

责任编辑：何嘉琳
封面设计：盛唐文化

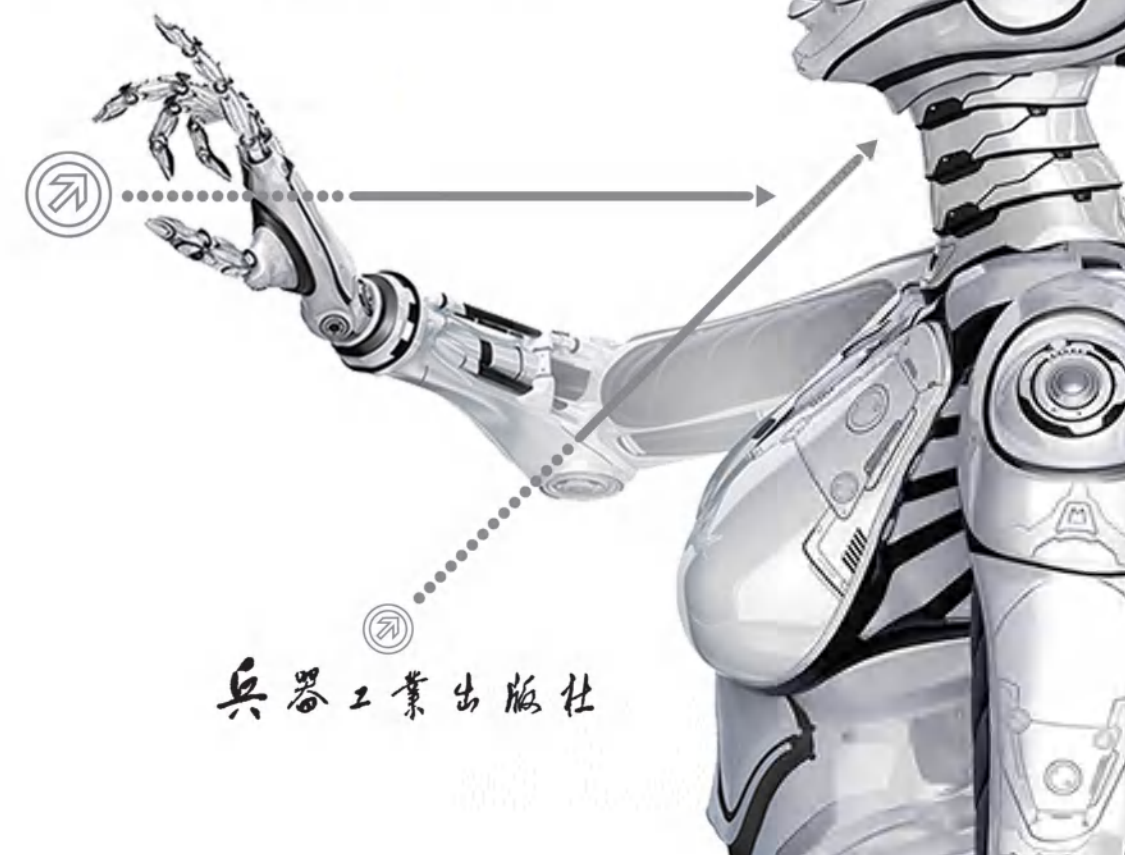
首届全国大模型与决策智能大会论文集

中国指挥与控制学会 编

兵器工业出版社

首届全国大模型 与决策智能大会 论文集

中国指挥与控制学会 编



兵器工业出版社

首届全国大模型 与决策智能大会

论文集

ISBN 978-7-5181-1083-4



定价：256.00元

首届全国大模型与决策智能 大会论文集

中国指挥与控制学会 编

兵器工业出版社

内 容 简 介

首届全国大模型与决策智能大会论文集是敏锐抓住科技革命方向，大力推动科技跨越发展，勇攀科技高峰的重要媒介，是我国指挥控制领域科技工作者研究成果的汇集，充分展示了指挥控制领域科技工作者在大模型与决策智能领域最新的研究进展和成果。2024年，论文征集工作正式启动，大会组委会收到了大量论文，经论文评审委员会审核，汇编成《首届全国大模型与决策智能大会论文集》，并出版发行。

本书可供大模型与决策智能领域相关从业者及研究人员参考使用。

图书在版编目（CIP）数据

首届全国大模型与决策智能大会论文集 / 中国指挥与控制学会编. — 北京：兵器工业出版社，2024. 11.
ISBN 978-7-5181-1083-4

I. TP18-53

中国国家版本馆CIP数据核字第2024DA0278号

出版发行：兵器工业出版社

发行电话：010-68962596，68962591

邮 编：100089

社 址：北京市海淀区车道沟10号

经 销：各地新华书店

印 刷：北京华夏瑞诚科技有限公司

版 次：2024年11月第1版第1次印刷

责任编辑：何嘉琳

封面设计：盛唐文化

责任校对：任 丽

责任印制：王京华

开 本：787×1092 1/16

印 张：21.5

字 数：508千字

定 价：256.00元

前 言

为深入贯彻党的二十大精神，坚持以习近平新时代中国特色社会主义思想为指导，全面落实“增加新域新质作战力量比重，加快无人智能作战力量发展”和“研究掌握信息化智能化战争特点规律”的重要指示精神，为牢牢把握智能化核心技术创新发展原动力，构建产学研相融合的协同创新体系，加快军事智能化发展，提升锻造智能化作战能力，加速推进军事智能化的高质量发展。由中国指挥与控制学会主办，国防科技大学系统工程学院承办，于2024年7月19—21日在杭州召开以“大模型与决策智能交融共进”为主题的“首届全国大模型与决策智能大会”。《首届全国大模型与决策智能大会论文集》作为我国指挥与控制领域和人工智能领域科技工作者成果的汇编，是广大科技工作者展示学科发展焦点、领域创新思维、科研实践结果的重要媒介，是推动智能指挥控制学科技术领域学术交流的重要载体。自2023年12月启动本届大会论文征集工作以来，经大会评审委员会审核，选出37篇论文汇集成《首届全国大模型与决策智能大会论文集》出版发行。值此论文集出版之际，对所有关心与支持本届大模型与决策智能大会的单位、领导、专家和学者表示衷心的感谢，同时，祝愿同行们在智能指挥控制技术领域的探索道路上取得更加辉煌的成就。

编者

2024年7月

目 录

ChatGPT 在教育教学的应用：多学科视角下的文献计量分析

..... 谢远涵 赵金辉 黄 山 王 涛 (1)

SWARM-LLM：基于大语言模型的无人集群任务规划系统

..... 李婷婷 王 琪 王嘉康 徐勇军 (13)

大模型赋能航空战术分析应用研究 ... 贾长江 范 鹏 杨凯达 张龙飞 夏少杰 (15)

大模型启发增强的未知混叠雷达信号分选方法

..... 牛恺锐 齐佩汉 李 甫 林 云 (25)

大模型驱动多智能体的军事需求生成框架 李嘉晖 张萌萌 陈洪辉 (34)

大模型在陆战兵棋推演中的应用研究

..... 刘大勇 董志明 刘倬立 邱雪欢 冯琦琦 (36)

大小模型协同推理在阵地部署和火力分配中的应用

..... 黄成琪 梁文谦 张 勇 家会臣 胡 月 (47)

大语言模型赋能冲突博弈分析 顾天阳 葛冰峰 黄宇铭 韩思宁 侯泽强 (56)

多智能体决策新范式：强化学习与大模型融通演进技术分析及

军事应用展望 张伊丹 陈 展 赵新昱 王 磊 贾 婕 刘晓暄 (67)

基于 PP-LCNet 微调的电子器件文档解析 吴枕畅 陈泓材 (75)

基于大模型 RAG 微调与增强的智能运维方法 林 白 高锦杰 李宏伟 (82)

基于大模型检索增强的情报智能认知技术研究

..... 栾 真 王又辰 李 楠 刘宝琪 冯 帆 (90)

基于大语言模型的复杂问题分解流程自动生成方法

..... 李 敏 牛 婵 闫 林 樊志强 夏晓凯 (99)

基于大语言模型的军事方案自动生成框架设计 王晓明 包 括 滕 飞 (110)

基于大语言模型的军事智能翻译算法研究 张聚憬 杨 娟 谢林川 (120)

基于大语言模型的智能决策技术概览

..... 王 琪 李雪飞 李婷婷 王嘉康 徐勇军 (128)

基于大语言模型的作战辅助决策智能体框架设计

..... 李 凯 王 瑞 许 霄 郭圣明 陶九阳 (142)

基于多模态大模型的态势认知方法与应用

..... 武 霞 王元斌 李 鼎 王振杰 高子文 (152)

基于混合检索增强的双塔模型技术研究

..... 郜洪奎 马瑞祥 包骥豪 夏少杰 瞿崇晓 (160)

基于两阶段检索增强的信息问答方法

..... 张 然 江 松 郑明琪 刘 冰 张 兵 陈晓慧 (169)

基于模仿学习的多智能体追捕决策方法

..... 王焱宁 张锋镝 肖登敏 孙中奇 杜长坤 (180)

基于三段式检索增强框架的 NL2SQL 技术研究

..... 马瑞祥 郜洪奎 雷 达 郎 彬 瞿崇晓 (191)

基于输入扰动的多模态大语言模型不确定性估计

..... 荆诗雨 陈 炜 龚闪闪 张星辉 崔 星 (198)

基于算子融合和向量化访存的大语言模型部署优化研究

..... 明 刚 张艳霞 李旭胜 叶子扬 冯 力 邢焕来 朱宗海 (207)

基于智能体工作流的体系智能架构研究

..... 李 广 肖 一 胡鹏举 聂 璐 赵晓宁 (218)

基于综合智能推理链方法 (IIRC) 的芯片技术文档解析与模型生成

..... 许一品 陈泓材 (228)

