓**相图** (phase portrait), 是指在 (x_1, x_2) 平面上绘出的解曲线 (轨线) 族以及流向箭头。不同的特征值类型对应着拓扑上截然不同的相图结构。

为方便讨论, 设 A 的特征多项式为 $\lambda^2 - \tau\lambda + \delta$, 其中 $\tau = \text{tr}(A)$, $\delta = \det(A)$, 判别式 $\Delta = \tau^2 - 4\delta$ 。特征根为 $\lambda = \frac{\tau \pm \sqrt{\Delta}}{2}$ 。

1. **稳定结点** (stable node): $\Delta > 0, \lambda_1 < \lambda_2 < 0$ (两个不等负实根)。所有轨线沿特征方向 $\mathbf{v}_1, \mathbf{v}_2$ 趋于原点, 远离原点时沿衰减较慢的 \mathbf{v}_2 方向靠拢 (因 $|\lambda_2| < |\lambda_1|$), 原点渐近稳定。
2. **不稳定结点** (unstable node): $\Delta > 0, 0 < \lambda_1 < \lambda_2$ (两个不等正实根)。将稳定结点的时间反向即得——所有轨线从原点发散。
3. **鞍点** (saddle point): $\Delta > 0, \lambda_1 < 0 < \lambda_2$ (一正一负实根)。轨线沿 \mathbf{v}_1 方向趋于原点, 沿 \mathbf{v}_2 方向远离, 一般轨线呈双曲线形状。原点不稳定。
4. **螺旋汇** (stable spiral/focus): $\Delta < 0, \text{Re}(\lambda) < 0$ (共轭复根, 负实部)。轨线螺旋地趋向原点, 旋转方向由 A 的反对称部分决定。原点渐近稳定。
5. **中心** (center): $\Delta < 0, \text{Re}(\lambda) = 0$ (纯虚共轭根)。轨线为围绕原点的封闭椭圆 (或被 A 变形的椭圆)。原点稳定但不渐近稳定。
6. **退化结点** (degenerate/improper node): $\Delta = 0, \lambda_1 = \lambda_2 < 0$ (负二重根), 且若尔当块为 $J_2(\lambda)$ (即 A 不可对角化)。轨线沿唯一的特征方向切入原点, 呈“偏向一侧的结点”形态。原点渐近稳定。

图21展示了这六种典型相图, 我们用具体的矩阵绘制解曲线。

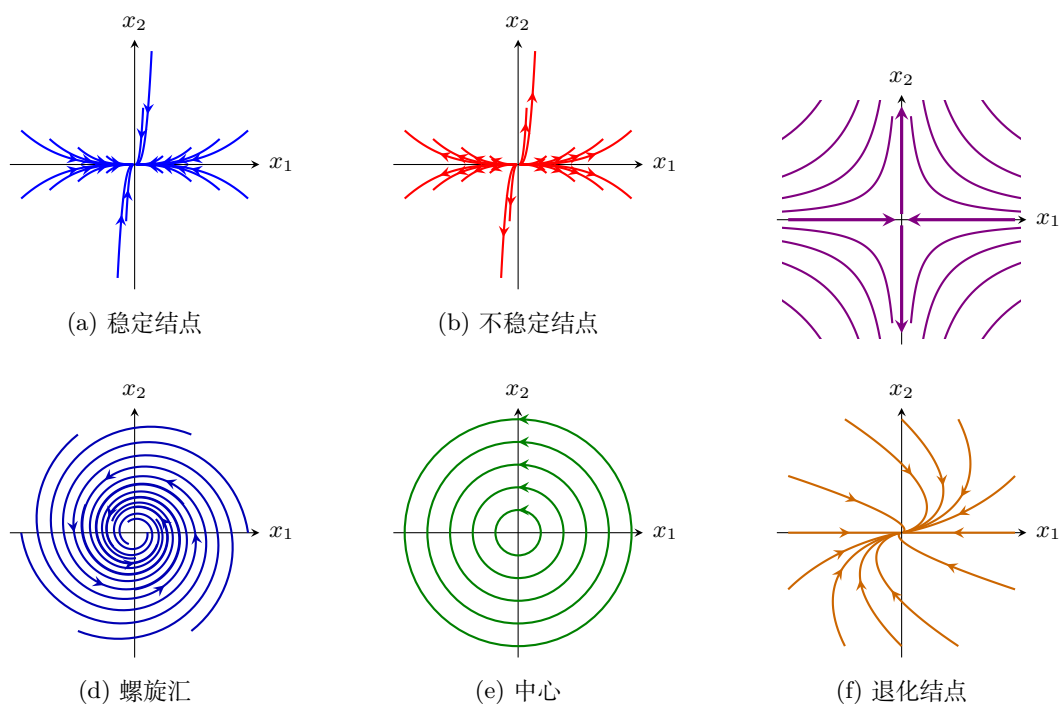


图 21: 二维线性系统 $\mathbf{x}' = A\mathbf{x}$ 的六种典型相图。箭头指示 t 增大的方向 (流向)。

注 14.6. 图 21 只展示六种最常见的典型相图。完整分类还要包括若干反向或边界情形: 当 $\Delta < 0$ 且 $\text{Re}(\lambda) > 0$ 时得到**螺旋源**; 当 $\Delta = 0$ 且二重特征值为正并且不可对角化时得到**不稳定退化结点**; 当 $\Delta = 0$ 且 $A = \lambda I$ 时所有方向都是特征方向, 轨线为通过原点的径向射线, 称为**星形结点** ($\lambda < 0$ 稳定, $\lambda > 0$ 不稳定); 当 $\delta = \det(A) = 0$ 时, A 有零特征值, 原点通常不再是孤立平衡点, 可能出现一条或整个平面的不动点。

上述相图的几何结构可以通过以下方式理解。设 A 可对角化 (或化为若尔当标准型), 令 P 为过渡矩阵, $\mathbf{y} = P^{-1}\mathbf{x}$, 则在 \mathbf{y} -坐标下系统变为 $\mathbf{y}' = J\mathbf{y}$, 其解的几何意义是“标准的” (对角情形为沿坐标轴的独立指数运动, 旋转情形为等速圆周运动)。变换 $\mathbf{x} = P\mathbf{y}$ 是一个线性变换, 它将标准相图做了一个线性变形 (椭圆代替圆、斜方向代替坐标轴方向), 但拓扑结构 (稳定/不稳定、旋转方向等) 保持不变。

非线性系统的线性化。 以上讨论限于常系数线性系统 $\mathbf{x}' = A\mathbf{x}$ 。然而, 自然界中绝大多数微分方程是**非线性的**。考虑一般的自治系统

$$\mathbf{x}'(t) = \mathbf{f}(\mathbf{x}(t)), \quad (20)$$

其中 $\mathbf{f}: U \rightarrow \mathbb{R}^n$ 是定义在开集 $U \subseteq \mathbb{R}^n$ 上的光滑 (至少 C^1) 向量场。向量 $\mathbf{x}_0 \in U$ 称为系统的**平衡点** (或**奇点**), 如果 $\mathbf{f}(\mathbf{x}_0) = \mathbf{0}$ 。

对于非线性系统，我们无法写出像 $e^{tA}\mathbf{x}_0$ 这样的全局解析解。但是，线性代数为我们提供了一个强有力的**局部**分析工具：在平衡点附近做泰勒展开。

设 \mathbf{x}_0 是方程(20)的平衡点。令 $\mathbf{y} = \mathbf{x} - \mathbf{x}_0$ 为偏离平衡点的小扰动，则

$$\mathbf{y}' = \mathbf{f}(\mathbf{x}_0 + \mathbf{y}) = \underbrace{\mathbf{f}(\mathbf{x}_0)}_{=0} + D\mathbf{f}(\mathbf{x}_0)\mathbf{y} + O(\|\mathbf{y}\|^2),$$

其中

$$D\mathbf{f}(\mathbf{x}_0) = \left(\frac{\partial f_i}{\partial x_j}(\mathbf{x}_0) \right)_{1 \leq i, j \leq n} \in M_n(\mathbb{R})$$

是 \mathbf{f} 在 \mathbf{x}_0 处的 **Jacobian 矩阵**（即全微分/导数矩阵）。当 \mathbf{y} 很小时，高阶项 $O(\|\mathbf{y}\|^2)$ 可以忽略，于是在 \mathbf{x}_0 附近，非线性系统近似为**线性化系统**

$$\mathbf{y}' = D\mathbf{f}(\mathbf{x}_0)\mathbf{y}. \quad (21)$$

这正是我们已经完整分析过的常系数线性 ODE！由此，Jacobian 矩阵 $D\mathbf{f}(\mathbf{x}_0)$ 的特征值就成为了判断非线性系统在平衡点附近行为的关键。

一个自然的问题是：线性化系统(21)的定性行为能否忠实地反映原非线性系统(20)在 \mathbf{x}_0 附近的行为？以下定理给出了肯定的回答（在一定条件下）。

定理 14.4 (Hartman–Grobman 定理(非正式表述)). 设 \mathbf{x}_0 是方程(20)的平衡点, 且 *Jacobian* 矩阵 $D\mathbf{f}(\mathbf{x}_0)$ 的所有特征值实部均非零 (即 $\operatorname{Re}(\lambda_i) \neq 0, \forall i$). 则称 \mathbf{x}_0 为**双曲平衡点** (*hyperbolic equilibrium*). 此时, 在 \mathbf{x}_0 的某个邻域内, 非线性系统(20)的相图与其线性化系统(21)的相图是**拓扑等价**的——即存在一个保持轨线方向的同胚映射将前者的轨线映为后者的轨线。

注 14.7. *Hartman–Grobman* 定理的严格证明超出了本课程的范围 (需要用到 *Banach* 不动点定理和微分方程的稳定流形理论), 我们在此仅承认其结论。该定理的核心意义在于: 对于双曲平衡点, *Jacobian* 矩阵的线性化信息足以判断非线性系统在该平衡点附近的**拓扑类型**; 在二维情形中, 只需计算 *Jacobian* 矩阵的特征值, 然后按照图 21 及上述补充情形读出局部相图。

