中图分类号:　　　　　　　　　　　　　　　　　　学校代码:　10055
UDC:　　　　　　　　　　　　　　　　　　　　　　密级:　公开

南開大學

硕 士 学 位 论 文

张量分解及其在图像加密和压缩中的应用

Tensor Decomposition and its Application in Image Encryption and Compression

论文作者　冯晓丹　　　　指导教师　杨庆之教授
申请学位　理学硕士　　　培养单位　数学科学学院
学科专业　计算数学　　　研究方向　最优化方法
答辩委员会主席　朱少红　评　阅　人　黄正海、吴春林

南开大学研究生院

二〇二〇年三月

南开大学学位论文使用授权书

本人完全了解《南开大学关于研究生学位论文收藏和利用管理办法》关于南开大学(简称“学校”)研究生学位论文收藏和利用的管理规定，同意向南开大学提交本人的学位论文电子版及相应的纸质本。

本人了解南开大学拥有在《中华人民共和国著作权法》规定范围内的学位论文使用权，同意在以下几方面向学校授权。即：

1.学校将学位论文编入《南开大学博硕士学位论文全文数据库》，并作为资料在学校图书馆等场所提供阅览，在校园网上提供论文目录检索、文摘及前16页的浏览等信息服务；

2.学校可以采用影印、缩印或其他复制手段保存学位论文；学校根据规定向教育部指定的收藏和存档单位提交学位论文；

3.非公开学位论文在解密后的使用权同公开论文。

本人承诺：本人的学位论文是在南开大学学习期间创作完成的作品，并已通过论文答辩；提交的学位论文电子版与纸质本论文的内容一致，如因不同造成不良后果由本人自负。

本人签署本授权书一份（此授权书为论文中一页)，交图书馆留存。

学位论文作者暨授权人(亲笔)签字：冯晓丹

2020 年 6 月 8 日

南开大学研究生学位论文作者信息

论文题目	张量分解及其在图像加密和压缩中的应用					
姓名	冯晓丹	学号	2120170039	答辩日期	2020 年 5 月 21 日	
论文类别	博士 □	学历硕士 √	专业学位硕士 □	同等学力硕士 □	划 √ 选择	
学院（单位）	数学科学学院	学科/专业（专业学位）名称	计算数学			
联系电话	18722559773	电子邮箱	18829280371@163.com			
通信地址(邮编)：	天津市卫津路94号南开大学，300071					
非公开论文编号		备注				

注：本授权书适用我校授予的所有博士、硕士的学位论文。由作者填写一份并签字后交校图书馆，如已批准为非公开学位论文，须附批准通过的《南开大学研究生申请非公开学位论文审批表》和“非公开学位论文标注说明”页。

南开大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师指导下进行研究工作所取得的研究成果。除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人创作的、已公开发表或者没有公开发表的作品的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。本学位论文原创性声明的法律责任由本人承担。

学位论文作者签名：冯晓丹　　2020 年 6 月 8 日

非公开学位论文标注说明

（本页表中填写内容须打印）

根据南开大学有关规定，非公开学位论文须经指导教师同意、作者本人申请和相关部门批准方能标注。未经批准的均为公开学位论文，公开学位论文本说明为空白。

<table>
<tr><td>论文题目</td><td colspan="3"></td></tr>
<tr><td>申请密级</td><td colspan="3">□限制(≤2 年)　□秘密(≤10 年)　□机密(≤20 年)</td></tr>
<tr><td>保密期限</td><td colspan="3">20 　年　月　日至 20 　年　月　日</td></tr>
<tr><td>审批表编号</td><td></td><td>批准日期</td><td>20 　年　月　日</td></tr>
</table>

南开大学学位评定委员会办公室盖章(有效)

注：限制★2 年(可少于 2 年)；秘密★10 年(可少于 10 年)；机密★20 年(可少于 20 年)

摘要

随着互联网技术的飞速发展，图像信息在人们的生活中越来越重要。图像的传输与存储过程中涉及到图像的安全问题以及图像对空间的占用问题，因此需要对图像进行加密和压缩。传统的图像加密方法大多是基于光学的加密。后来有学者提出了矩阵奇异值分解（SVD）与光学加密相结合的加密方法，将矩阵知识应用到了图像加密之中。但由于光学加密计算较复杂，所以上述方法计算效率不够高。本文从张量的角度，提出了基于张量 TTr1SVD（Tensor-Train rank-1 SVD）的图像加密方法。其基本思想是将图像数据表示为张量，分解为有限项秩-1 正交因子的线性组合，并将分解后的因子作为密文进行传输或存储。该方法的密钥空间较大，密文对重组顺序敏感，计算效率高于矩阵 SVD 和光学加密相结合的方法。矩阵 SVD 在灰度图像压缩中也有所应用，但其在彩色图像压缩中的应用性有限。本文利用彩色图像自然的张量特性，提出了基于张量 TTr1SVD 的图像压缩方法。此方法得到的压缩图像与原图像的近似误差是可度量的，而且可以根据不同的图像峰值信噪比（PSNR）得到不同程度的压缩图像。通过数值实验对上述方法进行了实现并验证了基于张量 TTr1SVD 的图像加密和图像压缩方法的可行性。