空战博弈场景下态势事件图谱构建及决策应用

..... 郎 彬 雷 达 陈久红 马瑞祥 胡天祥 (236)

面向气象领域的大语言模型增量预训练技术研究

..... 雷 达 马瑞祥 瞿崇晓 张永晋 余华峰 (246)

面向时变环境的大小模型协同决策方法研究

..... 韩云君 王 玮 张羽丰 陶志坤 沈 震 (255)

面向用例生成与代码优化的多智能体软件测试框架

..... 杨 军 何宇巍 刘行健 (265)

融合检索增强和思维链提示的大模型关系抽取方法

..... 刘 琦 张长亮 杨雨婷 方 志 郑一凡 (273)

生成式任务网：基于大模型的任务规划与执行新范式

..... 黄雪芹 张 胜 朱先强 张千桢 朱 承 (282)

视觉语言大模型在目标分析领域的应用 张明新 陈亚洲 (285)

视觉语言大模型在网络舆情分析领域的应用：潜力与挑战 刘晓亮 马 壮 (310)

通信网络与 AI 大模型的融合发展研究

..... 瞿崇晓 唐宇波 吴高洁 范长军 张永晋 刘 硕 (322)

一种基于知识图谱的检索增强生成情报问答技术

..... 成志宇 陈星霖 王 菁 周中元 张志政 (324)

一种结合敏感词匹配和提示词构建的仇恨言论检测方法

..... 徐 磊 孙家栋 胡亚豪 潘志松 (326)

ChatGPT 在教育教学的应用：多学科视角下的文献计量分析

谢远涵¹ 赵金辉¹ 黄山¹ 王涛^{1*}

摘要 文章揭示了 ChatGPT 在艺术与人文、生命科学与生物医药、理学、社会科学、技术五个领域教育应用的情况。研究发现，ChatGPT 在个性化学习、自动评估和协作学习等方面展现出显著优势，能有效提高学习效率、增强学习动机和培养某些高阶思维技能。影响 ChatGPT 教学效果的关键因素包括学生的技术接受度、教师的 AI 素养、学科特性等。然而，现有研究无法回答其在不同学科和学习任务中的效果差异。某些重要领域 ChatGPT 的教育应用研究相对不足。

关键词 ChatGPT, 教育应用, 系统文献综述, 个性化学习, 教学效果, 跨学科应用

Empowering Teaching with ChatGPT: A Bibliometric Analysis from Multidisciplinary Perspectives

XIE Yuan-Han¹ ZHAO Jin-Hui¹ HUANG Shan¹ WANG Tao^{1*}

Abstract This study reveals the application of ChatGPT in education across five domains: arts and humanities, life sciences and biomedicine, physical sciences, social sciences, and technology. The research finds that ChatGPT demonstrates significant advantages in personalized learning, automatic assessment, and collaborative learning, effectively improving learning efficiency, enhancing learning motivation, and cultivating certain higher-order thinking skills. Key factors influencing ChatGPT's teaching effectiveness include students' technology acceptance, teachers' AI literacy, and subject characteristics. However, existing studies cannot fully address the differences in its effectiveness across various disciplines and learning tasks. Research on ChatGPT's educational applications is relatively insufficient in certain important fields.

Key words ChatGPT, educational applications, systematic literature review, personalized learning, teaching effectiveness, interdisciplinary applications

0 引言

自 ChatGPT 问世以来，因其出色的知

识表现，其在教育教学中的应用研究呈现爆炸式增长^[1]。这些研究涵盖了广泛的主题，包括：① ChatGPT 在协助教师、辅导学生、个性化学习和自动化评估等方面的

1. 国防科技大学系统工程学院

1. College of Systems Engineering, National University of Defense Technology

优势；②ChatGPT 应用中的挑战，如内容不准确、学术诚信问题、伦理和隐私风险，以及对用户创造力和批判性思维能力的潜在影响；③关于更新教学评估方法、制定机构政策、促进教师专业发展和提高学生 AI 素养等方面的建议和未来趋势^[2-3]。值得注意的是，研究趋势已经从初期的立场和概念性论文逐渐向对教育教学的实证研究转变。

本文旨在通过对 298 篇相关文献的全面回顾和分析，从多学科视角探究大模型在各个专业领域的教学应用情况。本文将重点关注：①ChatGPT 在不同教育场景和学科中的应用及积极影响；②ChatGPT 驱动的创新教学方法和学习体验；③ChatGPT 在教育中应用的未来趋势和建议。

1 相关工作

ChatGPT 在教育中的应用已成为一个跨学科的研究热点。如其在研究指导、科学教育等特定领域的潜力^[4-6]、探讨 AI 工具在教育中的多样化应用，包括认知思维促进、形成性评估、个性化学习支持、团队协作等多个方面^[7-9]。

ChatGPT 在教育领域的应用正在推动智能决策的新前沿，为个性化学习、教学评估和教师培训等方面提供了创新性解决方案。

在个性化学习方面，大语言模型能够通过分析学生的学习行为和表现，为每个学生制定最优的学习路径。研究^[10]表明，基于 ChatGPT 的翻转学习指导方法（ChatGPT-FLGA）显著提高了学生的课件项目表现、自我效能感、学习态度、内在动机和创造性思维。这种方法不仅提供了即时的个性化指导，还优化了翻转课堂的教学效果。

在教学评估和反馈方面，文献 [11] 指出，ChatGPT 能够生成比人类教师更详细、

流畅和连贯的反馈，在评估学生作业主题时与教师达成高度一致，并能就学生完成任务的过程提供有益于学习技能发展的反馈。

此外，大语言模型在教师培训中也发挥着重要作用。文献 [12] 表明，在 STEM（Science, Technology, Engineering, Mathematics）教师培训课程中，基于 ChatGPT 的协作学习显著提高了师范生的学习表现，并降低了认知负荷。

尽管 ChatGPT 在教育中展现出巨大潜力，但其技术限制和准确性问题仍然存在。文献 [13] 指出，ChatGPT 生成的内容存在假阳性和假阴性检测的问题，这可能导致信息的不准确性。在伦理和学术诚信方面，ChatGPT 的应用引发了广泛争议。文献 [14] 使用间接问询技术研究越南本科生的学术作弊行为，发现使用 AI 辅助作弊的实际比例（23%）远高于直接询问的结果（8%），揭示了 ChatGPT 可能带来的学术诚信风险。研究 [15] 对 142 份高等教育机构的学术诚信政策进行分析，发现只有 23% 的政策明确提及人工智能或相关技术，凸显了教育政策在应对 AI 带来的挑战方面的滞后。

2 研究数据与方法

本研究采用系统文献综述方法，通过 Web of Science 数据库进行文献检索和分析，选择 Web of Science 核心合集作为文献来源。以“chatgpt”为检索词，在“Topic”字段中进行检索，并将范围限定在“Education Educational Research”类别。以探讨 ChatGPT 在教育教学领域的应用现状及研究趋势。通过上述检索策略，共获得 300 篇文献。检索时间截至 2024 年 6 月 30 日。排除修订类（1 篇）和书信类（1 篇），共获得 298 篇相关文献。

3 描述性统计分析

本研究采用了 Web of Science 的分类方法，将论文类型划分为期刊论文、Early Access、会议论文、编辑评论、综述性文章五类；所有检索的论文中，发文量前十的子领域是：教育科学学科、计算机科学跨学科应用、语言学、计算机科学理论与方法、商业、管理、语言与语言学、计算机科学软件工程、科学史与哲学、教育心

理学。需要指出的是，有的论文同时属于多个类别，如图 1、表 1 所示。

表 1 描述性统计分析

论文类型	数量	占比
期刊论文	227	76.17%
Early Access	100	33.56%
会议论文	48	16.11%
编辑评论	13	4.36%
综述性文章	10	3.36%
合计	298	

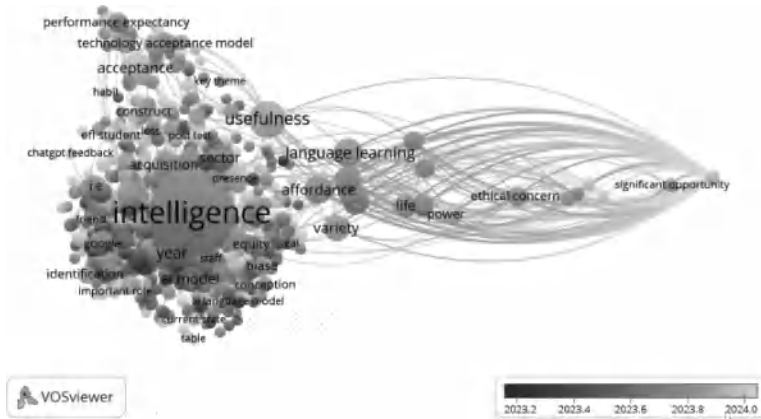


图 1 关键词共线图

通过对 298 篇文献的标题、关键词、摘要进行聚类分析，在 vosviewer 中得到 14 个聚类。ChatGPT 在教育领域的研究呈现出快速发展、深化和拓展的特点。从时间维度来看，研究焦点从初期的技术接受转向对教育本质和长期影响的探讨。从地域空间来看，研究已经形成了全球化的视野，特别是在亚洲国家的研究显著增加。研究主题也从单一的使用意图拓展到了包括教育评估、教师角色、学生伦理观等多个方面。

4 ChatGPT 在五大研究领域的教育教学应用

Web of Science 的主题领域分类体系在

2024 年包括五个大的学科类别：艺术与人文、生命科学与生物医药、理学、社会科学、技术，下文将分别分析 ChatGPT 在五大研究领域的教育教学应用。

4.1 ChatGPT 在艺术与人文教育的应用

写作教育是 ChatGPT 应用最广泛的艺术与人文领域之一。文献 [16] 提到，他们开发的 AI 驱动教学助理系统旨在引导学生找到解决方案，而不是直接提供解决方案。学生对此反应积极，表示感觉像有一位私人导师。这表明，ChatGPT 的引导方式，特别是启发式引导而非直接给答案，