但需要特别警惕的是: 当 $D\mathbf{f}(\mathbf{x}_0)$ 存在**纯虚特征值** (即 $\operatorname{Re}(\lambda) = 0$) 时, 平衡点不是双曲的, *Hartman–Grobman* 定理**不适用**。此时线性化系统给出”中心”的判定, 但非线性项可能将其变为螺旋汇 (渐近稳定) 或螺旋源 (不稳定)。要确定这种情形下的稳定性, 需要更精细的工具, 如 *Lyapunov* 函数法或**中心流形理论**。

总结而言, 对于非线性系统的每个平衡点, 分析步骤为:

1. 求出所有平衡点 \mathbf{x}_0 (解方程 $\mathbf{f}(\mathbf{x}_0) = \mathbf{0}$)。
2. 计算 *Jacobian* 矩阵 $D\mathbf{f}(\mathbf{x}_0)$ 。
3. 求 $D\mathbf{f}(\mathbf{x}_0)$ 的特征值。

4. 若所有特征值实部非零（双曲情形），则由 Hartman–Grobman 定理，直接按线性系统的分类判断局部相图和稳定性。
5. 若存在纯虚特征值，则需要额外分析。

下面我们用一个经典的物理例子来演示上述分析流程。

例 14.10 (无阻尼单摆). 考虑无阻尼的理想单摆：一根长度为 l 的不可伸长轻杆，一端固定，另一端悬挂质量为 m 的质点，在重力场 g 中自由摆动。设 θ 为摆角（以竖直向下为零），则运动方程为

$$\theta'' = -\frac{g}{l} \sin \theta.$$

归一化取 $g/l = 1$ ，并引入状态变量 $x_1 = \theta$ （角位移）、 $x_2 = \theta'$ （角速度），写成一阶系统：

$$\begin{cases} x_1' = x_2, \\ x_2' = -\sin x_1. \end{cases}$$

即 $\mathbf{f}(x_1, x_2) = (x_2, -\sin x_1)^T$ 。

第一步：求平衡点。 解 $\mathbf{f}(x_1, x_2) = \mathbf{0}$ ，即 $x_2 = 0, \sin x_1 = 0$ ，得

$$\mathbf{x}_0 = (n\pi, 0), \quad n \in \mathbb{Z}.$$

其中偶数 n 对应摆锤在**最低点** ($\theta = 0, \pm 2\pi, \dots$ ，即自然悬垂位置)，奇数 n 对应摆锤在**最高点** ($\theta = \pm\pi, \pm 3\pi, \dots$ ，即倒立位置)。按周期性，本质上只需分析两类平衡点： $(0, 0)$ 和 $(\pi, 0)$ 。

第二步：计算 Jacobian 矩阵。

$$D\mathbf{f}(x_1, x_2) = \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -\cos x_1 & 0 \end{pmatrix}.$$

第三步：在每个平衡点处求特征值。

平衡点 $(0, 0)$ (最低点)：

$$D\mathbf{f}(0, 0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \text{特征值 } \lambda = \pm i.$$

这正是例 14.5 中的简谐振子矩阵！特征值为纯虚数，线性化系统给出“中心”的判定。但请注意：由于 $\operatorname{Re}(\lambda) = 0$ ，平衡点**不是双曲的**，Hartman–Grobman 定理不直接适用。不过，对于无阻尼单摆，可以通过守恒量（能量函数）

$$E(\theta, \dot{\theta}) = \frac{1}{2}\dot{\theta}^2 - \cos \theta$$

证明 $(0,0)$ 确实是中心型的——附近的轨道是围绕原点的闭合曲线（对应于小幅摆动），这与线性化的预测一致。物理上，这就是我们熟知的钟摆做小角度近似下的简谐运动。

平衡点 $(\pi,0)$ （倒立位置）：

$$Df(\pi,0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{特征值 } \lambda = \pm 1.$$

一正一负实特征值：这是一个鞍点，且是双曲的 $(\text{Re}(\lambda) \neq 0)$ 。由 *Hartman-Grobman* 定理，非线性系统在 $(\pi,0)$ 附近的相图拓扑上等价于线性鞍点（图 21(c)）。物理上，倒立摆是不稳定的——任何微小的扰动都会导致摆锤偏离倒立位置。

第四步：绘制全局相图。 图 22 展示了单摆在 $(\theta, \dot{\theta})$ 平面上的相图。中心 $(0,0)$ 被闭合轨道（振动解）包围；鞍点 $(\pm\pi,0)$ 之间由分离线（*separatrix*，对应能量 $E = 1$ 的特殊轨道）相连。分离线以外的轨道对应摆锤做旋转运动（越过最高点，不断转圈）。

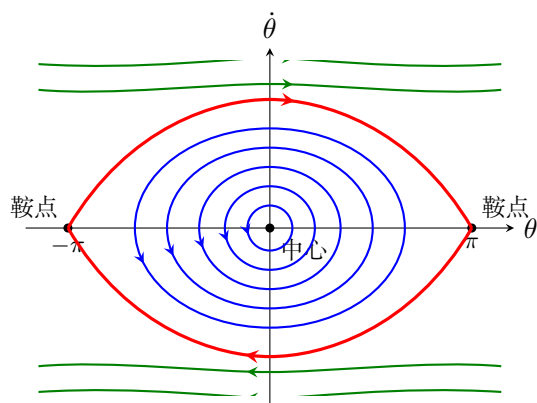


图 22: 无阻尼单摆的相图（示意）。蓝色闭合轨道对应振动解 $(E < 1)$ ，红色粗线为分离线 $(E = 1, \text{异宿轨道})$ ，绿色轨道对应旋转解 $(E > 1)$ 。原点 $(0,0)$ 为中心， $(\pm\pi,0)$ 为鞍点。

注 14.8. 单摆例子完美地展示了线性代数在非线性动力系统分析中的威力：仅凭 *Jacobian* 矩阵这一个 2×2 矩阵的特征值，就能判定两类平衡点的定性行为——中心（小振动）与鞍点（倒立不稳定）。这一思想在更高维的系统中同样适用：无论系统多么复杂，平衡点附近的行为总是由 *Jacobian* 矩阵的若尔当标准型所主宰。

14.6 习题

14.6.1 练习题

习题 14.1（矩阵指数与旋转）。设

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

1. 计算 A^2, A^3, A^4 .

2. 利用幂级数证明

$$e^{tA} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}.$$

3. 求微分方程 $x'(t) = Ax(t)$, $x(0) = (1, 0)^T$ 的解, 并画出轨迹.

习题 14.2 (矩阵指数的直接计算). 计算下列矩阵的矩阵指数 e^A :

1. $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$

2. $A = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix};$

3. $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};$

4. $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$

习题 14.3 (矩阵指数的基本性质). 证明命题 14.1 中的以下两条:

1. 若 $AB = BA$, 则 $e^{A+B} = e^A e^B$.

(提示: 展开两边的级数, 利用 $AB = BA$ 使得二项式定理 $(A+B)^k = \sum_{j=0}^k \binom{k}{j} A^j B^{k-j}$ 成立.)

2. $\det(e^A) = e^{\text{tr}(A)}$.

(提示: 先对上三角矩阵证明, 再利用相似不变性推广到一般情形.)

习题 14.4 (不可交换的反例). 设 $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. 验证 $AB \neq BA$, 并直接计算 e^{A+B} 、 $e^A e^B$ 、 $e^B e^A$, 说明三者互不相等.

习题 14.5 (矩阵指数与一阶方程组). 求解下列初值问题的通解 (或满足给定初值的特解):

1. $\mathbf{x}' = \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \mathbf{x}$, $\mathbf{x}(0) = (1, 3)^T$;

2. $\mathbf{x}' = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \mathbf{x}$;

3. $\mathbf{x}' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mathbf{x}$, $\mathbf{x}(0) = (2, 0)^T$;

$$4. \mathbf{x}' = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mathbf{x}.$$

习题 14.6 (3×3 系统). 求解方程组

$$\mathbf{x}' = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \mathbf{x}$$

的通解, 并验证你的答案。

习题 14.7 (高阶标量 ODE). 求解下列微分方程的通解:

$$1. y'' - 5y' + 6y = 0;$$

$$2. y'' + 4y' + 4y = 0, \quad y(0) = 1, \quad y'(0) = 0;$$

$$3. y''' - y = 0;$$

$$4. y^{(4)} + 2y'' + y = 0.$$

习题 14.8 (稳定性判断). 对下列矩阵 A , 判断线性系统 $\mathbf{x}' = A\mathbf{x}$ 的原点是渐近稳定、稳定 (但不渐近稳定) 还是不稳定:

$$1. A = \begin{pmatrix} -1 & 2 \\ 0 & -3 \end{pmatrix};$$

$$2. A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

$$3. A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix};$$

$$4. A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix};$$

$$5. A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

习题 14.9 (非线性系统的线性化). 考虑非线性系统

$$\begin{cases} x' = y, \\ y' = x - x^3. \end{cases}$$

1. 求出所有平衡点。
2. 计算每个平衡点处的 *Jacobian* 矩阵及其特征值。
3. 判断哪些平衡点是双曲的, 并利用 *Hartman-Grobman* 定理确定其局部相图类型 (结点、鞍点、螺旋等)。
4. 对于非双曲的平衡点 (如果有的话), 说明为何 *Hartman-Grobman* 定理不适用。

习题 14.10 (矩阵指数的性质). 设 $A \in M_n(\mathbb{C})$. 证明:

1. 映射 $t \mapsto e^{tA}$ 满足 $e^{(s+t)A} = e^{sA}e^{tA}$ (即它是一个单参数群)。
2. 若 A 是实的斜对称矩阵 ($A^T = -A$), 则 e^{tA} 对所有 t 都是正交矩阵。
3. 若 A 是实的对称矩阵 ($A^T = A$), 则 e^{tA} 对所有 t 都是正定对称矩阵。

习题 14.11. 设

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}.$$

写出 e^{tD} 。

习题 14.12. 设

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

利用 $N^2 = 0$ 计算 e^{tN} 。

习题 14.13. 解微分方程组

$$\frac{d}{dt} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} x(0) \\ y(0) \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