关键词： 张量分解；TTr1SVD；图像加密；图像压缩

Abstract

With the rapid development of Internet technology, image information is more and more important in people's life. In the process of image transmission and storage, the image security and image space occupation problems are involved, so it is necessary to encrypt and compress the image. Most of the traditional image encryption methods are based on optical encryption. Some scholars put forward the encryption method combining matrix singular value decomposition (SVD) and optical encryption methods, they applied the knowledge of matrix to image encryption. Since the calculation of optical encryption is relatively complicated, the calculation efficiency of the above method is not high enough. From a tensor perspective, this paper proposes an image encryption method based on TTr1SVD (Tensor-Train rank-1 SVD). The main idea is to represent the image data as a tensor, and then decompose the tensor into a linear combination of a finite number of rank-1 orthogonal factors, and transfer or store the decomposed factors as ciphertext. The key space of this method is large, the ciphertext is sensitive to the reorganization order, and the calculation efficiency is higher than the method of the combination of matrix SVD and optical encryption. Matrix SVD is also used in gray image compression, but its application in color image compression is limited. In this paper, a method of image compression based on TTr1SVD is proposed by using the natural tensor property of color image. The approximate error between the compressed image and the original image is measurable, and the compressed image can be obtained in different degrees according to different PSNR. The feasibility of image encryption and compression based on TTr1SVD is verified by numerical experiments.

Key Words: Tensor Decomposition; TTr1SVD; Image Encryption; Image Compression

目录

第一章　前言

第一节　背景介绍

随着互联网技术的飞速发展，人们的日常工作与生活中充斥着越来越多的信息，有文本、音频、图像（包含静态图片和动态视频）等。而图像信息又因其形象直观的特点，成为了当今社会人们表达及传递信息的主要方式。目前图像的传输和存储过程中面临着两个重要问题，一个是图像的安全问题，另一个是图像对传输信道带宽和存储空间的占用问题。图像的安全性主要表现在传输或存储的过程中不能被第三方窃取，或者遭遇恶意处理。尤其在一些特殊领域（如国防、军事、政府机关等）图像的安全性变得尤为重要。因为非法攻击者随时都有可能对这些信息进行恶意攻击或破坏，甚至利用窃取的信息从事一些破坏社会稳定和国家安全的活动。因此，图像安全是一个亟待解决的问题。图像在存储和传输的过程中占据了巨大的通信信道带宽及存储空间，这大大降低了人们对图像信息获取的效率。对其进行高效的压缩处理毫无疑问会使人们获取和利用图像信息的过程更加快捷。图像压缩正是解决如上问题的一个重要方法，其原理是尽量减少表示数字图像所需要的数据量。图像信息之所以能被压缩，是因为数据中存在着冗余。图像中的数据冗余主要有：编码冗余、像素冗余、心理视觉冗余。当这三种冗余中的一种或多种得到减少或消除时，就可以实现数据压缩的目的。

图像由最开始的黑白图像一步步发展为今天的彩色图像，其包含的数据量越来越大，数据维度也越来越高。因此矩阵逐渐不再能满足图像数据的表达需求。而张量做为矩阵的一个很自然的高维推广，能够方便直接地将图像信息进行表达。例如彩色 RGB 图像，它使用红（R）、绿（G）、蓝（B）三原色合成人类视力所能感知的任意颜色，每个像素点都用一个三维数组（R,G,B）表示，数组中每个元素代表对应颜色的灰度值。因此 RGB 图像可以很自然地用 $M\times N\times 3$ 的三阶张量表示。其中第三个维度值为“3”，代表 R、G、B 三个颜色信道，每个信道的数据用一个 $M\times N$ 的灰度矩阵表示。张量对高维数据表达的直观性使得张量逐渐成为人们研究高维数据的利器。矩阵分解有许多优良的性质，比如