是影响其教学效果的一个关键因素。文献 [17] 探讨了将规格评分法 (Specifications Grading) 与 AI 写作工具结合的创新方法。

这种方法旨在促进学生参与和批判性思考,可能有助于学生更深入地参与写作过程,但需要进一步研究数据验证,如表 2 所示。

表 2 ChatGPT 在艺术与人文教育的应用

应用场景	创新方法	实现方式	效果
多模态写作	GenAI 辅助多模态作文	文献 [16] 研究了 ChatGPT 和 Bing Image Creator 在 EFL 学生多模态 Power-Point 项目中的应用	帮助学生构建更多桥接文本和例子,改善多模态写作能力
技术教育	技术教育冰山模型	文献 [18] 提出了一个框架,帮助教育者规划和反思如何教授技术相关内容	促进学生对技术的批判性思考,但未直接测试效果
音乐教育	AI 增强音乐教育	文献 [19] 研究了 ChatGPT-4 在音乐教育中的应用,通过个性化教学材料来匹配学生的学习目标和音乐偏好	实验组在音乐知识获取方面表现更好,学生倾向于将其作为提高音乐学习能力的工具
道德教育	使用 LLMs 模拟道德推理过程	文献 [20] 使用 ChatGPT 进行道德困境实验和道德榜样测试	LLMs 能够解决道德困境并体验道德提升

文献 [21] 开发的基于 ChatGPT 的教学聊天机器人,通过情境化的对话设计和及时反馈,有效提高了学生的参与度和学习效果。文献 [22] 的 EvalMate 系统则通过详细的反馈报告设计,帮助学生更好地认识自己的写作优缺点。这些研究表明,针对具体教学需求的人机交互设计,是发挥 ChatGPT 教学效能的关键。

在音乐教育领域,ChatGPT 被用于优化远程教学和个性化学习体验^[23]。文献 [19] 探讨了如何借助 ChatGPT-4 生成个性化教学材料,匹配学生的学习目标和音

乐偏好。结果显示,使用 ChatGPT-4 的实验组在音乐知识获取方面表现更好。尽管研究没有提供具体的量化改善程度,但强调学生倾向于将 ChatGPT-4 作为提高音乐学习能力的工具。这一发现表明,AI 技术可以有效地增强音乐教育的个性化程度,提高学习效果。

在道德哲学教育方面,文献 [20] 使用 ChatGPT 进行道德困境实验和道德榜样测试,发现 LLMs 能够基于推理解决道德困境,并根据外部输入修改其推理过程,如表 3 所示。

表 3 ChatGPT 在生命科学与生物医药教育的应用

应用场景	创新方法	实现方式	效果
医院临床教师专业发展	ChatGPT 基础培训模式 (ChatGPT-TM)	文献 [24] 提出了基于 ChatGPT 的培训模式,用于案例教学培训	显著提高了临床教师的案例教学学习成就、自我价值感和自信心
公共卫生教育	基于 ChatGPT 的情景写作	文献 [25] 提出了三步提示工程过程 (WCV) 用于情景式学习的情景创作,可应用于公共卫生教育	能够在短时间内高效创建高质量的情景式学习场景,提高学生的内在动机和学习表现

续表

应用场景	创新方法	实现方式	效果
药学教育	自我调节学习促进	文献 [6] 开发的 SRLbot 可以应用于药学教育, 促进学生的自我调节学习	显著提高了学生的科学知识、行为参与度和学习动机
医学课程设计	设计思维+生成式 AI 的教育框架	文献 [26] 提出新框架, 包括讲座、工作坊和项目辅导	创建了以学生为中心的学习体验, 增强了医学教育
儿科临床技能培训	AI 辅助教学	文献 [27] 比较了 ChatGPT 辅助教学与传统教学方法在培养儿科实习生临床技能方面的效果	使用 ChatGPT 的群组在迷你临床评估练习 (Mini-CEX) 分数上显著提高, 特别是在患者沟通和临床判断方面
解剖学教学	AI 辅助教学	文献 [28] 研究了 ChatGPT 在解剖学教学中的应用	提高了学生的参与度和自主学习能力
医学药理学自学	AI 作为交互式学习平台	文献 [29] 使用 ChatGPT 作为学生提问多选题并获得答案和解释的交互式平台	在回答医学药理学多选题时的总体准确率为 76.0%

4.2 ChatGPT 在生命科学与生物医药教育的应用

ChatGPT 在生命科学与生物医药教育中的应用涵盖了多个子领域, 包括医学教育、公共卫生、药学和营养学等, 为传统教学方法带来了诸多变化。

在公共卫生教育领域, ChatGPT 在情景式学习中的应用显示出了创新性。文献 [24] 提出了三步提示工程过程 (WCV) 用于情景式学习的情景创作, 研究表明, 这种方法能够在短时间内高效创建高质量的情景式学习场景, 提高学生的内在动机和学习表现。

在儿科临床技能培训方面, 文献 [27] 比较了 ChatGPT 辅助教学与传统教学方法的效果。结果显示, 使用 ChatGPT 的群组在迷你临床评估练习 (Mini-CEX) 分数上显著提高, 特别是在患者沟通和临床判断方面 ($p < 0.05$)。

在护理教育方面, 文献 [30] 将

ChatGPT 系统整合到护理和健康教育设计课程中。研究采用准实验设计, 招募了两个班级的护理本科生进行对比实验。结果表明, 使用 ChatGPT 系统的实验组在批判性思维能力、问题解决能力和学习兴趣方面都有显著提高。

在药学教育方面, ChatGPT 在促进自我调节学习方面展现出了潜力。文献 [31] 发现, SRLbot 显著提高了学生的科学知识、行为参与度和学习动机。在为期 3 周的实验中, 74 名中学生使用 SRLbot 进行学习, 结果显示实验组在科学知识、行为参与度和动机方面都显著优于对照组。这一发现为药学教育中的自我调节学习提供了新的工具和方法。

4.3 ChatGPT 在理学教育的应用

ChatGPT 在理学教育教学中的应用主要集中在物理、化学和数学等核心学科, 具体案例如表 4 所示, 这些实证与理论研究为传统教学方法带来了新的可能性和挑战。

表 4 ChatGPT 在理学教育的应用

应用场景	创新方法	实现方式	效果
物理课程 辅助教学	ChatGPT 作为虚拟导师	文献 [32] 等 (2023) 研究了在物理课程中使用 ChatGPT 作为助手工具来解答物理问题	尽管 ChatGPT 在回答问题时存在一些不准确性, 但大多数学生信任其提供正确答案的能力
化学基础 课程	基于指导的 ChatGPT 辅助学习 (GCLA)	文献 [33] 在台湾大学的化学基础课程中应用 GCLA 方法	GCLA 显著提高了学生的自我调节学习、高阶思维技能和知识构建能力
数学问题 解决	利用大型语言模型解决数学难题	Nature 研究表明生成式大型语言模型可以破解经典数学难题 ^[34]	不仅能给出答案, 而且还能给出超越传统方案的解题步骤
解决运动学 图表问题	使用多模态 AI 模型解决视觉问题	文献 [35] 比较了 GPT-4V 和 Bard 在解决视觉 Parsons 问题上的表现	GPT-4V 在解决 Parsons 问题上表现出色 (96.7% 成功率)
微积分学习	AI 辅助论证过程	文献 [36] 使学生与 ChatGPT 在微积分学习中交互	协助完成微积分论证

在物理学、化学等领域, ChatGPT 被广泛应用于解决复杂问题、理解物理概念和模拟考试评估。文献 [35] 发现, GPT-4V 能够解决 96.7% 的视觉 Parsons 问题, 远超传统语言模型 Bard 的 69.2%。这一惊人的结果表明, 多模态 AI 模型在处理物理学中的视觉问题方面具有显著优势, 为物理教育中的问题解决和可视化学学习开辟了新的可能性。Lee 等 (2024) 在台湾大学的化学基础课程中应用了基于指导的 ChatGPT 辅助学习 (GCLA) 方法。研究结果显示, GCLA 显著提高了学生的自我调节学习、高阶思维技能和知识构建能力^[33]。

在数学教育方面, Nature 研究表明生成式大型语言模型 (如 ChatGPT) 可以破解经典数学难题^[34]。更令人惊讶的是, 这些模型不仅能给出答案, 还能提供超越传统方案的解题步骤^[34]。在微积分学习中, 文献 [36] 研究了学生与 ChatGPT 在微积分学习中的交互, 特别是在探讨无法对函数图像绘制切线的情况时。研究使用 Toulmin 模型和 Habermas 的理性构念分析了大学生与 ChatGPT 之间的论证过程。结果表明, ChatGPT 在连续性、导数和切线

概念定义的认识论理性背景下为学生的推理提供了合理支持。

然而, 这些研究也揭示了一些局限性和挑战。例如, ChatGPT 在处理需要深入视觉理解的任务时可能存在困难, 且可能复制学生常见的错误观念。此外, 在数学推理的某些方面, ChatGPT 的回应可能存在问题, 需要人类专家的监督和干预。

4.4 ChatGPT 在社会科学教育的应用

ChatGPT 在社会科学教育教学中的应用涵盖了教育研究、心理学、商业教育、法律和社会工作等多个领域, 如表 5 所示。

教育研究中, 文献 [12] 研究了 ChatGPT 支持的协作学习在 STEM 教师培训中的应用。研究采用准实验设计, 对 36 名大二本科师范生进行了为期 8 周的研究。结果显示, 使用 ChatGPT 的师范生在学习表现和认知负荷方面表现优异。文献 [9] 探讨了 ChatGPT 在虚拟团队学习中的应用, 被试对象为 344 名研究生。研究发现, AI 的可解释性显著提高了知识更新感知, 而 AI 自主性的积极效果取决于