习题 14.14. 设

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

计算 A^2 , 并根据旋转的几何意义猜测 e^{tA} 的形式。

习题 14.15. 若 $A = PDP^{-1}$, 其中 $D = \text{diag}(\lambda_1, \lambda_2)$. 说明为什么

$$e^{tA} = Pe^{tD}P^{-1}.$$

14.6.2 思考题

习题 14.16 (Lotka-Volterra 捕食-被捕食模型). 考虑捕食者-被捕食者的 Lotka-Volterra 方程:

$$\begin{cases} x' = \alpha x - \beta xy, \\ y' = \delta xy - \gamma y, \end{cases}$$

其中 $x(t)$ 为猎物种群数量, $y(t)$ 为捕食者种群数量, $\alpha, \beta, \gamma, \delta > 0$ 为正常数。

1. 求出两个平衡点 $(0, 0)$ 和 $(\gamma/\delta, \alpha/\beta)$ 。
2. 在每个平衡点处计算 *Jacobian* 矩阵和特征值, 判断局部稳定性类型。
3. 对于非双曲的平衡点, 说明为何需要额外分析 (提示: 可以构造守恒量 $H(x, y) = \delta x - \gamma \ln x + \beta y - \alpha \ln y$, 验证 $\frac{d}{dt}H(x(t), y(t)) = 0$)。

习题 14.17 (矩阵指数的基本性质). 对方阵 $A \in M_n(\mathbb{C})$, 定义

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

1. 设

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

计算 $e^{\theta J}$ 。

2. 若

$$J = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$$

且 $AJ = -JA^T$, 判定是否一定有 $e^A J e^{A^T} = J$ 。反之是否成立?

3. 证明 $\det(e^A) = e^{\text{tr}(A)}$ 。
4. 若 A 是实反对称矩阵, 证明 e^A 是正交矩阵。

习题 14.18 (多项式空间上的微分与差分算子). 设 $V = \mathbb{R}_n[x]$ 是所有次数不超过 n 的实系数多项式构成的向量空间。在 V 上定义微分算子

$$(Df)(x) = f'(x)$$

和向后差分算子

$$(\Delta f)(x) = f(x) - f(x-1).$$

证明:

1.

$$I - \Delta = \sum_{k=0}^n \frac{(-D)^k}{k!}.$$

2.

$$f'(x) = \sum_{k=1}^n \frac{1}{k} \Delta^k f(x).$$

3. 是否存在 V 上的可逆 \mathbb{R} -线性变换 P , 使得 $P\Delta P^{-1} = D$?

习题 14.19 (Liouville 公式). 设矩阵值函数 $X(t)$ 满足常微分方程系统

$$X'(t) = A(t)X(t),$$

且在 $t = t_0$ 时的初值为非奇异矩阵 $X(t_0)$, 其中 $A(t)$ 为连续矩阵值函数。证明: 对于任意 t , 有

$$\det X(t) = \det X(t_0) \exp \left(\int_{t_0}^t \operatorname{tr}(A(s)) ds \right).$$

15 挑战选读: 有理标准型

选学背景

有理标准型是在任意域上替代若尔当标准型的分类工具, 需要多项式环、不可约分解、商空间和循环子空间等背景. 它不作为高中友好主线内容, 更适合作为大学代数方向的挑战阅读.

若尔当标准型 (定理13.3) 要求底域为代数闭域, 使得特征多项式可以完全分裂为一次因式的乘积. 当底域 \mathbb{F} 不是代数闭域时 (例如 $\mathbb{F} = \mathbb{R}$ 或 $\mathbb{F} = \mathbb{Q}$), 特征多项式可能含有不可约因式 $p(\lambda)$, 其中 $\deg p \geq 2$, 此时若尔当标准型不再可用. 本节的目标是建立**有理标准型**(rational canonical form), 它对任意域 \mathbb{F} 上的线性变换都成立, 给出了相似类的完全分类.

最简单也最有说服力的例子是平面上的 90° 旋转矩阵

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

它在 \mathbb{R} 上没有特征值, 因而谈不上实数域上的若尔当标准型. 但它的特征多项式和极小多项式都是 $x^2 + 1$, 仍可被有理标准型精确刻画. 这说明有理标准型并不是额外包装, 而是在底域不够大时真正接管分类任务的对象.

从历史上看, Frobenius 将矩阵分类问题推进到了一个不依赖代数闭包的层面, 使不变因子和有理标准型成为更稳健的答案. 从应用角度看, 友阵和伴随矩阵在控制论、状态空间实现以及线性递推数列中都会自然出现, 因而本章也成为前面多项式理论、特征值理论与标准型理论的汇合点.

整体思路和若尔当标准型的推导完全平行, 分为三步:

1. **准素分解**: 广义特征子空间分解 (定理13.1) 的证明仅使用了互素多项式的核分解 (推论7.1), 不需要特征多项式完全分裂. 因此在任意域上, 将 χ_T 按不可约因式分解后, 仍可将 V 分解为若干 T -不变子空间的直和, 每个子空间上 T 的特征多项式是某不可约多项式的幂.
2. **$p(T)$ -拟幂零变换的结构**: 在每个准素分量上, 不可约多项式 $p(\lambda)$ 扮演了若尔当标准型中 $(\lambda - \lambda_0)$ 的角色. 通过分析 $\ker p(T) \subset \ker p(T)^2 \subset \dots$ 的核空间链, 并利用商空间上 $\mathbb{F}[\lambda]/(p(\lambda))$ 的结构, 可以进行类似幂零若尔当标准型的构造.
3. **组合**: 将各准素分量上的标准型组合, 得到有理标准型.

15.1 准素分解

回顾若尔当标准型的推导过程. 第一步是广义特征子空间分解 (定理13.1): 假设 χ_T 在 \mathbb{F} 上完全分裂为 $\chi_T(\lambda) = (\lambda - \lambda_1)^{n_1} \cdots (\lambda - \lambda_s)^{n_s}$, 则

$$V = \ker(T - \lambda_1 I)^{n_1} \oplus \cdots \oplus \ker(T - \lambda_s I)^{n_s}.$$

其证明的关键是: 由 Cayley-Hamilton 定理 (定理8.4) 得 $\chi_T(T) = 0$, 再利用多项式 $(\lambda - \lambda_1)^{n_1}, \dots, (\lambda - \lambda_s)^{n_s}$ 两两互素, 由推论7.1得到核的直和分解. 注意, 这一论证仅依赖于 χ_T 能分解为两两互素的因式之积, 完全不需要这些因式是一次多项式.

现在设 \mathbb{F} 为任意域, $T: V \rightarrow V$ 为 \mathbb{F} -线性变换. 将特征多项式在 $\mathbb{F}[\lambda]$ 中做不可约分解:

$$\chi_T(\lambda) = p_1(\lambda)^{m_1} \cdots p_s(\lambda)^{m_s},$$

其中 $p_1, \dots, p_s \in \mathbb{F}[\lambda]$ 为两两不相伴的首一不可约多项式, $m_1, \dots, m_s \geq 1$ (唯一分解定理7.4). 由于不可约多项式两两不相伴, 有 $\gcd(p_i^{m_i}, p_j^{m_j}) = 1$ (对 $i \neq j$), 即因式 $p_1^{m_1}, \dots, p_s^{m_s}$ 两两互素.

定理 15.1 (准素分解). 设 V 是有限维 \mathbb{F} -线性空间, $T: V \rightarrow V$ 是 \mathbb{F} -线性变换, 特征多项式分解为

$$\chi_T(\lambda) = p_1(\lambda)^{m_1} \cdots p_s(\lambda)^{m_s},$$

其中 p_1, \dots, p_s 为两两不相伴的首一不可约多项式. 定义**准素分量**(primary component):

$$V[p_i] := \ker p_i(T)^{m_i}.$$

则:

1. 每个 $V[p_i]$ 都是 T -不变子空间;
2. $V = V[p_1] \oplus \cdots \oplus V[p_s]$;
3. $T|_{V[p_i]}$ 的特征多项式为 $p_i(\lambda)^{m_i}$, 从而 $\dim V[p_i] = m_i \deg p_i$.

证明. 由 Cayley-Hamilton 定理, $\chi_T(T) = 0$. 因式 $p_1^{m_1}, \dots, p_s^{m_s}$ 两两互素, 反复应用核分解 (推论7.1) 得到 (1) 和 (2): $V = \bigoplus_{i=1}^s V[p_i]$, 且每个 $V[p_i]$ 是 T -不变子空间.

对于 (3), 记 f_i 为 $T_i = T|_{V[p_i]}$ 的特征多项式, 则

$$\chi_T = f_1 \cdots f_s.$$

由于 $p_i(T_i)^{m_i} = 0$, 暂时把底域扩大到代数闭包来看特征值: 若 α 是 T_i 的特征值, 则 $p_i(\alpha)^{m_i} = 0$, 因而 $p_i(\alpha) = 0$. 所以 f_i 的所有根都来自 p_i 的根, 回到 $\mathbb{F}[\lambda]$ 中就说明 f_i 的不可约因子只能是 p_i . 于是可写 $f_i = p_i^{b_i}$, 其中 $b_i \geq 0$. 再比较 $\chi_T = f_1 \cdots f_s = p_1^{m_1} \cdots p_s^{m_s}$ 两边 p_i 的幂次, 由唯一分解定理立即得到 $b_i = m_i$. 因此 $f_i = p_i^{m_i}$, 从而 $\dim V[p_i] = \deg f_i = m_i \deg p_i$. \square

注 15.1. 准素分解是广义特征子空间分解的推广. 当 \mathbb{F} 为代数闭域 (例如 $\mathbb{F} = \mathbb{C}$) 时, 每个不可约多项式都是一次的, 即 $p_i(\lambda) = \lambda - \lambda_i$, 从而 $V[p_i] = \ker(T - \lambda_i I)^{m_i} = V[\lambda_i]$, 定理 15.1 退化为定理 13.1.

例 15.1. 设 $A = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in M_4(\mathbb{R})$, 特征多项式为

$$\chi_A(\lambda) = (\lambda^2 + 1)(\lambda^2 + 4).$$

在 \mathbb{R} 上, $p_1(\lambda) = \lambda^2 + 1$ 和 $p_2(\lambda) = \lambda^2 + 4$ 均不可约, 且互素. 令 T 为 A 对应的线性变换, 则

$$\mathbb{R}^4 = \ker(T^2 + I) \oplus \ker(T^2 + 4I).$$

直接计算可得 $V[p_1] = \text{span}\{e_1, e_2\}$, $V[p_2] = \text{span}\{e_3, e_4\}$.