最优低秩逼近以及误差可度量性，在很多方面都有应用。因此，尝试将矩阵分解的优良性质推广到张量分解，将更有助于探索高维数据的内在联系。

张量分解是近几十年来一个重要的研究方向，通过分解可以将高维海量数据用低维的数据来表示，这样可以大大减少对存储空间的占用。张量分解在很多领域都有所应用，例如计算机视觉、数据挖掘、信号处理、图分析等 [6-9]。张量分解有多种形式，例如 CP 分解、Tucker 分解 [1]、TT 分解、TTr1 分解等。这些分解形式都是矩阵奇异值分解（SVD）的高阶推广，因此可以将矩阵奇异值分解的一些良好性质推广到张量分解中。1927 年 Hitchcock[2,3] 首先提出了张量可以表示为有限个秩-1 张量和的思想。1944 年 Cattel[4,5] 又提出了平行比例分析的思想。直到 1970 年由 Carroll 和 Chang[10] 以 CANDECOMP 形式，Harshman[11] 以 PARAFAC 形式引入到心理计量领域才开始流行起来。后来人们将这一分解思想称为 CANECOMP/PARAFAC 分解（CP 分解）。CP 分解保留了矩阵奇异值分解中奇异值矩阵对角的性质，但因子矩阵的正交性无法保证。此外，CP 分解目前还没有既稳定又高效的算法，现有的大多数计算 CP 分解的算法都基于优化方法，比如 CP 分解中常用的算法——交替最小二乘算法（CP-ALS）。Tucker 分解于 1963 年由 Tucker[12] 首先提出，随后 Levin[13] 和 Tucker[14] 对其进行了改进。其思想是将张量分解为一个核张量沿着各个模态分别乘以对应的矩阵的形式。后来 De Lathauwer[15] 等人强调了分解的因子矩阵的正交性，将这种具有因子矩阵正交性的 Tucker 分解称为高阶奇异值分解（HOSVD），并证明了高阶奇异值分解是矩阵奇异值分解的有效推广。HOSVD 算法也成为求解 Tucker 分解的一种方法。值得注意的是，Tucker 分解并不是唯一的而且 Tucker 分解也不能作为求解张量秩的一种有效方法。此外，由于 Tucker 分解的核张量的规模随着张量阶数的增大呈指数增长，这样会带来维数灾难。对于上述两个张量分解形式存在的不足，Oseledets[16] 提出了一种简单的非递归的张量分解方法，称为 Tensor-Train 分解 (TT 分解)。通过矩阵奇异值分解和矩阵重塑将张量表示为三阶张量乘积和的形式，从而实现将 N 阶张量的存储转化为三阶辅助张量的存储，避免了维数灾难。这一分解过程可以用 TT-SVD 算法来实现。受到 TT 分解思想的启发，Batselier 等 [17] 提出了一种构造性的算法用于计算将张量分解为有限个秩-1 正交外积和的形式，这种分解形式称为 Tensor-Train rank-1 分解（TTr1 分解）。其求解算法称为 TTr1SVD 算法，工作原理是通过不断地利用矩阵 SVD 及向量重塑为矩阵，将原张量转换为 TTr1 形式。TTr1SVD 是矩阵 SVD 在张量情

形的自然推广。对于固定维度指标顺序的张量，TTr1SVD 求得的分解是唯一的。而且基于 TTr1 分解的低阶近似张量与原张量的误差也是容易度量的。

近些年，人们已经提出了很多图像加密算法，如基于矩阵变换的图像加密、基于混沌的图像加密、基于频域的图像加密 [18-20] 等。Chen 等在 [21] 中首先将矩阵奇异值分解 (SVD) 应用到图像加密中，提出了一种基于矩阵 SVD 和 Arnold 变换的图像加密算法。该方法先将图像转换到分数傅里叶域，然后在频率域中对图像矩阵进行 SVD，将分解得到的三个因子矩阵作为传输和存储的密文。这种方法增加了密钥空间的复杂度，提高了安全性。但该方法只将矩阵 SVD 应用到了灰度图像。相对于灰度图像，彩色图像包含更多的信息，可以描述更丰富的内容，因此对彩色图像的加密更具有现实意义。Abuturab 在 [22] 中首次提出了将矩阵 SVD 与 Gyrator 变换相结合的彩色图像加密算法，增强了密钥空间的复杂度和安全性。[23] 进一步将 HOSVD 与 Gyrator 变换和双相位随机掩膜相结合用于彩色图像加密。由于 SVD 和 HOSVD 的因子重组顺序较少，因此必须与已有的光学加密方法相结合。但光学加密方法也存在计算效率不高的问题。本文提出了基于张量 TTr1SVD 的图像加密方法，其基本思想是将图像数据表示为张量分解为有限项秩-1 正交因子的线性组合，并将分解后的因子作为密文进行传输或存储。由于 TTr1SVD 的分解因子数量多而且对重组顺序极其敏感，因此该方法的密钥空间比较大，密钥的敏感性也比较高。