表 5 ChatGPT 在社会科学教育的应用

应用场景	创新方法	实现方式	效果
高等教育课程评估	ChatGPT 辅助分析学生评价	文献 [37] 使用 ChatGPT 分析学生的开放式课程评价意见	ChatGPT 在分析课程评价意见时比教师更快，且结果具有高度一致性
虚拟团队学习	AI 辅助知识获取	文献 [9] 研究 ChatGPT 在虚拟团队学习中的应用	AI 的可解释性显著提高了知识更新感知，AI 自主性的效果取决于团队感知虚拟性
教师专业发展	ChatGPT 辅助课程设计	文献 [38] 使用 ChatGPT 设计职前科学教师课程计划	ChatGPT 在开发可实施的课程计划、提供适应性信息和节省时间方面表现出色
STEM 教师培训	AI 辅助协作学习	文献 [12] 研究了 ChatGPT 支持的协作学习在 STEM 教师培训中的应用	使用 ChatGPT 的师范生在学习表现和认知负荷方面表现优异
创业教育	AI 辅助创意生成和商业规划	文献 [39] 研究学生使用 ChatGPT 进行创意风暴、构建商业模式、撰写商业计划等	简化创业教育过程，提高学生效率，支持某些类型的创造力
多语言编程教育	AI 生成多语言编程练习	文献 [40] 使用 OpenAI GPT-3.5 以多种语言生成编程问题、样本解决方案和测试用例	英语、西班牙语和越南语生成的问题大多合理且易于理解
旅游教育	AI 辅助实验性学习	文献 [41] 让学生使用 ChatGPT 进行实验性学习，然后通过在线调查反馈学习体验	ChatGPT 对学习成果有积极影响，数字素养起中介作用

团队感知虚拟性 (TPV)。这一发现为理解 AI 如何影响团队动态和学习过程提供了重要见解。

在心理学教育领域，ChatGPT 被用于培养批判性思维能力。文献 [42] 研究了 ChatGPT 对英国商学院研究生批判性思维技能的影响。研究采用混合方法，涉及 107 名参与者。结果显示，在 Bloom 分类法的低层次上，学生的批判性思维技能有最显著的改善。

在商业与经济学教育中，ChatGPT 被用于增强创业教育和经济学评估。文献 [39] 研究了学生使用 ChatGPT 进行创意风暴、构建商业模式和撰写商业计划的过程。研究结果表明，ChatGPT 能够简化创业教育

过程，提高学生效率，并支持某些类型的创造力。文献 [43] 探讨了技术整合如何通过影响学生动机来提高学业表现。研究发现，技术整合通过影响学生的学习欲望、自我效能感和未来信念，最终提高了学业表现。

ChatGPT 在社会科学教育中展现出了巨大的潜力，但在某些社会科学子领域（如人类学、考古学等）的应用研究仍然相对缺乏。

4.5 ChatGPT 在技术教育的应用

ChatGPT 在技术教育教学中的应用主要集中在计算机科学、信息科学、工程教育等领域，如表 6 所示。

表 6 ChatGPT 在技术教育的应用

应用场景	创新方法	实现方式	效果
工程教育	生成式 AI 辅助教学设计	文献 [44] 开发了基于自我决定理论的分类工具, 指导教师设计利用 ChatGPT 的学习活动	工具可以帮助教师修改活动以满足学生需求, 促进自我调节学习
人机协作知识构建	提示工程促进论证对话	文献 [45] 探讨了如何利用 GenAI 工具进行个人学习和集体知识构建	适当的提示可以促进人类与 AI 工具之间的论证对话, 实现共同知识构建
编程课程辅助教学	AI 辅助编程反馈生成	文献 [46] 开发了 GPT4Hints - GPT3.5Val 技术, 使用 GPT-4 生成编程提示, GPT-3.5 验证提示质量	提高了编程提示的质量和个性化程度
计算思维培养	AI 辅助脚手架系统	文献 [47] 提出了一个基于 ChatGPT 的智能编程脚手架系统	大多数学生对系统持积极态度, 系统在总体上有效提高了学生的计算思维能力
软件工程教育	AI 知识助手增强上下文感知学习体验	文献 [48] 使用 AI 驱动的 Kanban 项目跟踪分析学生报告, 用 GPT-3.5 和 GPT-4 API 提供改进建议	显著提高了学生对推荐内容的理解容易度、相关性、新颖性和意外性

在计算机科学和编程教育中, ChatGPT 被广泛应用于提供个性化学习支持和自动化反馈。文献 [46] 开发了创新的 GPT4Hints - GPT3.5Val 技术, 利用 GPT-4 生成编程提示, 并使用 GPT-3.5 验证提示质量。结果显示, 该方法在生成高质量编程提示方面表现出色, 特别是在利用失败测试用例的符号信息和修复来提高生成质量方面。这种方法提高了编程提示的质量和个性化程度, 有效模拟了人类导师的反馈风格。

在软件工程教育中, ChatGPT 被用于改善项目管理技能和协作能力。文献 [48] 研究了使用生成式 AI 来产生 StandUp 报告建议, 帮助学生提高报告的质量和有效性。研究涉及 179 名学生参与 16 个真实世界的软件开发项目, 为期一学期。结果显示, AI 辅助的推荐系统帮助学生在整个学期内显著提高了 StandUp 报告的整体质量。

在人机协作知识构建方面, ChatGPT

也显示出了潜力。文献 [45] 探讨了如何利用生成式 AI 工具进行个人学习和集体知识构建。研究指出, 通过设计适当的提示, 可以促进人类与 AI 工具之间的论证对话, 实现共同知识构建。

然而, 在提高高阶问题解决技能方面, ChatGPT 的效果可能不如预期。此外, 如何在利用 AI 优势的同时确保学生独立思考和实践能力的发 展, 仍是一个需要深入研究的问题。

5 结束语

5.1 ChatGPT 在教育中的跨学科应用: 模式差异与共性

尽管 ChatGPT 在各学科教育中的应用均呈现出积极效果, 但其具体应用模式存在差异, 这些差异源于各学科的独特特性和教学需求。在艺术与人文领域, ChatGPT 主要用于激发创意思维和培养批

判性思考能力，如多模态写作和音乐教育中的应用^[13,15]。该领域强调主观表达和文化理解，ChatGPT 在此主要发挥创意激发和文化阐释的功能。相较而言，在生命科学与生物医药教育中，ChatGPT 的应用更侧重于案例分析和诊断推理，如在医学教育和公共卫生教学中的运用^{[21][23]}。该领域对信息准确性和伦理考量的要求极为严格，ChatGPT 在此充当知识库和决策支持系统的角色。理学教育中，ChatGPT 的应用模式主要围绕问题建模和数学推导展开，如在物理和化学课程中的实践^[31-32]。该领域强调抽象概念的理解和复杂问题的解决，ChatGPT 在此扮演虚拟导师和问题解析器的角色。社会科学教育则更多地利用 ChatGPT 进行定性分析和理论构建，如在高等教育评估和虚拟团队学习中的应用^[6,37]。该领域需要处理大量文本数据和复杂的社会现象，ChatGPT 在此发挥数据分析和模式识别的功能。在技术教育领域，ChatGPT 的应用模式主要体现在实践导向和项目学习上，如编程教育和软件工程教学中的运用^[47,49]。该领域需要即时反馈和个性化指导，ChatGPT 在此担任编程辅助和项目管理工具的角色。

尽管存在上述差异，各学科应用 ChatGPT 也呈现出若干共性，如提供个性化学习体验、促进自主学习、增强学习动机等。这些共性反映了 ChatGPT 作为教育工具的普适价值，同时也凸显了在不同学科背景下开发专门的人工智能辅助教学模型的必要性。深入理解这些模式差异和共性，对于有效将 ChatGPT 整合到各学科的教学实践中具有重要意义。未来研究应进一步探讨如何基于学科特性优化 ChatGPT 的应用策略，以最大化其在教育领域的价值。

5.2 ChatGPT 教育应用研究的贡献

ChatGPT 影响教学效果的因素是多元的。学生的技术接受度和数字素养水平、教师的 AI 素养和使用能力、AI 辅助的游戏化学习都是关键影响因素。学科特性也影响 ChatGPT 的应用效果：在需要高度创造性和批判性思维的领域，ChatGPT 的效果可能不如在知识传授和基础技能培养方面显著。这一发现强调了在实施 AI 辅助教学时需要采取全面和个性化的策略。

ChatGPT 在不同学科领域的教育教学中表现出明显的差异性，反映了各学科特点和教学需求的多样性。在具体应用效果上，ChatGPT 在提高学习效率、增强学习动机和培养某些高阶思维技能方面展现出潜力。特别是在低阶认知任务和结构化学习任务中，ChatGPT 的表现尤为出色。然而，在涉及高度创造性和复杂批判性思维的领域，其效果则相对有限，这一发现为 AI 辅助教学的边界提供了重要参考。

总之，ChatGPT 在教育领域的应用研究需要进一步拓展和深化。探索更多学科领域的应用可能性、深入研究对学生长期学习效果的影响、开发更有效的人机协作模式，以及研究如何将 ChatGPT 更好地整合到现有教育体系中，将是推动教育创新和提升教育质量的关键。这不仅需要持续的技术创新，更需要教育理论的深化和跨学科的紧密合作。