例 15.2. 设 $\mathbb{F} = \mathbb{Q}$, $T: \mathbb{Q}^6 \rightarrow \mathbb{Q}^6$ 的特征多项式为

$$\chi_T(\lambda) = (\lambda^2 + 1)^2(\lambda - 1)^2.$$

在 \mathbb{Q} 上, $\lambda^2 + 1$ 不可约, $\lambda - 1$ 不可约. 准素分解给出

$$\mathbb{Q}^6 = \ker((T^2 + I)^2) \oplus \ker((T - I)^2).$$

其中 $\dim V[\lambda^2 + 1] = 2 \cdot 2 = 4$, $\dim V[\lambda - 1] = 2 \cdot 1 = 2$.

准素分解将相似问题约化到每个准素分量上. 正如若尔当标准型的情形 (参见定理 13.1 之后的注记), T 和 S 相似当且仅当在适当重排准素分量后, 对应的 $T|_{V[p_i]}$ 和 $S|_{W[p_i]}$ 分别相似. 因此, 下一步我们只需研究特征多项式为不可约多项式之幂 $p(\lambda)^m$ 的情形.

15.2 $p(T)$ -拟幂零变换的结构

现在我们假设 V 上的线性变换 T 满足特征多项式为 $\chi_T(\lambda) = p(\lambda)^m$, 其中 $p(\lambda) \in \mathbb{F}[\lambda]$ 是首一不可约多项式, 且 $d = \deg p \geq 1$. 此时 $\dim V = md$. 我们的目标是找到 V 的直和分解以及相应的一组基, 使得 T 在这组基下的矩阵具有最简分块形式, 且每个分块是某个 $p(\lambda)^k$ 的友阵.

这完全平行于幂零变换 (即 $p(\lambda) = \lambda$) 的若尔当标准型的推导. 令极小多项式为 $p(\lambda)^\ell$ ($1 \leq \ell \leq m$), 并记 $P = p(T)$. 由于 $P^\ell = 0$ 而 $P^{\ell-1} \neq 0$, 可以将 T 视作一种广义的幂零变换, 称作 $p(T)$ -拟幂零变换.

像引理 13.1 那样, 我们考虑下列从大到小的核子空间链:

$$V_0 = \ker P^\ell = V, V_1 = \ker P^{\ell-1}, \dots, V_i = \ker P^{\ell-i}, \dots, V_\ell = \ker P^0 = \{0\}.$$

在这个递减链中, 商空间 V_i/V_{i+1} 具有比原来更丰富的代数结构. 注意到 T 与 $P = p(T)$ 可交换, 这意味着每个 $\ker P^j$ 都是 T -不变子空间. 在商空间 V_i/V_{i+1} 上, $P = p(T)$ 的作用为零 (因为 $P(\ker P^{\ell-i}) \subset \ker P^{\ell-i-1}$).

考虑多项式环 $\mathbb{F}[\lambda]$, 映射 $f(\lambda) \mapsto f(T)$ 给出了多项式在 V_i/V_{i+1} 上的作用. 由于 $p(\lambda)$ 的作用为零, 这个作用只依赖于 $f(\lambda)$ 模 $p(\lambda)$ 的余式. 因为 $p(\lambda)$ 不可约, $K := \mathbb{F}[\lambda]/(p(\lambda))$ 是一个域 (它是 \mathbb{F} 的 d 次扩域; 关于这一构造的详细讨论, 参见注记6.7). 由此, 每一个商空间 V_i/V_{i+1} 都可以看作是域 K 上的线性空间, 从而它作为 \mathbb{F} -向量空间的维数必定是 d 的倍数.

此外, 变换 P 诱导了映射 $\tilde{P}: V_i/V_{i+1} \rightarrow V_{i+1}/V_{i+2}$, 定义为 $\tilde{P}(\bar{v}) = \overline{Pv}$. 与引理13.1的(4)完全同样地可以验证, \tilde{P} 是单射. 由于 P 与 T 交换, \tilde{P} 不改变多项式的作用, 因而 \tilde{P} 是 K -线性的.

这允许我们完全照搬关于幂零变换的 Young 图构造 (参见 §13.2), 只需要将所有的基底选取从域 \mathbb{F} 替换为域 K . 直觉上, 将 P 视为“ K -线性空间上的幂零变换”, 对其实施幂零标准型的构造, 就能获得若干条 P -链. 每一条 P -链上的一个 K -基向量, 通过 T 的作用展开为 d 个 \mathbb{F} -基向量. 这样, P 的幂零分解所生成的全部 \mathbb{F} -向量将构成 V 的一组 \mathbb{F} -基, 从而给出所需的直和分解.

定理 15.2 (不可约多项式次幂的标准型). 设 V 是维数为 md 的 \mathbb{F} -线性空间, $T: V \rightarrow V$ 的特征多项式为 $p(\lambda)^m$, 其中 $p(\lambda) \in \mathbb{F}[\lambda]$ 为首一不可约多项式, 且 $\deg p = d$. 则存在 V 的直和分解

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_s,$$

其中每个 W_i 是 T -循环子空间. 特别地, 存在 $u_i \in W_i$ 使得 $W_i = \text{span}\{u_i, Tu_i, \dots, T^{k_i d-1}u_i\}$. 在这个基下, 各个 $T|_{W_i}$ 的矩阵为友阵 $C(p^{k_i})$, 且正整数序列满足 $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$, 以及 $\sum_{i=1}^s k_i = m$. 两个具有相同特征多项式 $p(\lambda)^m$ 的线性变换相似, 当且仅当它们的块尺寸序列 (k_1, \dots, k_s) 相同.

证明. 存在性. 令 $P = p(T)$, 设 T 的极小多项式为 $p(\lambda)^\ell$ ($1 \leq \ell \leq m$). 则 $P^\ell = 0$ 且 $P^{\ell-1} \neq 0$. 考虑核空间的递减链

$$V = \ker P^\ell \supset \ker P^{\ell-1} \supset \cdots \supset \ker P^0 = \{0\}.$$

记 $V_i = \ker P^{\ell-i}$, 则 $V_0 = V$, $V_\ell = \{0\}$. 如前所述, P 诱导 K -线性单射 $\tilde{P}: V_i/V_{i+1} \hookrightarrow V_{i+1}/V_{i+2}$, 且每个 V_i/V_{i+1} 是域 K 上的线性空间.

我们首先说明 K -基与 \mathbb{F} -基的对应关系. 取 V_i/V_{i+1} 的一组 K -基 $\bar{w}_1, \dots, \bar{w}_r$, 记 \bar{T} 为 T 在商空间 V_i/V_{i+1} 上诱导的算子. 由于 $K = \mathbb{F}[\lambda]/(p(\lambda))$ 作为 \mathbb{F} -线性空间的一组基为 $\{1, \bar{\lambda}, \dots, \bar{\lambda}^{d-1}\}$, 而 $\bar{\lambda}$ 的乘法作用正对应 \bar{T} , 所以

$$\bar{w}_1, \bar{T}\bar{w}_1, \dots, \bar{T}^{d-1}\bar{w}_1, \dots, \bar{w}_r, \bar{T}\bar{w}_r, \dots, \bar{T}^{d-1}\bar{w}_r$$

构成 V_i/V_{i+1} 的一组 \mathbb{F} -基. 特别地, $\dim_{\mathbb{F}}(V_i/V_{i+1}) = d \cdot \dim_K(V_i/V_{i+1})$.

现在, 由于 P 是 V 上的幂零变换 ($P^\ell = 0$), 而每个 V_i/V_{i+1} 都是 K -线性空间, 且 \tilde{P} 是 K -线性单射, 引理13.1的全部结论在各个商空间上可以按 K -线性版本使用. 需要注意的是, 整个 V 本身仍只是 \mathbb{F} -线性空间; 因而从商空间选出 K -线性无关向量后, 回到 V 时要先按上段方法展开成 \mathbb{F} -向量, 再利用引理13.1(5) 得到 \mathbb{F} -线性无关性.

于是, 我们可以在 K -线性空间的框架下, 完全照搬 §13.2中幂零变换若尔当标准型的 Young 图构造:

1. 取 V_0/V_1 的一组 K -基 $\overline{u}_1, \dots, \overline{u}_{s_0}$, 其原像 u_j 生成长度为 ℓ 的 P -链;
2. 在 V_1/V_2 中将 $\tilde{P}(\overline{u}_1), \dots, \tilde{P}(\overline{u}_{s_0})$ 扩充为 K -基, 新增向量生成长度为 $\ell - 1$ 的 P -链;
3. 以此类推, 直至所有 V_i/V_{i+1} 的 K -基选取完毕.

这一构造产生了若干条 P -链. 设一条 P -链的长度为 k , 起始向量为 u , 则 P -链上的向量为

$$u, Pu, P^2u, \dots, P^{k-1}u.$$

关键一步是将取法中的在 V_i/V_{i+1} 中的 K -线性无关性转化为 \mathbb{F} -线性无关性. 将每条 P -链上的每个向量 $P^j u$ 展开为 d 个 \mathbb{F} -向量: $P^j u, TP^j u, \dots, T^{d-1}P^j u$. 这样, 一条长度为 k 的 P -链生成如下 kd 个 \mathbb{F} -向量:

$$\begin{array}{cccc} u, & Tu, & \dots, & T^{d-1}u, \\ Pu, & TPu, & \dots, & T^{d-1}Pu, \\ \vdots & \vdots & \ddots & \vdots \\ P^{k-1}u, & TP^{k-1}u, & \dots, & T^{d-1}P^{k-1}u. \end{array}$$

由上面的 K -基与 \mathbb{F} -基的对应关系, 这些向量在各商空间 V_i/V_{i+1} 中恰好给出 P -链中 K -基向量展开而成的 \mathbb{F} -基向量. 因此, 将所有 P -链展开后得到的全部 \mathbb{F} -向量, 恰好满足引理13.1(5) 的条件 (在 \mathbb{F} 上): 它们在每一层 V_i/V_{i+1} 中分别 \mathbb{F} -线性无关, 从而在 V 中 \mathbb{F} -线性无关. 合计共有 $md = \dim V$ 个, 因此构成 V 的一组 \mathbb{F} -基.