图像压缩的方法有有损压缩和无损压缩。有损压缩利用人眼的视觉特性去除图像中的冗余信息和视觉不敏感的细节分量，经压缩后的图像在重构后与原始图像相比存在一定失真，但并不影响观看。有损压缩适用于人眼不敏感的自然图像，如广播电视、视频会议、日常生活中的图像等。有损压缩已经有很多压缩方法，比如基于离散余弦变换（DCT）的 JPEG 图像压缩方法，基于离散小波变换（DWT）的 JPEG2000 图像压缩方法，这些都是基于变换域的图像压缩方法。除此之外，还有在空间域中基于矩阵 SVD 的图像压缩方法 [24-26]。但是该方法主要应用于灰度图像，对于彩色图像其应用性有限。本文提出了基于张量 TTr1SVD 的图像压缩方法，该方法可以直接在空间域对彩色图像或者彩色视频图像进行压缩处理。由此方法得到的压缩图像的近似误差可度量，且可以根据给定的图像 PSNR 和近似误差 ε 来得到不同程度的压缩图像。

本文内容主要安排如下：

第二章首先介绍了张量相关的基本概念，如张量范数的定义，Kronecker 积，

张量与矩阵的模-n 乘积及其性质等。然后介绍了四种张量分解形式：Tucker 分解、CP 分解、TT 分解以及 TTr1 分解的基本思想、主要的求解算法及不同分解形式之间的关系。

第三章介绍了基于张量分解的图像加密方法。首先介绍了已有的基于矩阵 SVD 和 Gyrator 变换的的图像加密算法和基于张量 HOSVD 和 Gyrator 变换的图像加密算法。将矩阵或张量分解应用于图像加密有效地增加了密钥空间的复杂性，增强了密文的安全性。然后提出将张量 TTr1 分解应用到彩色图像加密中，并且观察到相比于基于 SVD 和 HOSVD 的方法，基于 TTr1SVD 的图像加密方法密钥空间更大，而且密钥对于重组顺序极其敏感。因此进一步增大了密钥空间，增加了密文的破解难度，计算效率也有所提高。

第四章主要介绍了张量分解在图像压缩上的应用。首先介绍了基于矩阵 SVD 的灰度图像压缩方法。然后提出基于张量 TTr1SVD 的彩色图像和彩色视频的压缩方法。TTr1SVD 方法得到的近似张量的误差可度量，且对于给定的 PSNR 值或误差值 ε，可以快速得到满足条件的压缩图像。

第五章对于本文的工作进行了总结，对当前存在的问题进行了分析，并对未来的工作进行了展望。

第二节 符号说明

在本文中，用小写字母 a,u,v 来表示标量；小写加粗的 $\mathbf{a},\mathbf{u},\mathbf{v}$ 表示向量，其中向量 $\mathbf{a}$ 的第 i 个元素用 $\mathbf{a}_i$ 表示；用大写字母 A,U,V,S 表示矩阵，矩阵 A 的第 (i,j) 项元素表示为 $A(i,j)=a_{ij}$，矩阵的第 i 行表示为 $A(i,:)$，第 j 列表示为 $A(:,j)$；用花体大写字母 $\mathcal{A},\mathcal{B},\mathcal{C}$ 表示张量，N 阶张量 $\mathcal{A}$ 的第 $(i_1,i_2,\cdots,i_N)$ 项元素记为 $\mathcal{A}(i_1,i_2,\cdots,i_N)=a_{i_1i_2\cdots i_N}$。$\mathbb{R}^{I_1}$ 表示向量空间，$\mathbb{R}^{I_1\times I_2}$ 表示矩阵空间，$\mathbb{R}^{I_1\times I_2\times\cdots\times I_N}$ 表示 N 阶张量空间。

第二章　张量和张量分解

张量是矩阵的高阶推广，矩阵中的一些基本运算及性质都可以推广到高阶张量。本章主要介绍张量的基本概念及基本运算和性质。其中着重介绍了张量的分解及求解算法。

第一节　张量基本知识

一般地，将一维数组称为向量，二维数组称为矩阵，三维及以上的数组称为张量。一个 N 维数组，即 N 阶张量可表示为如下形式：

$$\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$$

张量中的元素表示为 $\mathcal{A}(i_1, i_2, \cdots, i_N) = a_{i_1 i_2 \cdots i_N}$，其中 $i_k = 1, 2, \cdots, I_k$。