参考文献

- 1 宋萑, 林敏. ChatGPT/生成式人工智能时代下教师的工作变革: 机遇、挑战与应对 [J]. 华东师范大学学报(教育科学版), 2023,

- 7 (41): 78 - 90. DOI: 10. 16382/j. cnki. 1000-5560. 2023. 07. 008.
- 2 李育辉, 庞菊爱, 谭北平. 人工智能与人类的创造力比较研究: 基于专家和消费者的双重视角 [J]. 商业经济与管理, 2023 (10): 23-35. DOI: 10. 14134/j. cnki. cn33 - 1336/f. 2023. 10. 002.
- 3 袁玉芝, 杜育红. 人工智能对技能需求的影响及其对教育供给的启示: 基于程序性假设的实证研究 [J]. 教育研究, 2019, 2 (40): 113-123.
- 4 COWLING M, CRAWFORD J, ALLEN K, et al. Using leadership to leverage ChatGPT and artificial intelligence for undergraduate and postgraduate research supervision [J]. Australasian Journal of Educational Technology, 2023, 39 (4): 89 - 103. DOI: 10. 14742/ajet. 8598.
- 5 JHO H, HA M. Towards Effective Argumentation; Design and Implementation of a Generative AI-Based Evaluation and Feedback System [J]. Journal of Baltic Science Education, 2024, 23 (2): 280 - 291. DOI: 10. 33225/jbse/24. 23. 280.
- 6 NG D, TAN C, LEUNG J. Empowering student self - regulated learning and science education through ChatGPT: A pioneering pilot study [J]. British Journal of Educational Technology, 2024. DOI: 10. 1111/bjet. 13454.
- 7 HUI E. Incorporating Bloom's taxonomy into promoting cognitive thinking mechanism in artificial intelligence-supported learning environments [J]. Interactive Learning Environments, 2024. DOI: 10. 1080/10494820. 2024. 2364237.
- 8 YILDIRIM - ERBASLI S, BULUT O. Innovating Assessment with Conversational Agents: A Technology-Enhanced Approach to Formative Assessments [C] //CHANG M, CHEN N, KUO R, et al. University of Alberta. 2023: 331 - 335. DOI: 10. 1109/ICALT58122. 2023. 00103.
- 9 DARBAN M. Navigating virtual teams in generative AI-led learning: The moderation of team perceived virtuality [J]. Education and Information Technologies, 2024. DOI: 10. 1007/s10639 - 024 - 12681-4.
- 10 LI H. Effects of a ChatGPT-based flipped learning guiding approach on learners' courseware project performances and perceptions [J]. Australasian Journal of Educational Technology, 2023, 39 (5): 40-58. DOI: 10. 14742/ajet. 8923.
- 11 DAI W, LIN J, JIN H, et al. Can Large Language Models Provide Feedback to Students? A Case Study on ChatGPT [C] //CHANG M, CHEN N, KUO R, et al. Monash University. 2023: 323 - 325. DOI: 10. 1109/ICALT58122. 2023. 00100.
- 12 JI Y, ZOU X, LI T, et al. The Effectiveness of ChatGPT on Preservice Teachers' STEM Teaching Literacy, Learning Performance and Cognitive Load in STEM Teacher Training Courses [C] // South China Normal University. 2023: 16-22. DOI: 10. 1145/3637907. 3637948.
- 13 DALALAH D, DALALAH O. The false positives and false negatives of generative AI detection tools in education and academic research: The case of ChatGPT [J]. International Journal of Management Education, 2023, 21 (2). DOI: 10. 1016/j. ijme. 2023. 100822.
- 14 NGUYEN H, GOTO D. Unmasking academic cheating behavior in the artificial intelligence era: Evidence from Vietnamese undergraduates [J]. Education and Information Technologies, 2024. DOI: 10. 1007/s10639-024-12495-4.
- 15 PERKINS M, ROE J. Decoding Academic Integrity Policies: A Corpus Linguistics Investigation of AI and Other Technological Threats [J]. Higher Education Policy, 2023. DOI: 10. 1057/s41307-023-00323-2.
- 16 LIU M, M'HIRI F, ASSOC C M. Beyond Traditional Teaching: Large Language Models as Simulated Teaching Assistants in Computer Science [C] //McGill University. 2024: 743-749. DOI: 10. 1145/3626252. 3630789.
- 17 GRAVES B. Specifications grading to promote student engagement, motivation and learning: Possibilities and cautions [J]. Assessing Writing, 2023, 57. DOI: 10. 1016/j. asw. 2023. 100754.
- 18 KRUTKA D, PLEASANTS J, NICHOLS T. Talking the technology talk [J]. Phi Delta Kappan, 2023, 104 (7): 42 - 46. DOI: 10.

- 1177/00317217231168262.
- 19 ZHOU W, KIM Y. Innovative music education: An empirical assessment of ChatGPT-4's impact on student learning experiences [J]. *Education and Information Technologies*, 2024. DOI: 10.1007/s10639-024-12705-z.
- 20 HAN H. Potential benefits of employing large language models in research in moral education and development [J]. *Journal of Moral Education*, 2023. DOI: 10.1080/03057240.2023.2250570.
- 21 FARAH J, INGRAM S, SPAENLEHAUER B, et al. Prompting Large Language Models to Power Educational Chatbots [C] //XIE H, LAI C, CHEN W, et al. *Swiss Federal Institutes of Technology Domain*: 14409. 2023: 169-188. DOI: 10.1007/978-981-99-8385-8_14.
- 22 GUO K. EvaluMate: Using AI to support students' feedback provision in peer assessment for writing [J]. *Assessing Writing*, 2024, 61. DOI: 10.1016/j.asw.2024.100864.
- 23 JIANG H, CHEONG K. Developing teaching strategies for rural school pupils' concentration in the distance music classroom [J]. *Education and Information Technologies*, 2024, 29 (5): 5903-5920. DOI: 10.1007/s10639-023-12056-1.
- 24 CHANG C, HWANG G. ChatGPT-facilitated professional development: evidence from professional trainers' learning achievements, self-worth, and self-confidence [J]. *Interactive Learning Environments*, 2024. DOI: 10.1080/10494820.2024.2362798.
- 25 BAI S, GONDA D, HEW K. Write-Curate-Verify: A Case Study of Leveraging Generative AI for Scenario Writing in Scenario-Based Learning [J]. *IEEE Transactions on Learning Technologies*, 2024, 17: 1313-1324. DOI: 10.1109/TLT.2024.3378306.
- 26 HOUSSAINI M, ABOUTAJEDDINE A, TOUGHRAI I, et al. Development of a design course for medical curriculum: Using design thinking as an instructional design method empowered by constructive alignment and generative AI [J]. *Thinking Skills and Creativity*, 2024, 52. DOI: 10.1016/j.tsc.2024.101491.
- 27 BA H, ZHANG L, YI Z. Enhancing clinical skills in pediatric trainees: a comparative study of ChatGPT-assisted and traditional teaching methods [J]. *BMC Medical Education*, 2024, 24 (1). DOI: 10.1186/s12909-024-05565-1.
- 28 LENG L. Challenge, integration, and change: ChatGPT and future anatomical education [J]. *Medical Education Online*, 2024, 29 (1). DOI: 10.1080/10872981.2024.2304973.
- 29 CHOI W. Assessment of the capacity of ChatGPT as a self-learning tool in medical pharmacology: a study using MCQs [J]. *BMC Medical Education*, 2023, 23 (1). DOI: 10.1186/s12909-023-04832-x.
- 30 CHANG C, YANG C, JEN H, et al. Facilitating nursing and health nursing and health education education by incorporating ChatGPT into learning designs [J]. *Educational Technology & Society*, 2024, 27 (1): 215-230. DOI: 10.30191/ETS.202401_27 (1). TP02.
- 31 NG D, TAN C, LEUNG J. Empowering student self-regulated learning and science education through ChatGPT: A pioneering pilot study [J]. *British Journal of Educational Technology*, 2024. DOI: 10.1111/bjet.13454.
- 32 DING L, LI T, JIANG S, et al. Students' perceptions of using ChatGPT in a physics class as a virtual tutor [J]. *International Journal of Educational Technology in Higher Education*, 2023, 20 (1). DOI: 10.1186/s41239-023-00434-1.
- 33 LEE H, CHEN P, WANG W, et al. Empowering ChatGPT with guidance mechanism in blended learning: effect of self-regulated learning, higher-order thinking skills, and knowledge construction [J]. *International Journal of Educational Technology in Higher Education*, 2024, 21 (1). DOI: 10.1186/s41239-024-00447-4.
- 34 Mathematical discoveries from program search with large language models | *Nature* [EB/OL]. [2024-07-16]. <https://www.nature.com/articles/s41586-023-06924-6>.
- 35 HOU I, MAN O, METTILLE S, et al. More Ro-