最后, 我们证明每条 P -链生成的 \mathbb{F} -子空间就是相应的 T -循环子空间. 由于 $P = p(T)$ 是 T 的 d 次首一多项式, 上述 kd 个 \mathbb{F} -向量 $\{T^a P^b u : 0 \leq a \leq d-1, 0 \leq b \leq k-1\}$ 中每个元素 $T^a P^b u = T^a p(T)^b u$ 都是 T 在 u 上的多项式作用, 即属于 T -循环子空间 $\text{span}_{\mathbb{F}}\{u, Tu, \dots, T^{kd-1}u\}$. 反之, 由 $P = p(T) = T^d + (\text{低次项})$, 通过对 $T^d u = Pu - (\text{低次项})$ 的递推, 可以将 $T^n u$ ($n \geq d$) 表示为 $\{T^a P^b u\}$ 的 \mathbb{F} -线性组合. 因此

$$W := \text{span}_{\mathbb{F}}\{u, Tu, \dots, T^{kd-1}u\} = \text{span}_{\mathbb{F}}\{T^a P^b u : 0 \leq a \leq d-1, 0 \leq b \leq k-1\},$$

且 $\dim W = kd$. 由 $p(T)^k u = P^k u = 0$ 且 $P^{k-1}u \neq 0$, $T|_W$ 的极小多项式为 $p(\lambda)^k$, 而 $\dim W = kd = \deg p^k$ 等于特征多项式的次数, 故极小多项式等于特征多项式. 由定理8.6, $T|_W$ 在循环基 $(u, Tu, \dots, T^{kd-1}u)$ 下的矩阵为友阵 $C(p^k)$.

将所有 P -链生成的 T -循环子空间合并, 由上面的 \mathbb{F} -线性无关性知它们的和是直和, 且合计维数为 $\sum k_i d = md = \dim V$. 因此 $V = W_1 \oplus \cdots \oplus W_s$, 其中 $k_1 \geq \cdots \geq k_s \geq 1$, $\sum k_i = m$.

唯一性. 块尺寸序列 (k_1, \dots, k_s) 由如下相似不变量唯一决定: 对每个 $j \geq 1$, 核维数 $\dim \ker p(T)^j$ 不依赖于基的选取. 而

$$\dim \ker p(T)^j = d \sum_{i=1}^s \min(j, k_i) = d \sum_{k_i \leq j} k_i + jd \cdot \#\{i : k_i > j\}$$

的差分 $\dim \ker p(T)^j - \dim \ker p(T)^{j-1} = d \cdot \#\{i : k_i \geq j\}$ 恰好给出序列 (k_1, \dots, k_s) 的共轭分拆 (类比幂零情形 Young 图的列长度), 从而唯一确定 (k_1, \dots, k_s) . \square

定义 15.1 (初等因子). 在定理 15.2 的记号下, 集合 $\{p(\lambda)^{k_1}, \dots, p(\lambda)^{k_s}\}$ (计入重复) 称为该准素分量的**初等因子** (*elementary divisors*).

15.3 有理标准型定理

现在我们将前两步的结果合并, 得到一般域上线性变换的完全分类及其有理标准型.

定理 15.3 (有理标准型定理——初等因子形式). 设 V 是有限维 \mathbb{F} -线性空间, $T: V \rightarrow V$ 是线性变换. 设 T 的特征多项式在 $\mathbb{F}[\lambda]$ 中具有不可约分解:

$$\chi_T(\lambda) = p_1(\lambda)^{m_1} \cdots p_s(\lambda)^{m_s}.$$

则存在 V 的一组基, 使得 T 在这一基下的矩阵呈分块对角形:

$$[T]_B = \text{diag}\{C(p_1^{k_{1,1}}), \dots, C(p_1^{k_{1,r_1}}), \dots, C(p_s^{k_{s,1}}), \dots, C(p_s^{k_{s,r_s}})\},$$

其中对每个 $i = 1, \dots, s$, 整数序列满足 $k_{i,1} \geq k_{i,2} \geq \cdots \geq k_{i,r_i} \geq 1$ 且 $\sum_{j=1}^{r_i} k_{i,j} = m_i$.

上式中的每一个对角块都是某个多项式 $p_i(\lambda)^k$ 的友阵. 集合

$$\mathcal{E}(T) = \{p_i(\lambda)^{k_{i,j}} \mid 1 \leq i \leq s, 1 \leq j \leq r_i\}$$

称为 T 的**初等因子** (*elementary divisors*) 集合.

对于给定域 \mathbb{F} 上的两个方阵 $A, B \in M_n(\mathbb{F})$, 它们相似当且仅当它们具有完全相同的初等因子集合. 因此, 上述不计块顺序的分块对角矩阵被称为 A 的**第一有理标准型**(初等因子形式). 它是由 A 的相似类唯一确定的.

证明. 根据定理 15.1 (准素分解), 空间 V 分解为各不可约多项式的准素分量 $V[p_i] = \ker p_i(T)^{m_i}$ 的直和. 在每个准素分量 $V[p_i]$ 上, 限制变换 $T_i = T|_{V[p_i]}$ 的特征多项式为 $p_i(\lambda)^{m_i}$.

根据定理 15.2, 在每个 $V[p_i]$ 内, 存在循环子空间的直和分解, 使得表示矩阵为友阵的直和: $\text{diag}\{C(p_i^{k_{i,1}}), \dots, C(p_i^{k_{i,r_i}})\}$. 将这 s 个分量上的基合并, 即得到整个空间上满足定理要求的分块形式.

关于唯一性: 对每个 i , 准素分量 $V[p_i]$ 上的初等因子由定理15.2的唯一性保证, 而准素分量本身由 χ_T 的不可约分解唯一确定. 因此, 初等因子集合 $\mathcal{E}(T)$ 是 T 的相似不变量. 反之, 若两个变换具有相同的初等因子集合, 则它们在相同基下的矩阵都等于同一分块对角矩阵, 故相似. \square

注 15.2 (不变因子). 除了以上基于底域多项式不可约分解而产生的第一有理标准型 (初等因子形式), 还有另外一种不依赖不可约分解的方式刻画的有理标准型. 关键事实是: 当两个首一多项式 $f(\lambda), g(\lambda)$ 互素时, 分块对角矩阵 $\text{diag}\{C(f), C(g)\}$ 相似于友阵 $C(fg)$. 这是因为 $\text{diag}\{C(f), C(g)\}$ 的极小多项式为 $\text{lcm}(f, g) = fg$ (由互素性), 同时特征多项式也为 fg , 故由定理8.6得到结论.

利用这一“合并”事实, 我们可以对定理15.3中的初等因子重新打包组合. 对于每个不同下标 p_i , 将其所对应的次幂最高的一项拿出来, 把所有这 s 项乘在一起得到 $f_1(\lambda) = \prod_{i=1}^s p_i^{k_{i,1}}$. 因为它们底数两两互素, 它们组成的友阵块直和整体相似于一块大的友阵 $C(f_1)$. (注意到这里 f_1 恰巧就是 T 的极小多项式 $m_T(\lambda)$). 接下来, 我们在剩下未被选取的初等因子中再挑每个质因子次高的幂乘起来得到 $f_2(\lambda)$, 以此类推. 如果某个质因子没有剩余了, 那它在后面多项式中的幂次就视作 0. 这样操作完后, 我们就得到了一个满足整除关系的多项式序列:

$$f_r(\lambda) \mid \cdots \mid f_2(\lambda) \mid f_1(\lambda),$$

以及相对应的另一种直和分解形式:

$$[T]_{B'} = \text{diag}\{C(f_r), \dots, C(f_2), C(f_1)\}.$$

多项式序列 f_r, \dots, f_1 完全决定了 T 的相似类, 它们被称为 T 的**不变因子** (*invariant factors*), 而这种具有整除关系友阵按块构成的矩阵被称为定理的**第二有理标准型** (或不变因子形式有理标准型). 需要注意的是, 不变因子是相对于当前底域 \mathbb{F} 而言的: 若把底域扩大, 原本不可约的多项式可能继续分解, 相应的标准型描述也会随之细化.

15.4 与若尔当标准型的统一

至此, 我们看到有理标准型在任意域上的推广具有完美的普适性. 如果我们再回归到若尔当标准型要求的前提——代数闭域 (例如 \mathbb{C})——上, 所有的不可约多项式只能是一次多项式 $p_i(\lambda) = \lambda - \lambda_i$. 此时:

1. 准素分解 $V[p_i] = \ker(T - \lambda_i I)^{m_i}$ 会自然退化回第一步的广义特征子空间分解 (参见定理13.1).
2. 对于一次多项式 $\lambda - \lambda_i$ 的次幂 $(\lambda - \lambda_i)^k$, 这种结构对应的初等因子就是 $(\lambda - \lambda_i)^k$. 在该子空间内, 有理标准型给出的是其对应的友阵 $C((\lambda - \lambda_i)^k)$, 而若尔当标准型给出的是 k 阶若尔当块 $J_k(\lambda_i)$.

3. 这二者其实是同一现象在不同视角下的不同表达基。代数特征上, 两者的特征多项式和极小多项式均为 $(\lambda - \lambda_i)^k$, 因此 $C((\lambda - \lambda_i)^k)$ 与 $J_k(\lambda_i)$ 是精确相似的 (可用定理 8.6 证明)。

若尔当块的矩阵形式具有对角占优和移位结构, 在解析研究 (如常微分方程的矩阵指数) 中非常直观; 而有理标准型不要求出多项式的根, 仅需不可约分解, 所依赖的全部运算都在 \mathbb{F} 上完成. 因此有理标准型在符号计算和控制论等需要在特定域上精确工作的场景中具有重要应用.