类似于矩阵的行和列，将张量中除 i_k 之外的其他维度下标固定的形式 $\mathcal{A}(i_1, \cdots, i_{k-1}, :, i_{k+1}, \cdots, i_N) = a_{i_1 \cdots i_{k-1} : i_{k+1} \cdots i_N}$ 称为张量的纤维（fibers）。例如三阶张量 $\mathcal{A} \in \mathbb{R}^{I \times J \times K}$ 有列纤维 $a_{:jk}$、行纤维 $a_{i:k}$ 和管纤维 $a_{ij:}$。将张量中除两个维度以外的其余维度下标固定的形式称为张量的切片（slices），如三阶张量有水平切片 $a_{i::}$、横向切片 $a_{:j:}$ 和正面切片 $a_{::k}$。

以下定义及性质主要参考自文献 [1]。

定义 2.1 张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的范数 *(Frobenius-norms)* 是其所有元素平方求和后的平方根，表示为：

$$\|\mathcal{A}\|_F = \sqrt{\sum_{i_1=1}^{I_1} \sum_{i_2=1}^{I_2} \cdots \sum_{i_N=1}^{I_N} a_{i_1 i_2 \cdots i_N}^2}$$

定义 2.2 两个规模相同的张量 $\mathcal{A}, \mathcal{B} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的内积等于两个张量对应元素乘积的和，表示为：

$$\langle \mathcal{A}, \mathcal{B} \rangle = \sum_{i_1=1}^{I_1} \sum_{i_2=1}^{I_2} \cdots \sum_{i_N=1}^{I_N} a_{i_1 i_2 \cdots i_N} b_{i_1 i_2 \cdots i_N}$$

由张量范数和张量内积的定义可以很自然得出：$\langle \mathcal{A}, \mathcal{A} \rangle = \|\mathcal{A}\|_F^2$。

定义 2.3 给定两个张量 $\mathcal{A}, \mathcal{B} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，如果这两个张量满足：

$$\langle \mathcal{A}, \mathcal{B} \rangle = 0$$

则称张量 $\mathcal{A}$ 和 $\mathcal{B}$ 是正交的。

定义 2.4 如果 N 阶张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 可以表示为 N 个向量外积的形式：

$$\mathcal{A} = a^{(1)} \circ a^{(2)} \circ \cdots \circ a^{(N)}$$

则称张量 $\mathcal{A}$ 是秩-*1* 的，其中“$\circ$”为向量的外积运算。秩-*1* 张量的元素可表示为：

$$\mathcal{A}(i_1, i_2, \cdots, i_N) = a_{i_1}^{(1)} a_{i_2}^{(2)} \cdots a_{i_N}^{(N)}\ , \quad (1 \leq i_k \leq I_k)$$

既然张量是矩阵的高阶推广，那么就涉及到两者之间的转化问题：如何将张量转化为矩阵形式。于是提出了张量的矩阵化，即张量的模-n 展开，是一个将张量的模-n 纤维根据特定的下标顺序重排为矩阵的过程。张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的模-n 矩阵表示为 $A_{(n)} \in \mathbb{R}^{I_n \times I_1 \cdots I_{n-1} I_{n+1} \cdots I_N}$。原张量中的元素 $\mathcal{A}(i_1, i_2, \cdots, i_N)$ 与模-n 展开后的矩阵中元素 $A_{(n)}(i_n, j)$ 的对应关系满足：

$$j = 1 + \sum_{k=1,\ k \neq n}^{N} (i_k - 1)\mathbf{J}_k\ , \quad \text{其中：} \mathbf{J}_k = \sum_{m=1,\ m \neq n}^{k-1} \mathbf{I}_m$$

本文采用了上述张量矩阵化方法，其余更多的张量矩阵化方法可以见 [27]。

定义 2.5 如果张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的元素满足当且仅当 $i_1 = i_2 = \cdots = i_N$ 时才有 $a_{i_1 i_2 \cdots i_N} \neq 0$ 成立，则称 $\mathcal{A}$ 是对角张量。

矩阵中有矩阵和向量以及矩阵和标量的乘积，那么将这些乘法运算推广到张量中，就有如下乘积计算形式：

定义 2.6 张量与矩阵的模-n 乘积。张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 与矩阵 $C \in \mathbb{R}^{J \times I_n}$ 模-n 乘积表示为：

$$\mathcal{B} = \mathcal{A} \times_n C$$

其中 $\mathcal{B} \in \mathbb{R}^{I_1 \times \cdots \times I_{n-1} \times J \times I_{n+1} \times \cdots \times I_N}$。张量与矩阵模-$n$ 乘积的元素可表示为：

$$(\mathcal{A} \times_n C)_{i_1 \cdots i_{n-1} j i_{n+1} \cdots i_N} = \sum_{i_n=1}^{I_n} a_{i_1 i_2 \cdots i_N} c_{j i_n}$$