- bots are Coming: Large Multimodal Models (ChatGPT) can Solve Visually Diverse Images of Parsons Problems [C] //Pennsylvania Commonwealth System of Higher Education (PCSHE). 2024; 29–38. DOI: 10. 1145/3636243. 3636247.
- 36 URHAN S, GENÇASLAN O, DOST S. An argumentation experience regarding concepts of calculus with ChatGPT [J]. *Interactive Learning Environments*, 2024. DOI: 10. 1080/10494820. 2024. 2308093.
- 37 FULLER K, MORBITZER K, ZEEMAN J, et al. Exploring the use of ChatGPT to analyze student course evaluation comments [J]. *BMC Medical Education*, 2024, 24 (1). DOI: 10. 1186/s12909-024-05316-2.
- 38 OKULU H, MUSLU N. Designing a course for pre-service science teachers using ChatGPT: what ChatGPT brings to the table [J]. *Interactive Learning Environments*, 2024. DOI: 10. 1080/10494820. 2024. 2322462.
- 39 VECCHIARINI M, SOMIÀ T. Redefining entrepreneurship education in the age of artificial intelligence: An explorative analysis [J]. *International Journal of Management Education*, 2023, 21 (3). DOI: 10. 1016/j. ijme. 2023. 100879.
- 40 JORDAN M, LY K, RAJ A, et al. Need a Programming Exercise Generated in Your Native Language? ChatGPT's Got Your Back: Automatic Generation of Non-English Programming Exercises Using OpenAI GPT-3.5 [C] //North Carolina State University. 2024; 618 – 624. DOI: 10. 1145/3626252. 3630897.
- 41 DALGIC A, YASAR E, DEMIR M. ChatGPT and learning outcomes in tourism education: The role of digital literacy and individualized learning [J]. *Journal of Hospitality Leisure Sport & Tourism Education*, 2024, 34. DOI: 10. 1016/j. jhlste. 2024. 100481.
- 42 ESSIEN A, BUKOYE O, O' DEA C, et al. The influence of AI text generators on critical thinking skills in UK business schools [J]. *Studies in Higher Education*, 2024, 49 (5): 865 – 882. DOI: 10. 1080/03075079. 2024. 2316881.
- 43 GAO L, LÓPEZ-PÉREZ M, MELERO-POLO I, et al. Ask ChatGPT first! Transforming learning experiences in the age of artificial intelligence [J]. *Studies in Higher Education*, 2024. DOI: 10. 1080/03075079. 2024. 2323571.
- 44 CHIU T. A classification tool to foster self-regulated learning with generative artificial intelligence by applying self-determination theory: a case of ChatGPT [J]. *ETR&D-Educational Technology Research and Development*, 2024. DOI: 10. 1007/s11423 – 024 – 10366-w.
- 45 CRESS U, KIMMERLE J. Co-constructing knowledge with generative AI tools: Reflections from a CSCL perspective [J]. *International Journal of Computer-Supported Collaborative Learning*, 2023, 18 (4): 607–614. DOI: 10. 1007/s11412 – 023 – 09409-w.
- 46 PHUNG T, PADUREAN V, SINGH A, et al. Automating Human Tutor – Style Programming Feedback: Leveraging GPT-4 Tutor Model for Hint Generation and GPT-3.5 Student Model for Hint Validation [C] //University of Michigan System. 2024; 12 – 23. DOI: 10. 1145/3636555. 3636846.
- 47 LIAO J, ZHONG L, ZHE L, et al. Scaffolding Computational Thinking With ChatGPT [J]. *IEEE Transactions on Learning Technologies*, 2024, 17: 1668 – 1682. DOI: 10. 1109/TLT. 2024. 3392896.
- 48 NEYEM A, GONZÁLEZ L, MENDOZA M, et al. Toward an AI Knowledge Assistant for Context-Aware Learning Experiences in Software Capstone Project Development [J]. *Ieee Transactions on Learning Technologies*, 2024, 17: 1639 – 1654. DOI: 10. 1109/TLT. 2024. 3396735.
- 49 ANASTASOPOULOS I, SHEEL S, PARDOS Z, et al. Introducing an Open – source Adaptive Tutoring System to Accelerate Learning Sciences Experimentation [C] //ACM. University of California System. 2023; 251–253. DOI: 10. 1145/3573051. 3593399.

SWARM-LLM：基于大语言模型的无人集群任务规划系统

李婷婷¹ 王琪^{1,2*} 王嘉康^{1,2} 徐勇军^{1,2*}

目的：文章旨在解决无人集群系统中存在的自主智能性不足、异构无人集群协同效率低、任务分配不均衡等问题。针对无人集群自主规划、高效协作、智能决策的需求，提出了一种基于大语言模型的无人集群任务规划系统框架（SWARM-LLM），以提升多无人系统的任务规划能力。

方法：SWARM-LLM 框架利用大语言模型将高层次的任务指令转化为具体的智能无人集群任务规划方案，通过任务分解、任务分配、任务执行等多个阶段来实现无人集群协同任务。在任务分解阶段，SWARM-LLM 利用大语言模型对任务需求和无人机能力进行深入分析，将复杂任务细化为多个可执行的子任务，为后续的任务分配和执行打下坚实基础。任务分配阶段，SWARM-LLM 根据子任务的执行要求和无人机的技能特性，进行合理的任务分配，确保每项任务都能由最适合的无人机执行，从而优化资源配置，提高协同效率。任务执行阶段，无人机依据大语言模型生成的任务分配计划，执行具体任务，并通过 API（不同接口）调用与环境进行交互，完成既定目标。进一步地，文章设计了一套适用于无人集群规划的提示工程方法，用来指导和优化上述各阶段的实施。最终，在无人集群仿真环境（AirSim）中构建了元任务、简单任务、复杂任务和异构任务，覆盖不同复杂性的任务场景，并进行了评估实验。

结果：实验结果表明，在不同任务规划模型的性能比较中，SWARM-LLM 系列模型（包括 GPT-3.5-Turbo、GPT-4、GPT-4o 和 Claude3）在无人集群任务规划中的表现均优于传统优化算法和机器学习方法，尤其是任务成功率上展现出显著优势，平均性能提升了 47.8%。消融实验进一步分析了不同提示方法对任务规划性能的影响，结果表明无人集群规划的提示工程方法在复杂任务和异构任务中的任务成功率得到了显著提升。此外，实验还通过可视化手段展示了无人机任务规划和执行的全流程，包括任务分配、协调和执行任务的场景，为无人集群任务规划提供了直观的参考。

结论：SWARM-LLM 框架有效地提升了无人集群任务规划的效率和成功率，验证了大语言模型在解决无人集群任务规划问题中的潜力。该框架不仅在实验中表现出色，还为未来无人集群任务规划技术的发展提供了新的方向。后续工作将继续探索 SWARM-LLM 实现无人机之间实时动态任务规划的可能性，并研究多智能体 LLM 框架（多智能体大模型框架），以进一步提升无人集群在复杂、动态环境中的适应性和决策能力，推动无人集群任务规划技术的发展。

关键词 任务规划，无人集群，大语言模型，协同策略

* 通讯作者

1. 中国科学院计算技术研究所 2. 中国科学院大学

1. Institute of Computing Technology, Chinese Academy of Sciences 2. University of Chinese Academy of Sciences

SWARM-LLM: A Swarm Task Planning System Based on Large Language Models

LI Ting-Ting¹ WANG Qi^{1,2*} WANG Jia-Kang^{1,2} XU Yong-Jun^{1,2*}

Objective: This paper aims to address issues such as insufficient autonomous intelligence, low coordination efficiency in heterogeneous unmanned swarms, and unbalanced task allocation in unmanned swarm systems. In response to the needs for autonomous planning, efficient collaboration, and intelligent decision-making in unmanned swarms, a framework for an unmanned swarm task planning system based on large language models (SWARM-LLM) is proposed to enhance the task planning capabilities of multi-unmanned systems.

Method: The SWARM-LLM framework utilizes large language models to transform high-level task instructions into specific intelligent unmanned swarm task planning schemes. It achieves collaborative tasks in unmanned swarms through multiple stages such as task decomposition, task allocation, and task execution. In the task decomposition phase, SWARM-LLM uses large language models to conduct an in-depth analysis of task requirements and UAV capabilities, breaking down complex tasks into multiple executable subtasks, laying a solid foundation for subsequent task allocation and execution. In the task allocation phase, SWARM-LLM allocates tasks reasonably based on the execution requirements of subtasks and the skill characteristics of UAVs, ensuring that each task is performed by the most suitable UAV, thereby optimizing resource allocation and improving collaborative efficiency. In the task execution phase, UAVs execute specific tasks according to the task allocation plan generated by the large language model and interact with the environment through API calls to achieve set goals. Furthermore, this paper designs a set of prompt engineering methods suitable for unmanned swarm planning to guide and optimize the implementation of the aforementioned stages. Ultimately, we constructed meta-tasks, simple tasks, complex tasks, and heterogeneous tasks in an unmanned swarm simulation environment (AirSim), covering task scenarios of different complexities, and conducted evaluation experiments.

Results: The experimental results show that in the performance comparison of different task planning models, the SWARM-LLM series models (including GPT-3.5-Turbo, GPT-4, GPT-4o, and Claude3) all performed better than traditional optimization algorithms and machine learning methods in unmanned swarm task planning, especially showing a significant advantage in task success rate, with an average performance increase of 47.8%. Ablation experiments further analyzed the impact of different prompting methods on task planning performance, and the results indicated that the prompt engineering methods for unmanned swarm planning significantly increased the task success rate in complex and heterogeneous tasks. Additionally, the experiment also visually demonstrated the entire process of UAV task planning and execution, including scenarios of task allocation, coordination, and execution, providing an intuitive reference for unmanned swarm task planning.

Conclusion: The SWARM-LLM framework effectively enhances the efficiency and success rate of unmanned swarm task planning, verifying the potential of large language models in solving unmanned swarm task planning problems. The framework not only performed well in experiments but also provides a new direction for the development of future unmanned swarm task planning technology. Follow-up work will continue to explore the possibility of real-time dynamic task planning between UAVs using SWARM-LLM and study multi-agent LLM frameworks to further enhance the adaptability and decision-making capabilities of unmanned swarms in complex and dynamic environments, promoting the development of unmanned swarm task planning technology.

Key words task planning, unmanned swarms, large language models, collaborative strategies

大模型赋能航空战术分析应用研究

贾长江^{1*} 范鹏¹ 杨凯达² 张龙飞³ 夏少杰⁴

摘要 围绕航空战术分析场景中战术行为树构建问题,结合大模型技术在图结构数据以及行为树领域研究进展,提出了一种基于大语言模型驱动的逐步优化的战术行为树生成技术框架,利用大模型的上下文学习能力,通过大模型对自身生成的行为树的迭代优化,逐步生成更加高质量的行为树,以人机协同方式支撑战术分析人员高效开展战术行为树构建分析。

关键词 航空战术分析,大模型应用,行为树构建,应用研究

Applying Foundation Models to Empower the Aerial Tactics Analysis

JIA Chang-Jiang^{1*} FAN Peng¹ YANG Kai-Da² ZHANG Long-Fei³ XIA Shao-Jie⁴

Abstract This paper focuses on the behavior tree construction problem for the aerial tactics analysis. Based on the foundation models' capacities on processing graph data and behavior trees, this paper proposes a technical framework to generate tactical behavior trees with the step-by-step self-optimizations. The idea is to utilize the context learning capacities of foundation models to generate the behavior tree candidates, and then optimize them with the tactical evaluation feedbacks. This framework can help tactical analyzers to handle the behavior tree generation problem effectively and efficiently.