15.5 计算示例

在通过具体计算寻找有理标准型时, 计算每一个准素分量的核空间链或者推导 K -代数链理论上虽然具有确切的构造性, 但在人工手算上有时显得过于繁复。我们在这里提供两个例子, 直接利用特征多项式、极小多项式以及几何重数 (核的维数) 等信息, 逆向确立初等因子和不变因子。

例 15.3 (实数域上的不可约二次因子). 在 \mathbb{R} 上, 多项式

$$p(\lambda) = \lambda^2 + 1$$

不可约. 它的友阵为

$$C(p) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

这正是逆时针旋转 90° 的矩阵. 它在 \mathbb{R} 上没有特征值, 但仍满足 $p(C(p)) = C(p)^2 + I = 0$. 因而在实数域上, 这个 2×2 块就是一对共轭复特征值 $\pm i$ 的实形式.

再看 $p(\lambda)^2 = (\lambda^2 + 1)^2 = \lambda^4 + 2\lambda^2 + 1$. 其友阵为

$$C(p^2) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

由友阵性质,

$$\chi_{C(p^2)}(\lambda) = m_{C(p^2)}(\lambda) = (\lambda^2 + 1)^2,$$

所以它在 \mathbb{R} 上的第一有理标准型就是一个 4×4 块 $C(p^2)$.

与之对比, 分块对角矩阵

$$D = \text{diag}\{C(p), C(p)\}$$

也有特征多项式 $(\lambda^2 + 1)^2$, 但它已经满足 $p(D) = 0$, 因而

$$m_D(\lambda) = \lambda^2 + 1.$$

因此 D 的第一有理标准型是两个 2×2 块 $C(p) \oplus C(p)$, 而不是一个 4×4 块. 这个例子说明: 在实数域上, 不可约二次因子的“幂次”扮演着复数域上若尔当块大小的角色.

例 15.4. 设在 \mathbb{Q} 上的一个线性变换在某个基下的矩阵为

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & -2 \end{pmatrix}.$$

我们计算其在 \mathbb{Q} 上的有理标准型. 注意到 A 的次对角线全为 1, 最后一列为 $(-1, -2, -2, -2)^T$, 这正是友阵 (定义 8.15) 的形式, 即 $A = C(\chi_A)$. 尽管如此, 我们仍然完整展示计算过程.

(1) 特征多项式与不可约分解: 计算得 $\chi_A(\lambda) = \lambda^4 + 2\lambda^3 + 2\lambda^2 + 2\lambda + 1$. 对其在 \mathbb{Q} 上进行不可约分解: 由于 $\chi_A(-1) = 0$, 显然有因式 $\lambda + 1$. 做多项式长除法得到

$$\chi_A(\lambda) = (\lambda + 1)(\lambda^3 + \lambda^2 + \lambda + 1) = (\lambda + 1)^2(\lambda^2 + 1).$$

其在 \mathbb{Q} 上的首一不可约因子是 $p_1(\lambda) = \lambda + 1$ 和 $p_2(\lambda) = \lambda^2 + 1$, 对应的准素分量维数分别为 2 和 2.

(2) 确定初等因子类型: 对于 $p_2(\lambda) = \lambda^2 + 1$, 因为其代数重数为 1, 该分量的初等因子只能是 $p_2(\lambda)$ 本身 (对应一个 2 阶友阵).

对于 $p_1(\lambda) = \lambda + 1$, 其代数重数是 2, 所以对应的初等因子分配要么是 $\{(\lambda + 1)^2\}$, 要么是 $\{\lambda + 1, \lambda + 1\}$. 我们可以通过计算矩阵在 $\lambda = -1$ 处的降秩来判断. 考察 $A + I$:

$$A + I = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 1 & 1 & 0 & -2 \\ 0 & 1 & 1 & -2 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

容易验证其前三列线性无关, 即 $\text{rank}(A + I) = 3$, 从而 $\dim \ker(A + I) = 4 - 3 = 1$. 这说明关于因式 $\lambda + 1$ 的初等因子只有一个, 只能是 $(\lambda + 1)^2 = \lambda^2 + 2\lambda + 1$. 因此 A 的全体初等因子集合为 $\{\lambda^2 + 2\lambda + 1, \lambda^2 + 1\}$.

(3) 组合成第一有理标准型 (初等因子形式): 根据初等因子直接写出各自的友阵

$$C(\lambda^2 + 2\lambda + 1) = \begin{pmatrix} 0 & -1 \\ 1 & -2 \end{pmatrix}, \quad C(\lambda^2 + 1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

从而 A 的第一有理标准型为分块对角矩阵:

$$\text{diag} \{C(\lambda^2 + 2\lambda + 1), C(\lambda^2 + 1)\} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

(4) **不变因子形式 (第二有理标准型)**: 按照注记 15.2 提取最大次幂以组装不变因子: 由于两个初等底数 $p_1(\lambda)$ 与 $p_2(\lambda)$ 互素, 且各自只有一个初等因子, 我们直接将它们相乘打包在一起, 得到唯一的不变因子:

$$f_1(\lambda) = (\lambda^2 + 2\lambda + 1)(\lambda^2 + 1) = \chi_A(\lambda).$$

所以它的第二有理标准型就是一个完整的 4×4 友阵 $C(\chi_A)$, 计算写出即为矩阵 A 本身! 这刚好与前文关于循环矩阵的直观相吻合。

例 15.5. 设 $B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in M_4(\mathbb{R})$. 我们求 B 在 \mathbb{R} 上的有理标准型。

(1) **特征多项式与不可约分解**: 由于 B 已经是分块对角阵, 可直接写出 $\chi_B(\lambda) = (\lambda - 2)^2(\lambda^2 + 1)$. 在 \mathbb{R} 上, 首一不可约因式为 $p_1(\lambda) = \lambda - 2$ 和 $p_2(\lambda) = \lambda^2 + 1$, 代数重数分别为 $m_1 = 2$ 和 $m_2 = 1$.

(2) **确定初等因子**: 对于 $p_2(\lambda) = \lambda^2 + 1$, $m_2 = 1$, 对应的初等因子只能是 $\lambda^2 + 1$. 对于 $p_1(\lambda) = \lambda - 2$, $m_1 = 2$, 其初等因子可能是 $\{(\lambda - 2)^2\}$ 或 $\{\lambda - 2, \lambda - 2\}$. 我们计算考察特征子空间 $\ker(B - 2I)$ 的维数 (即几何重数):

$$B - 2I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & -1 \\ 0 & 0 & 1 & -2 \end{pmatrix}.$$

显然其非零行仅贡献秩 2, 即 $\text{rank}(B - 2I) = 2$, 故 $\dim \ker(B - 2I) = 4 - 2 = 2$. 几何重数为 2 说明存在 2 块关于 $(\lambda - 2)$ 的首一初等因子. 因此初等因子分配必定是 $\{\lambda - 2, \lambda - 2\}$. 综合起来, B 的初等因子集合为 $\mathcal{E}(B) = \{\lambda - 2, \lambda - 2, \lambda^2 + 1\}$.

(3) **第一有理标准型 (初等因子形式)**: 写出各初等因子对应的友阵: $C(\lambda - 2) = (2)$, $C(\lambda^2 + 1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. 于是 B 的第一有理标准型为:

$$\text{diag} \left\{ 2, 2, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

在这个例子里, 矩阵 B 恰好本身就是第一有理标准型。

(4) **不变因子与第二有理标准型**: 我们通过重新打包初等因子来求不变因子序列. 首先, 在所有不同的不可约底数中分别取出出现过的**最高次幂**, 乘在一起作为第一个最大的不

变因子 $f_1(\lambda)$ 。目前 p_1 的初等因子里最高次幂是 $(\lambda - 2)^1$, p_2 是 $(\lambda^2 + 1)^1$ 。因此:

$$f_1(\lambda) = (\lambda - 2)(\lambda^2 + 1) = \lambda^3 - 2\lambda^2 + \lambda - 2.$$

然后, 对剩余的初等因子重复此操作以构造 $f_2(\lambda)$: p_2 已无剩余 (视作 1), p_1 还剩余一项 $\lambda - 2$ 。将其乘起来得到:

$$f_2(\lambda) = \lambda - 2.$$

易见 $f_2 \mid f_1$ 且 $f_1 f_2 = \chi_B$ 。所以该矩阵的不变因子序列为 $f_2(\lambda), f_1(\lambda)$ 。

据此, 将这两个不变因子转化为相应的友阵 $C(f_2) = (2)$ 以及 $C(f_1) = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$

(由友阵定义 8.15, $f_1 = \lambda^3 - 2\lambda^2 + \lambda - 2$ 的系数给出最后一列 $(-a_0, -a_1, -a_2)^T = (2, -1, 2)^T$), 组合即可得到第二有理标准型 (不变因子形式):

$$\text{diag}\{C(f_2), C(f_1)\} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

15.6 习题

15.6.1 练习题

习题 15.1 (准素分解的直接应用). 设 T 是 \mathbb{Q} 上线性空间 V 上的线性变换, 且

$$\chi_T(\lambda) = (\lambda^2 + 1)^2(\lambda - 3).$$

写出准素分解给出的直和分解, 并求各个准素分量的维数.

习题 15.2 (实平面旋转的有理标准型). 设

$$R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \in M_2(\mathbb{R}),$$

其中 $\theta \not\equiv 0, \pi \pmod{2\pi}$. 求 R_θ 在 \mathbb{R} 上的特征多项式、极小多项式和有理标准型. 并说明为什么它在 \mathbb{R} 上没有若尔当标准型意义下的实特征值分解.

习题 15.3 (四阶矩阵的初等因子). 设 $A \in M_4(\mathbb{Q})$ 的特征多项式为

$$\chi_A(\lambda) = (\lambda^2 + 1)^2.$$

列出 A 可能的初等因子集合. 对每一种可能, 写出对应的第一有理标准型.

习题 15.4 (不变因子). 设某线性变换的初等因子为

$$(\lambda - 1)^3, (\lambda - 1), \lambda^2 + 1, (\lambda^2 + 1)^2.$$

求它的不变因子序列, 并写出第二有理标准型的分块形式.

习题 15.5. 在有理数域 \mathbb{Q} 上, 判断多项式 $x^2 - 2$ 是否能分解成一次因式的乘积. 再说明它在实数域 \mathbb{R} 上的情况.