由上述定义可以很容易得出如下张量和矩阵模-n 乘积的性质：

性质 2.1 给定张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，矩阵 $C \in \mathbb{R}^{J \times I_n}$，则有：

$$\mathcal{B} = \mathcal{A} \times_n C \Longleftrightarrow B_{(n)} = CA_{(n)}$$

性质 2.2 给定张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，矩阵 $B \in \mathbb{R}^{J_m \times I_m}$, 矩阵 $C \in \mathbb{R}^{J_n \times I_n}$，则有：

$$\mathcal{A} \times_m B \times_n C = \mathcal{A} \times_n C \times_m B\,, \quad (m \neq n)$$

当 $m = n$ 时有：

$$\mathcal{A} \times_n B \times_n C = \mathcal{A} \times_n (BC)$$

定义 2.7 张量与向量的模-n 乘积。张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 与向量 $\mathbf{v} \in \mathbb{R}^{I_n}$ 的模-n 乘积用 $\mathcal{A} \bar{\times}_n \mathbf{v}$ 表示，其结果是一个规模为 $I_1 \times \cdots \times I_{n-1} \times I_{n+1} \times \cdots \times I_N$ 的 $N-1$ 阶张量，元素形式表示如下：

$$(\mathcal{A} \bar{\times}_n \mathbf{v})_{i_1 \cdots i_{n-1} i_{n+1} \cdots i_N} = \sum_{i_n=1}^{I_n} a_{i_1 i_2 \cdots i_N}\, v_{i_n}$$

性质 2.3 给定张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，向量 $\mathbf{u} \in \mathbb{R}^{I_m}$ 和 $\mathbf{v} \in \mathbb{R}^{I_n}$，则有：

$$\mathcal{A} \bar{\times}_m \mathbf{u} \bar{\times}_n \mathbf{v} = (\mathcal{A} \bar{\times}_m \mathbf{u})\, \bar{\times}_{n-1} \mathbf{v} = (\mathcal{A} \bar{\times}_n \mathbf{v})\, \bar{\times}_m \mathbf{u}\,, \quad (m < n)$$

定义 2.8 及性质 2.4 主要参考自文献 [1, 28]。

定义 2.8 两个矩阵 $A \in \mathbb{R}^{I \times J}$ 和 $B \in \mathbb{R}^{K \times L}$ 的 *Kronecker* 乘积表示为 $A \otimes B$, 其结果是一个规模为 $IK \times JL$ 的矩阵。具体乘积过程表示为：

$$\begin{aligned} A \otimes B &= \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1J}B \\ a_{21}B & a_{22}B & \cdots & a_{2J}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{I1}B & a_{I2}B & \cdots & a_{IJ}B \end{bmatrix} \\ &= \begin{bmatrix} a_1 \otimes b_1 & a_1 \otimes b_2 & a_1 \otimes b_3 & \cdots & a_J \otimes b_{L-1} & a_J \otimes b_L \end{bmatrix} \end{aligned}$$

性质 2.4 $(A \otimes B)(C \otimes D) = AC \otimes BD$

根据上述张量和矩阵模-n 乘积的定义、性质以及 Kronecker 积的定义，可以得到如下性质：

性质 2.5 给定 N 阶张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，矩阵 $C^{(n)} \in \mathbb{R}^{J_n \times I_n}$，则对于任意的 $n \in \{1, \cdots, N\}$，有：

$$\mathcal{B} = \mathcal{A} \times_1 C^{(1)} \times_2 C^{(2)} \cdots \times_N C^{(N)}$$

$$\iff \quad B_{(n)} = C^{(n)} A_{(n)} \left(C^{(N)} \otimes \cdots \otimes C^{(n+1)} \otimes C^{(n-1)} \otimes \cdots \otimes C^{(1)} \right)^T$$

该性质的证明可见 [27]。

第二节 张量分解

张量分解是张量中非常重要的一个部分，有助于进一步探索研究张量元素之间的关系。本节对张量的 Tucker 分解、CP 分解、TT 分解以及 TTr1 分解的基本思想、相关求解算法以及各分解的优势与不足进行了简要的介绍。