Key words aerial tactics analysis, foundation models, behavior tree construction, applying research

0 引言

在现代战争中,综合运用各型航空平台及武器夺取制空权,是掌控战场局势、赢得战争胜利的关键。随着航空平台及武器性能快速发展,相应战术战法不断创新,需要相应的数字化工具,辅助开展战术效能评估、应对策略研究等分析工作。

航空战术分析是指围绕战斗机、轰炸机等航空作战编队,对其作战运用的战术决策、战法规则等内容进行分析研究的过程。目前主流的分析工具以数字化仿真推演为主,如在 AFSIM 仿真平台^[1]中,具备对空中巡逻、空中拦截等多种空中作战样式的任务级仿真能力。对于空中仿真任务中的实体行为建模,主流采用行为树结构进行规则描述,通过相应的仿真引擎驱动

* 通讯作者

1. 中国人民解放军 93209 部队 2. 中国人民解放军 95808 部队 3. 国防科技大学系统工程学院 4. 中国电子科技集团公司第五十二研究所

1. Unit 93209 of the PLA 2. Unit 95808 of the PLA 3. College of Systems Engineering, National University of Defense Technology 4. The 52th Research Institute of China Electronics Technology Group Corporation

生成对应仿真任务。

将行为树表征技术应用于航空战术分析领域^[2]，需要定义相应的航空战术行为节点和战术规则连接器节点，来完成对整个航空战术的行为建模。由于行为树结构和航空战术的复杂性，需要行为树构建技术人员和航空战术实施人员协同配合，才能准确、全面地完成航空战术行为树的构建，存在周期长、效率低的问题。

近年来，大模型技术快速发展^[3]，在游戏博弈、人机对话等诸多领域取得了突破性的进展。大模型通过 Copilot 模式，即作为 AI 助手，与人协同提高业务工作效率。借鉴 Copilot 这种大模型赋能模式，聚焦航空战术分析应用场景，为提升航空战术行为树构建效率，本文提出了一种基于大语言模型驱动的逐步优化的战术行为树生成技术框架，利用大语言模型的上下文学习能力，在不微调大模型的情况下，通过大模型对自身生成的行为树的迭代优化，逐步生成更加高质量的行为树，以人机协同方式支撑战术分析人员高效开展战术行为树构建分析。

1 航空战术分析领域行为树构建

1.1 航空战术分析问题描述

航空战术分析是指基于战斗机、轰炸机等航空作战编队，对其作战运用的战术决策、战法规则等内容进行分析研究的过程。以战斗机战术分析研究为例，其典型分析过程通常包括战术实体能力建模、战术规则行为描述、战术过程仿真推演、战术评估迭代优化等阶段，如图 1 所示。

其中，战术实体能力建模，是指对战术中涉及的飞机、导弹、雷达等实体要素的作战能力进行建模表示；首先，以此为

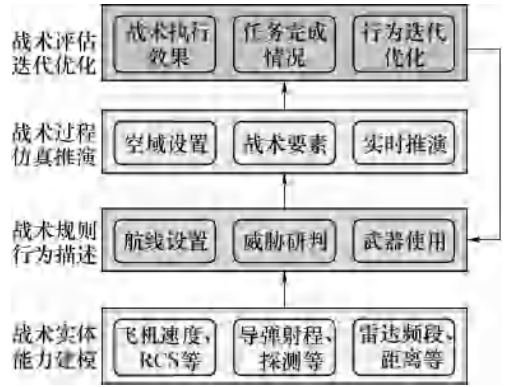


图 1 航空战术分析过程示意图

基础，描述战术规则行为，重点对各战术要素的动态行为规则进行表示，包括飞行航线设置、威胁分析研判、武器使用准则等；其次，利用仿真引擎，把构建的战术规则行为模型推演生成为可分析的实时动态战术过程；最后，分析人员针对实时战术过程以及复盘情况，从战术执行效果、任务完成情况等方面进行分析评估，并对战术规则行为模型提出优化修改意见，迭代优化战术规则行为模型。

在上述分析过程中，准确、快速地描述和迭代战术规则行为模型，是整个分析过程的关键。当前，该过程主要采用基于行为树的规则行为建模，下面以一个简单的空空战术行为树构建案例进行说明。

1.2 典型航空战术行为树案例

该案例^[4]以行为树方式对空战战术中的飞机行为进行建模描述。飞机在进行威胁分析和战术决策时，分析自身状态，包括是否接敌、面对敌机、弹药数量、健康状态等方面，相应状态数值空间见表 1。

在状态分析基础上，采用不同的战术行为来最优化当前的最佳战术目标，相关行为动作描述见表 2。

表 1 空空战术中飞机能力状态描述示例

飞机状态要素	数值空间
是否接敌	(1, 0): 1 表示接敌, 0 表示未接敌
面对敌机	(1, 0): 1 表示面对敌机, 0 表示未面对敌机
弹药数量	(3, 2, 1, 0): 3 表示弹药充足, 2 表示有弹药消耗, 1 表示弹药不足, 0 表示无弹药
健康状态	(3, 2, 1, 0): 3 表示机体完好, 2 表示有轻微毁伤, 1 表示严重毁伤, 0 表示飞机被摧毁

表 2 空空战术中飞机战术动作描述示例

飞机战术动作	行为描述
飞行巡逻	若无接敌, 则按照既定的航线设置进行飞机巡逻
开始攻击	若接敌并且面向敌机, 则开始攻击模式, 进行武器使用
转向接敌	如果在接敌时, 没有面向敌机, 则进行飞行转向, 形成攻击态势
撤离战场	在弹药数量和健康状态不理想时, 执行撤离战场操作

基于上述飞机状态空间和行为空间的描述定义, 其战术行为决策过程可构建为行为树, 作为该飞机的战术行为模型, 如图 2 所示。



图 2 空空战术飞机战术行为树示意图

图中通过设置选择节点 (Selector) 和动作节点 (Action), 实现在战术执行过程中对飞机状态的实时分析以及相应战术动

作的选择, 该行为树结构即为战术行为的数字模型, 是后续战术仿真推演的依据。

在上述构建战术行为树模型过程中, 传统方式下依赖特定领域专家和技术人员协同操作, 往往耗时耗力。结合当前大模型技术的强大表示能力和推理能力, 设计一种大模型驱动的航空战术行为树生成方法, 将极大提升战术行为树的构建效率。下面, 本文对大模型技术发展现状进行分析, 重点围绕在图结构数据理解和行为树构建领域的大模型技术研究进展进行讨论。

2 大模型与行为树研究现状

2.1 大模型技术发展概述

近年来, 人工智能生成内容技术蓬勃发展。通过在大规模语料库上对 Transformer 模型进行预训练, 提出了在自然语言处理任务中表现突出的预训练语言模型, 并发现随着参数规模的扩大, 模型会进化出上下文学习等新型特殊能力, 为区分不同参数规模下的语言模型, 大语言模型 (Large Language Model, LLM) 应运而生。行业大模型与通用大模型竞相培育, 伴随着生成内容的可控性增强, 垂直场景的试点与探索不断加速, 各行业领域纷纷探索适合自身发展的适配性场景。

大语言模型是基于 Transformer 架构^[5]的深度学习模型。模型规模非常庞大, 拥有数十亿甚至数万亿的参数, 使得它们能够学习复杂的语言模式, 并执行对于较小模型来说难以或不可能完成的任务。Transformer 架构包含编码器与解码器, 根据模型技术路线的不同, 大语言模型通常分为只使用编码器 (Encoder Only)、只使用解码器 (Decoder Only)、同时使用编码器与解码器 (Encoder-Decoder)。基于编

码器的大语言模型主要包括 BERT 模型^[6]及其后续变种模型，如 RoBERTA^[7]、ALBERT^[8]、ERNIE^[9-10]、ELECTRA^[11]、DeBERTa^[12]等。基于解码器的大语言模型主要包括 GPT 系列、LLaMA 系列，基于编码器与解码器的大模型主要有 BART^[13]、T5^[14]以及后续的 GLM 系列。

2.2 大模型处理图结构数据

行为树将决策逻辑以树形结构进行表达，如本文研究的战术行为树是以树状结构来描述整个战术过程的决策行动规则。随着大语言模型在自然语言处理中

的广泛应用，其在处理和生成树、图等结构化数据方面的能力引起了广泛关注。这些能力包括但不限于树结构、图结构数据的理解、生成以及复杂的推理任务。通过人机多轮迭代的方式，可以利用大模型自主生成初步的行为树结构，并通过专家反馈逐步优化，提高效率和准确性。

文献 [15] 研究了大语言模型在理解和操作图结构数据方面的能力，并提出了一种结合大语言模型和图数据结构的新技术框架 GPT4 Graph (图 3)，用来评估大语言模型在理解图数据方面的能力。

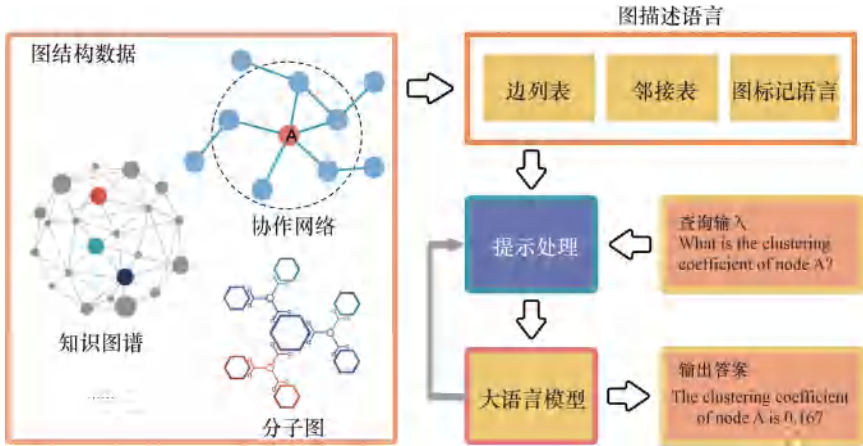


图 3 GPT4 Graph: 大语言模型和图结构数据结合技术框架

GPT4 Graph 通过手动和自生成的提示方法，评估了大语言模型在零样本和少样本设置中的表现。结构理解任务包括图大小检测、度数检测、边缘检测、属性检索、直径计算、聚类系数计算等任务。实验表明，输入设计对模型性能有显著影响，角色提示和示例对图理解有一定帮助。在语义理解任务方面，GPT4 Graph 发现大语言模型在知识图谱问答、图查询语言生成、节点分类、图分类等任务上表现出色，但与专门的图模型相比仍有差距。通过上述研究，GPT4 Graph 得出结论，大