习题 15.6. 写出多项式

$$p(x) = x^2 + 1$$

的伴随矩阵, 并计算它的特征多项式.

习题 15.7. 设

$$C = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

计算 C^2 , 并找出一个二次多项式 $p(x)$ 使 $p(C) = 0$.

习题 15.8. 说明为什么矩阵

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

在实数域上没有实特征值, 但仍然可以通过多项式 $x^2 + 1$ 来描述其行为.

习题 15.9. 设 T 是一个线性变换, 且满足 $T^2 = 0$, 但 $T \neq 0$. 给出一个 2×2 矩阵例子, 并说明它与幂零块的关系.

15.6.2 思考题

习题 15.10 (中心化子与循环矩阵). 设 $A \in M_n(F)$ 的极小多项式等于特征多项式. 证明所有与 A 交换的矩阵都可以写成 A 的多项式, 即

$$\{X \in M_n(F) \mid XA = AX\} = F[A].$$

习题 15.11 (有理数域上六阶线性变换的中心化子). 设 V 为有理数域 \mathbb{Q} 上的 6 维线性空间, $T: V \rightarrow V$ 为一个 6 阶线性变换, 即 $T^6 = I$, 且对任意 $0 < k < 6$ 均有 $T^k \neq I$. 记

$$C(T) = \{S \in \text{End}_{\mathbb{Q}}(V) \mid ST = TS\}.$$

请问 $C(T)$ 的可能维数有哪些? 请证明结论, 并写出当 $C(T)$ 维数取得最大值和最小值时, T 的特征多项式分别是什么样子的.

习题 15.12 (中心化子代数). 设 V 是 n 维复向量空间, $T: V \rightarrow V$ 是线性变换. 定义

$$C(T) = \{S \in \text{End}(V) \mid ST = TS\}.$$

1. 若 T 的极小多项式等于特征多项式, 证明

$$C(T) = \{p(T) \mid p \in \mathbb{C}[x]\},$$

并推出 $\dim C(T) = n$ 。

2. 若 $T = \text{diag}(\lambda_1 I_{n_1}, \dots, \lambda_k I_{n_k})$ 且 λ_i 两两不同, 证明

$$C(T) \cong M_{n_1}(\mathbb{C}) \oplus \dots \oplus M_{n_k}(\mathbb{C}),$$

并求维数。

3. 证明对一般的 T , $\dim C(T) \geq n$, 并讨论等号条件。

习题 15.13 (两个若尔当块的中心化子维数). 设整数 $m, n \geq 2$, a, b 是实数。设

$$A = \begin{pmatrix} J & 0 \\ 0 & K \end{pmatrix},$$

其中 J 是 m 阶若尔当型下三角块, K 是 n 阶若尔当型下三角块:

$$J = \begin{pmatrix} a & 0 & \cdots & 0 \\ 1 & a & \ddots & \vdots \\ 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & a \end{pmatrix}, \quad K = \begin{pmatrix} b & 0 & \cdots & 0 \\ 1 & b & \ddots & \vdots \\ 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & b \end{pmatrix}.$$

求线性空间

$$\{X \in M_{m+n}(\mathbb{R}) \mid AX = XA\}$$

的维数。

习题 15.14 (五阶线性变换的有理标准型). 设 n 为正整数, 使得存在 $A \in M_n(\mathbb{Q})$, 满足

$$A^5 = I_n, \quad A - I_n \text{ 非退化.}$$

1. 求 A 在 \mathbb{Q} 上的极小多项式。

2. 求 n 的所有可能值, 并证明。

习题 15.15 (有限域上的矩阵方程与相似类计数). 设 q 为素数幂, $A \in M_{m \times n}(\mathbb{F}_q)$ 为秩为 r 的矩阵。

1. 证明方程 $A\mathbf{x} = \mathbf{b}$ 在 \mathbb{F}_q^n 中的解的个数为

$$\#\{\mathbf{x} \in \mathbb{F}_q^n \mid A\mathbf{x} = \mathbf{b}\} = \begin{cases} q^{n-r}, & \mathbf{b} \in \text{Im } A, \\ 0, & \mathbf{b} \notin \text{Im } A. \end{cases}$$

2. 通过对所有 $\mathbf{b} \in \mathbb{F}_q^m$ 求和, 证明

$$\sum_{\mathbf{b} \in \mathbb{F}_q^m} \#\{\mathbf{x} \in \mathbb{F}_q^n \mid A\mathbf{x} = \mathbf{b}\}^2 = q^{2n-r}.$$

3. 设 $A \in M_{m \times n}(\mathbb{F}_q)$, $B \in M_{m \times \ell}(\mathbb{F}_q)$. 计算

$$N(A, B) = \#\{X \in M_{n \times \ell}(\mathbb{F}_q) \mid AX = B\},$$

并证明 $N(A, B) \neq 0$ 当且仅当 $\text{rank}(A) = \text{rank}(A \mid B)$; 此时 $N(A, B) = q^{(n-r)\ell}$.

4. 设 $A, B \in M_n(\mathbb{F}_q)$, 定义

$$S(A, B) = \#\{P \in \text{GL}_n(\mathbb{F}_q) \mid PAP^{-1} = B\}.$$

证明: 若 A 与 B 不相似, 则 $S(A, B) = 0$; 若 A 与 B 相似, 则

$$S(A, B) = \#C(A),$$

其中 $C(A) = \{P \in \text{GL}_n(\mathbb{F}_q) \mid PA = AP\}$ 是 A 在 $\text{GL}_n(\mathbb{F}_q)$ 中的中心化子。

5. 利用轨道-稳定子公式说明 A 的相似类大小为 $\#\text{GL}_n(\mathbb{F}_q)/\#C(A)$, 并证明

$$\sum_{\text{相似类}[A]} \frac{\#\text{GL}_n(\mathbb{F}_q)}{\#C(A)} = q^{n^2}.$$

对 $n = 2$ 的情形, 列举 $M_2(\mathbb{F}_2)$ 的所有相似类, 并验证该公式。

索引

- K -线性, K -linear, 375
 \mathbb{R} -线性空间, \mathbb{R} -vector space, 79
 $p(T)$ -拟幂零变换, $p(T)$ -quasinilpotent transformation, 372, 374
 q -二项式系数, q -binomial coefficient, 36
 q -整数, q -integer, 35
 q -阶乘, q -factorial, 36
- Beltrami, Eugenio, 270
- Cauchy-Binet 公式, 149
Cauchy-Schwarz 不等式, 240, 254
Cayley-Hamilton 定理, 200
- Eckart, Carl, 270
Eckart-Young 定理, 282
- Frobenius 内积, Frobenius inner product, 222
- Gauss, Carl Friedrich, 289
Golub, Gene, 270
Google 矩阵, Google matrix, 197
- Hilbert, David, 270
Hilbert 矩阵, Hilbert matrix, 235
Hotelling, Harold, 288
- Jacobian 矩阵, Jacobian matrix, 364
Jordan, Camille, 270
- Kahan, William, 270
KV 缓存, KV cache, 322
- Laplace 公式, 147
Legendre, Adrien-Marie, 289
logits 矩阵, logits matrix, 314
Lorentz 型, Lorentz form, 222
- Lyapunov 函数法, Lyapunov function method, 364
Lyapunov 稳定, Lyapunov stability, 360
- Markov 链, 196
- Nyquist 稳定性判据, 361
- one-hot 表示, one-hot representation, 303
- Pearson, Karl, 288
Piazzzi, Giuseppe, 289
- QR 分解, 244
- Routh-Hurwitz 判据, 361
rowsoftmax, 307
- Sarrus 法则, 138
Schmidt, Erhard, 270
softmax, 306
Sylvester, James Joseph, 270
Sylvester 惯性定理, 227
- teleportation, 198
token, 302
top- k 采样, top-k sampling, 321
top- p 采样, top-p sampling, 321
- Vandermonde 行列式, 144
- Young, Gale, 270
- 三角不等式, triangle inequality, 240
上三角阵, upper triangular matrix, 65
下三角阵, lower triangular matrix, 66
不动点, fixed point, 359
不变因子, invariant factors, 378
不变子空间, invariant subspace, 191

不可约多项式, irreducible polynomial, 182
 不相容的, inconsistent, 30
 不稳定, instability, 360
 不稳定极点, unstable pole, 361
 不稳定结点, unstable node, 362
 不稳定退化结点, unstable degenerate node, 363
 严格上三角阵, strictly upper triangular matrix, 66
 严格下三角阵, strictly lower triangular matrix, 66
 中心, center, 362
 中心流形理论, center manifold theory, 364
 主元, pivot, 24
 主元, principal unknowns, 28
 主成分, principal component, 286
 主成分分析, principal component analysis, 284
 二次型, quadratic form, 223
 二次曲线, conic, 258
 二次曲面, quadric, 259
 互素, coprime, 181
 交, intersection, 98
 交叉熵损失, cross-entropy loss, 316
 交错多重线性函数, alternating multilinear function, 134
 代数余子式, cofactor, 142
 代数元, algebraic element, 166
 代数重数, algebraic multiplicity, 199
 仿射空间, affine space, 78
 伪逆, pseudoinverse, 291
 伴随矩阵, adjugate matrix, 145
 伴随算子, adjoint operator, 233, 257
 位置编码, positional encoding, 304
 余子式, minor, 142
 值向量, value vector, 308
 偶排列, even permutation, 137
 像, image, 119
 克拉姆法则, Cramer's rule, 146
 共轭相合, congruence by conjugate transpose, 252
 典范同构, canonical isomorphism, 220
 内直和, internal direct sum, 101
 内积, inner product, 229, 240
 内积空间, inner product space, 240
 内自同构, inner automorphism, 263
 准素分解, primary decomposition, 372, 373
 准素分量, primary component, 373
 几何重数, geometric multiplicity, 199
 分块对角矩阵, block diagonal matrix, 53
 分拆, partition, 332
 分离线, separatrix, 366
 列向量, column vector, 14
 列向量空间, column vector space, 14
 列满秩矩阵, full column rank matrix, 27
 列空间, column space, 75
 列随机矩阵, column-stochastic matrix, 196
 初等因子, elementary divisors, 377
 初等矩阵, elementary matrix, 45
 前馈网络, feed-forward network, 312
 加法, addition, 14
 半正定, positive semidefinite, 228, 252
 半负定, negative semidefinite, 228, 253
 单位根, root of unity, 58
 单位矩阵, identity matrix, 24
 单位矩阵, identity matrix, 44
 厄米特内积空间, Hermitian inner