2.2.1 Tucker 分解

Tucker 分解是将 N 阶张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 表示成一个核张量和有限个因子矩阵模-n 乘积的形式：

$$\begin{aligned} \mathcal{A} &= \mathcal{G} \times_1 U^{(1)} \times_2 U^{(2)} \cdots \times_N U^{(N)} \\ &= \sum_{j_1=1}^{J_1} \sum_{j_2=1}^{J_2} \cdots \sum_{j_N=1}^{J_N} \mathcal{G}_{j_1 j_2 \cdots j_N} u_{j_1}^{(1)} \circ u_{j_2}^{(2)} \circ \cdots \circ u_{j_N}^{(N)} \end{aligned} \tag{2.1}$$

其中，$U^{(n)} = \left[u_1^{(n)} \ u_2^{(n)} \ \cdots u_{J_n}^{(n)} \right] \in \mathbb{R}^{I_n \times J_n}, (n = 1, 2, \cdots, N)$，为因子矩阵。$\mathcal{G} \in \mathbb{R}^{J_1 \times J_2 \times \cdots \times J_N}$ 为核张量，其元素代表不同因子矩阵之间的相互作用水平。张量 $\mathcal{A}$ 中每个元素可表示为：

$$a_{i_1 i_2 \cdots i_N} = \sum_{j_1=1}^{J_1} \sum_{j_2=1}^{J_2} \cdots \sum_{j_N=1}^{J_N} g_{j_1 j_2 \cdots j_N} u_{i_1 j_1}^{(1)} u_{i_2 j_2}^{(2)} \cdots u_{i_N j_N}^{(N)} \tag{2.2}$$

其中 $i_n = 1, 2, \cdots, I_n$, $n = 1, 2, \cdots, N$。

De Lathauwer 等在 [15] 中强调了 Tucker 分解的因子矩阵的正交性，得到了 Tucker 分解的一种特殊情况，称之为高阶奇异值分解（HOSVD），并且证明了 HOSVD 是矩阵 SVD 的一种很自然且令人信服的高阶推广。

定理 2.1 张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的 *HOSVD* 可表示为：

$$\mathcal{A} = \mathcal{S} \times_1 U^{(1)} \times_2 U^{(2)} \cdots \times_N U^{(N)} \tag{2.3}$$

其中，$U^{(n)} = \left[u_1^{(n)} u_2^{(n)} \cdots u_{I_n}^{(n)}\right]$ 是 $I_n \times I_n$ 的正交矩阵，$\mathcal{S} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 是核张量。用 $\mathcal{S}_{i_n=\alpha}$ 表示将 $\mathcal{S}$ 的第 n 维下标固定的子张量。那么核张量 $\mathcal{S}$ 具有如下性质：

1. 全正交性。对于任意的 n、α、β，$\alpha \neq \beta$, 子张量 $\mathcal{S}_{i_n=\alpha}$ 和 $\mathcal{S}_{i_n=\beta}$ 是正交的：

$$\left\langle \mathcal{S}_{i_n=\alpha}, \mathcal{S}_{i_n=\beta} \right\rangle = 0\,, \quad (\alpha \neq \beta) \tag{2.4}$$

2. 有序性。对于所有 n 的可能取值，有：

$$\|\mathcal{S}_{i_n=1}\|_F \geq \|\mathcal{S}_{i_n=2}\|_F \geq \cdots \geq \|\mathcal{S}_{i_n=I_n}\|_F \geq 0 \tag{2.5}$$

上述范数 $\|\mathcal{S}_{i_n=i}\|_F$ 也可记为 $\sigma_i^{(n)}$, 它是张量 $\mathcal{A}$ 的模-n 展开矩阵 $A_{(n)}$ 的第 i 个奇异值，称为 $\mathcal{A}$ 的模-n 奇异值。$A_{(n)}$ 的左奇异向量 $U_i^{(n)}$ 称为 $\mathcal{A}$ 的第 i 个模-n 奇异向量。

定理 2.1 的矩阵形式可等价表示为：

$$A_{(n)} = U^{(n)} \cdot S_{(n)} \cdot \left(U^{(N)} \otimes \cdots \otimes U^{(n+1)} \otimes U^{(n-1)} \otimes \cdots \otimes U^{(1)}\right)^T \tag{2.6}$$

[15] 表明了张量 HOSVD 中的因子矩阵 $U^{(1)}, U^{(2)} \cdots, U^{(N)}$ 可以分别由张量 $\mathcal{A}$ 的模-n 展开矩阵 $A_{(n)}$ 进行 SVD 后的左奇异矩阵 $U^{(n)}$ 得出。核张量 $\mathcal{S}$ 满足如下形式：

$$\mathcal{S} = \mathcal{A} \times_1 U^{(1)^T} \times_2 U^{(2)^T} \cdots \times_N U^{(N)^T} \tag{2.7}$$

由此可自然地给出一种求解特殊形式 Tucker 分解的算法，具体过程如下：

Algorithm 1 HOSVD

Input:

N 阶张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$;

Output:

核张量 $\mathcal{S}$，正交因子矩阵 $U^{(1)}, U^{(2)} \cdots, U^{(N)}$;

for $n = 1, 2, \cdots, N$ **do**
  $U^{(n)} \leftarrow$ 张量 $\mathcal{A}$ 的模-n 展开矩阵 $A_{(n)}$ 的左奇异矩阵;
end for
$\mathcal{S} = \mathcal{A} \times_1 U^{(1)^T} \times_2 U^{(2)^T} \cdots \times_N U^{(N)^T}$

下面引入张量 n-秩的概念 [1]:

定义 2.9 张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的 n-秩指的是张量的模-n 展开矩阵 $A_{(n)}$ 的列秩，记为 $rank_n(\mathcal{A})$，即 $rank_n(\mathcal{A}) = rank(A_{(n)})$。若一个 N 阶张量的 n-秩分别为 r_n, $n = 1, 2, \ldots, N$，则称该张量为秩-$(r_1, r_2, \ldots, r_N)$ 张量。

对于一个给定的张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$，根据 HOSVD 算法将很容易可以得到秩-$(r_1, r_2, \ldots, r_N)$ 的分解。当一个或者多个 r_n 满足 $r_n \leq rank_n(\mathcal{A})$ 时，此时得到的是张量的近似。

2.2.2 CP 分解

CP 分解是指将张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 表示为有限个秩-1 张量和的形式。具体表示如下：

$$\mathcal{A} \approx \sum_{r=1}^{R} v_r^{(1)} \circ v_r^{(2)} \circ \cdots \circ v_r^{(N)} \tag{2.8}$$

其中，R 是正整数，$v_r^{(n)} \in \mathbb{R}^{I_n}$, $r = 1, 2, \cdots, R$，$n = 1, 2, \cdots, N$。

在使用中，为了方便常把 $v_r^{(n)}$ 进行归一化，并将其长度参数统一用 λ_r 表示，于是 CP 分解又可表示为：

$$\mathcal{A} \approx \sum_{r=1}^{R} \lambda_r u_r^{(1)} \circ u_r^{(2)} \circ \cdots \circ u_r^{(N)} \tag{2.9}$$

其中，$\lambda = [\lambda_1\ \lambda_2\ \cdots \lambda_R] \in \mathbb{R}^R$。$u_r^{(i)}$ 是长度为 1 的向量，$i = 1, \cdots, N$，$r = 1, \cdots, R$。将秩-1 项中的各向量组合成矩阵形式 $U^{(n)} = \left[u_1^{(n)}\ u_2^{(n)}\ \cdots\ u_R^{(n)}\right]$，$U^{(n)} \in \mathbb{R}^{I_n \times R}$，$n = 1, 2, \cdots, N$，称之为 CP 分解的因子矩阵。

由张量 CP 分解的定义可知，CP 分解是核张量为 $R \times R \times \cdots \times R$ 对角张量的 Tucker 分解。因此，CP 分解是 Tucker 分解的一种特殊形式。CP 分解也是矩阵 SVD 的一个高阶推广，它有类似于矩阵 SVD 的奇异值的性质，但是并没有对各秩-1 张量中向量的正交性进行限制。

不同于矩阵秩的定义，张量秩的定义有多种。其中一种比较常用的秩：tensor rank，即张量秩，是基于张量的 CP 分解形式来定义的，具体定义如下 [1, 2]：

定义 2.10 *张量 $\mathcal{A} \in \mathbb{R}^{I_1 \times I_2 \times \cdots \times I_N}$ 的秩记为 $rank(\mathcal{A})$, 等于 $\mathcal{A}$ 的 CP 分解中最少的秩-1 张量的个数，数学表示为：*

$$rank(\mathcal{A}) := min\{R \mid \exists\, u_r^{(n)} \in R^{I_n}\ s.t.\ \mathcal{A} = \sum_{r=1}^{R} u_r^{(1)} \circ u_r^{(2)} \circ \cdots \circ u_r^{(N)}\}$$

张量秩与矩阵的秩还有一个不同之处就是，矩阵的秩目前有算法可以直接求得，而张量秩目前为止还没有可以直接求解的通用算法，计算张量秩是一个 NP-hard 的问题 [29]。大部分 CP 分解的算法都基于优化方法，如 CP 分解中常用的 ALS 算法 (交替最小二乘算法)[10,11]。值得注意的是，即使给定了张量秩 R，ALS 算法求解 CP 分解也可能是不适定的，其结果不能保证收敛到全局最优。