product space, 253
 厄米特变换, Hermitian transformation, 256
 厄米特型, Hermitian form, 251
 厄米特阵, Hermitian matrix, 252
 友阵, companion matrix, 167, 205
 双曲平衡点, hyperbolic equilibrium, 364
 双线性型, bilinear form, 220
 双线性型的核, kernel of bilinear form, 225
 反对称双线性型, skew-symmetric bilinear form, 220
 反对称矩阵, skew-symmetric matrix, 49
 反射, reflection, 250
 可对角化, diagonalizable, 193
 可逆, invertible, 47
 右奇异向量, right singular vector, 273
 右逆, right inverse, 47
 和, sum, 99
 商空间, quotient space, 103
 因果语言模型, causal language model, 315
 因果遮罩, causal mask, 310
 坐标, coordinate, 95
 域 K 上的线性空间, 375
 域, field, 160
 域扩张, field extension, 165
 基, basis, 90
 基点, base point, 78
 基础行变换, elementary row operations, 23
 增广矩阵, augmented matrix, 24
 复数结构, complex structure, 166
 外直和, external direct sum, 101
 外自同构, outer automorphism, 263
 多头注意力, multi-head attention, 311
 多项式环, polynomial ring, 178
 天体运动论, Theoria Motus, 289
 夹角, angle, 241
 奇异值, singular value, 272
 奇异值分解, singular value decomposition, 270, 272
 奇异值分解定理, 272
 奇排列, odd permutation, 137
 奇点, singular point, 359, 363
 子域, subfield, 162
 子空间, subspace, 73, 81
 实对称矩阵谱定理, 247
 对偶基, dual basis, 220
 对偶空间, dual space, 219
 对合矩阵, involution, 204
 对称双线性型, symmetric bilinear form, 220
 对称矩阵, symmetric matrix, 49
 对角化, diagonalizable, 189
 对角矩阵, diagonal matrix, 44
 层归一化, layer normalization, 312, 314
 嵌入矩阵, embedding matrix, 303
 嵌入维度, embedding dimension, 303
 左奇异向量, left singular vector, 273
 左逆, left inverse, 47
 常微分方程, ordinary differential equation, 350
 常系数线性递推, linear recurrence, 340
 幂等矩阵, idempotent matrix, 204
 幂迭代, power iteration, 198
 幂零, nilpotent, 117
 幂零变换, nilpotent, 331
 幂零矩阵, nilpotent matrix, 204, 331
 幂零若尔当块, nilpotent Jordan block, 331
 平凡因式, trivial factor, 179

平稳分布, stationary distribution, 196
 平衡点, equilibrium, 359, 363
 平衡点的稳定性, stability of equilibrium, 359
 广义特征子空间, generalized eigenspace, 199
 庞加莱多项式, Poincaré polynomial, 35
 度量空间, metric space, 242
 开左半平面, open left half-plane, 361
 形式导数, formal derivative, 184
 循环子空间, cyclic subspace, 375
 循环矩阵, circulant matrix, 261
 快速傅立叶变换, fast Fourier transformation, 58
 快速傅立叶逆变换, inverse fast Fourier transformation, 58

 惯性指数, inertia index, 227
 扩域, extension field, 162
 拓扑等价, topological equivalence, 364
 排列
 符号, sign, 137
 数乘, scalar product, 14
 整除, divides, 179
 斜厄米特变换, skew-Hermitian transformation, 256
 方向空间, direction space, 78
 方阵, square matrix, 23
 星形结点, star node, 363
 最优最小二乘解, minimum norm least squares solution, 290
 最大公因式, greatest common divisor, 180, 181
 最小二乘法, least squares method, 290
 最小多项式, minimal polynomial, 167
 最简行阶梯型, reduced row echelon form, 24
 有理函数域, rational function field, 170
 有理标准型, rational canonical form, 372
 有理标准型定理, 377
 有限域
 \mathbb{F}_p , 161
 有限域, finite field, 161
 本原单位根, primitive root of unity, 58
 极分解, polar decomposition, 293
 极大线性无关组, maximal linearly independent set, 87
 极大线性无关组, maximal linearly independent subset, 89
 极小多项式, minimal polynomial, 202
 查询向量, query vector, 308
 标准内积空间, standard inner product space, 240
 标准正交基, orthonormal basis, 240, 255
 标签移位, shifted labels, 316
 核, kernel, 74, 118
 根, radical, 226
 根, root, 183
 格拉姆-施密特正交化, Gram-Schmidt process, 243
 格拉姆矩阵, Gram matrix, 221, 305
 概率向量, probability vector, 196, 303
 次数, degree, 178
 欧几里得空间, Euclidean space, 229
 正交, orthogonality, 241
 正交变换, orthogonal transformation, 245
 正交基, orthogonal basis, 224
 正交对角化, orthogonally diagonalizable, 246
 正交投影, orthogonal projection, 243
 正交相似, orthogonally similar, 246
 正交矩阵, orthogonal matrix, 244

正交群, orthogonal group, 244
 正交补, orthogonal complement, 226
 正定, positive definite, 228, 252
 正规变换, normal transformation, 256
 正规方程, normal equation, 290
 正规矩阵, normal matrix, 255
 正规矩阵谱定理, 256
 残差连接, residual connection, 312
 汉明码, Hamming code, 164
 法向量, normal vector, 250
 注意力机制, attention mechanism, 305
 渐近稳定, asymptotic stability, 360
 温度采样, temperature sampling, 321
 满秩矩阵, full rank matrix, 27
 潜在语义分析, latent semantic analysis, 271

 特征值, eigenvalue, 190
 特征向量, eigenvector, 190
 特征多项式, characteristic polynomial, 190
 特征子空间, eigenspace, 192
 特征方程, characteristic equation, 340
 特征脸, Eigenface, 288
 特殊正交群, special orthogonal group, 245
 相似, similar, 193
 相似矩阵, similar matrix, 115
 相合, congruent, 221
 相图, phase portrait, 362
 相容的, consistent, 30
 相抵, equivalent, 51
 相抵标准形, rank normal form, 51
 矩阵, matrix, 23
 矩阵乘法, matrix multiplication, 42, 43
 矩阵函数, matrix function, 351
 矩阵指数, matrix exponential, 350
 确定的, definite, 30
 秩, rank, 27
 秩, rank, 115
 秩标准形, rank normal form, 51
 稳定极点, stable pole, 361
 稳定结点, stable node, 362
 符号差, signature, 227
 第一有理标准型, first rational canonical form, 377
 第二有理标准型, second rational canonical form, 378
 等距变换, isometry, 245
 等距同构, isometry, 221
 系数的限制, restriction of scalars, 165
 系数矩阵, coefficient matrix, 24
 纯量矩阵, scalar matrix, 44
 线性函数, linear function, 16
 线性函数, linear functional, 219
 线性化系统, linearized system, 364
 线性同构, linear isomorphism, 118
 线性方程组, solution of system of linear equations, 18
 线性方程组, system of linear equations, 18
 线性无关, linearly independent, 83
 线性映射, linear map, 110
 线性映射空间, space of linear maps, 112
 线性生成, linear span, 75
 线性生成空间, linear span, 82
 线性相关, linearly dependent, 83
 线性码, linear code, 164
 线性空间, vector space, 163
 线性组合, linear combination, 16
 线性组合, linear combination, 82
 维数, dimension, 90

缩放因子, scaling factor, 309
 自伴随, self-adjoint, 248
 自回归模型, autoregressive model, 310
 自回归生成, autoregressive generation, 321
 自然投射, canonical projection, 104
 自由元, free unknowns, 28
 舒伯特胞腔, Schubert cell, 33, 35
 良定义, well-defined, 103
 若尔当块, Jordan block, 331
 若尔当标准型
 幂零变换, 332
 若尔当标准型, Jordan normal form, 338
 若尔当标准型定理, 338
 范德蒙德矩阵, Vandermonde matrix, 58
 螺旋汇, stable spiral, 362
 螺旋源, unstable spiral, 363
 行列式, determinant, 136, 140
 行变换, row operations, 23
 行满秩矩阵, full row rank matrix, 27
 行空间, row space, 75
 行阶梯型, row echelon form, 24
 行随机矩阵, row-stochastic matrix, 306
 补空间, complement space, 102
 表示矩阵, representation matrix, 113
 词表, vocabulary, 302
 谱分解, spectral decomposition, 256
 谱定理
 实对称矩阵, 247
 正规矩阵, 256
 线性变换形式, 256
 谷神星, Ceres, 289
 负定, negative definite, 228, 253
 贪心选择, greedy decoding, 321
 赋值映射, evaluation map, 183
 超越元, transcendental element, 166
 距离, distance, 240
 转移矩阵, transition matrix, 95
 转置矩阵, transpose matrix, 49
 辗转相除法, Euclidean algorithm, 180
 辛变换, symplectic transformation, 263
 辛基, symplectic basis, 230
 辛矩阵, symplectic matrix, 230
 辛群, symplectic group, 230
 迷向子空间, isotropic subspace, 233
 退化结点, degenerate node, 362
 逆序, inversion, 137
 逆序数, 137
 酉变换, unitary transformation, 256
 酉相似, unitary similarity, 255
 酉矩阵, unitary matrix, 255
 酉空间, unitary space, 253
 重根, multiple root, 184
 键向量, key vector, 308
 长度, length, 240
 阶数, order of matrix, 23
 阻尼因子, damping factor, 197
 陪集, coset, 103
 零化多项式, annihilation polynomial, 200
 零空间, null space, 74
 零空间, zero space, 74
 非退化, non-degenerate, 225
 鞍点, saddle point, 362
 首一多项式, monic polynomial, 178
 高斯系数, Gaussian coefficient, 36
 齐次常系数线性递推关系, homogeneous linear recurrence with constant coefficients, 340
 齐次线性方程组, system of homogeneous linear equations, 29