语言模型在图结构数据的理解和处理上有显著潜力，但仍需进一步发展以达到专门图模型的水平。未来的研究应关注不同输入设计和角色提示技术的优化，探索图推广方法以提升语义理解任务的表现。

针对当前大语言模型训练依赖非结构化文本数据等限制，文献 [16] 开展了相关研究来评估大语言模型在理解图结构数据方面的能力。将图结构数据编码为文本以供大语言模型处理，并对多种图编码方法及其在不同图推理任务中的有效性进行了全面评估，技术框架如图 4 所示。

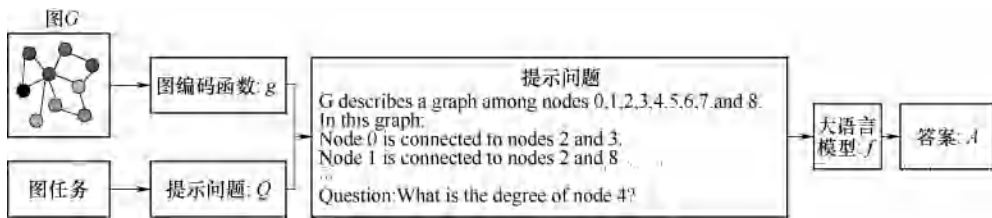


图4 使用大语言模型进行图推理技术框架示意图

该文献探讨了图编码技术、提示工程和基准测试的设计与实施，旨在提升大语言模型在图推理任务中的表现。研究表明，选择适当的图编码方法对大语言模型在图任务中的表现有显著影响。

2.3 大语言模型与行为树构建

行为树起源于视频游戏行业，然后被广泛应用于机器人等领域。与传统的任务表示如状态机、层次结构架构和决策树相比，行为树形式具有模块化、灵活性和可读性强等优点。行为树通常由人类专家花费大量时间进行设计，因此，近年来，行为树的自动化设计吸引了很多关注。传统的行为树构建方式主要分为基于学习的构建方式与基于规划的构建方式。基于学习的行为树生成方法通过有效地表示行为树结构中的战略行为，展现出卓越的适应性，利用大量的数据来学习行为模式和策略，使代理能够在不同的任务和环境中更有效地进行适应，通过自动发现和捕捉战略行为，学习方法赋予代理在复杂环境中做出自适应决策的能力，并且通过迭代训练，可以根据实际效果对生成的行为树进行改进，确保与期望目标和要求更好地对齐，包括基于强化学习的方法、基于进化算法的方法和基于演示的方法。另一类基于规划的方法为行为树生成提供了直观且可解释的框架，可以促进行为树的自动生成和动态更新，

有效地将行为树的模块化和反应性特性与自动规划的系统综合过程相结合。近年来，大型语言模型展示出强大的生成和语义理解能力，可以帮助生成详细的描述和定义，从而能够根据任务叙述或约束生成高质量的行为树，在任务描述、任务分解、节点选择、行为树结构化、初步行为树验证和迭代行为树改进等多个阶段发挥作用。

文献 [17] 首次尝试将大语言模型应用于机器人任务领域的行为树的生成，将其从顺序任务扩展到层次任务，通过结合行为树的模块化和可重用性，进一步减轻了最终用户设计的难度和负担，其技术流程如图5所示。

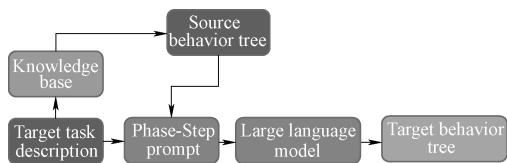


图5 基于大模型的机器人行为树生成流程示意图

该技术框架流程：首先从一个领域任务描述 (Target Task Description) 开始，经过一个相似度排序，从知识库 (Knowledge Base) 中找到最合适的基础行为树 (Source Behavior Tree) 模型，然后将基础行为树模型和领域任务描述一同输入阶段步骤提示模块 (Phase-Step Prompt)，该模块进入大语言模型 (Large Language Model) 进行不断

迭代生成完整的、符合任务描述的目标行为树 (Target Behavior Tree)。对于最终用户而言,只需要给出相应的任务描述信息,剩余过程都可以自动完成。

3 大模型驱动航空战术行为树构建

利用大模型技术对战术规则行为描述过程赋能,是提升航空战术分析效能的关键。基于大模型的行为树生成,通过微调小规模的大语言模型,用以直接输出行为树,或者通过大规模的大语言模型上下文学习直接生成行为树,这种端到端的直接生成方式,通常适用于相对简单的应用场景,对于航空战术分析场景,涉及不同类型航空平台能力、航空武器性能以及飞行员态势感知和决策规则水平,其最终的战术规则会非常复杂,因此,基于大模型端到端生成行为树的技术路径会极具挑战性,可能存在以下问题:

(1) 行为树规模较大,大语言模型直接将其作为序列输出,产生漏洞的可能性比较高,导致行为树不能直接用于实际应用,需要较长时间的人工校验过程。

(2) 大语言模型具有强大的语义理解与生成能力,但是目前在逻辑推理方面是欠缺的,尤其是航空战术专业领域的处理逻辑,因此,难以生成能够准确描述领域复杂逻辑关系的行为树。

(3) 受限于领域数据规模,基于大模型构建端到端的战术行为树生成模型,其训练优化过程缺少最优方案相应的训练数据,并且行为树生成问题的状态空间是复杂多样的,而训练数据是有限的,模型面临迁移泛化的考验,大语言模型对训练集之外的指令,生成最优行为树挑战性更大。

3.1 大模型驱动航空战术行为树生成技术框架

基于上述大模型在航空战术分析领域的应用限制,本文提出一种基于大语言模型驱动的逐步优化的战术行为树生成框架,利用大语言模型的上下文学习能力,在不微调大模型的情况下,通过大模型对自身生成的行为树的迭代优化,逐步生成更加高质量的行为树,技术框架包括四个部分:行为树的生成;行为树的调试;行为树的优化;行为树的评估。通过四个步骤迭代执行,最终实现战术行为树的逐步优化。技术框架如图6所示。

3.1.1 行为树的生成:构建基础战术行为树

首先由战术实施人员输入基本的战术规则指令,采用现有的大模型行为树生成方法,生成相应的战术行为树模板,作为后续行为树优化的基础。

在技术选型上,可以采用微调后的大语言模型生成质量更高的行为树,更高质量的行为树可以更快完成优化,达到其优化上限,但是也更容易陷入局部最优,其所能达到的优化上限明显低于最优解,因此,初始生成步骤需要考虑同时生成多个多样性强的行为树作为优化起点,从多个角度出发,在各自优化得到的行为树中选择表现更好的作为最终输出,提高生成的基础行为树的质量。

3.1.2 行为树的调试:保证行为树逻辑正确

战术行为树是一种严谨的领域逻辑规则数据结构,对于生成的战术行为树样例,需要进行调试检查,确保其正确性和合理性。

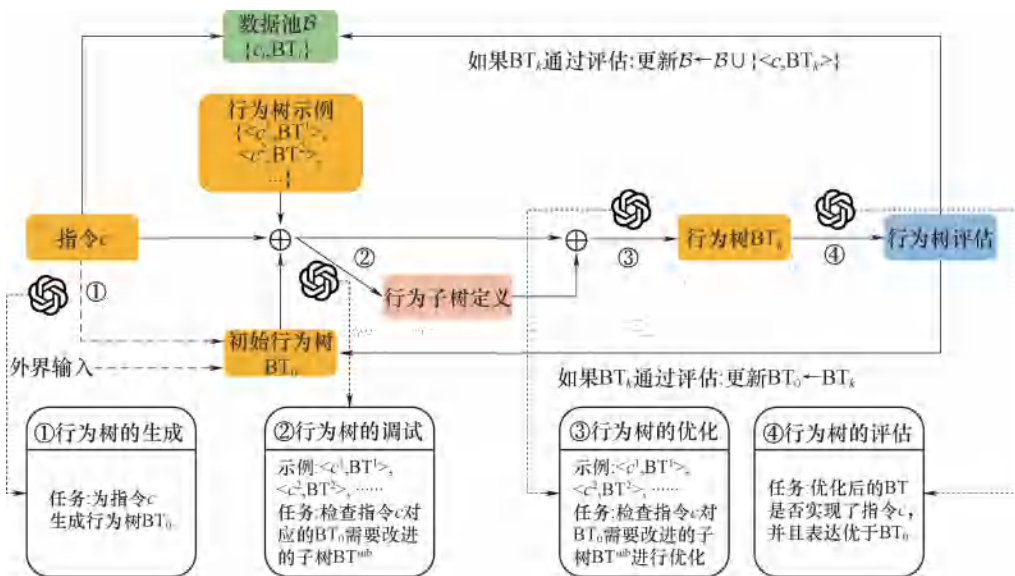


图6 大模型驱动的航空战术行为树生成技术框架

对于大语言模型而言，其主要是基于学习的生成式模型，通常以自回归的方式进行逐字符的生成，缺乏对生成内容的语法合法性检查，因此，对于战术行为树这种具有复杂领域指令和行为动作的数据结构而言，在生成过程中产生错误的概率可能快速上升，其中既包括语法错误，也包括逻辑错误，以及可能需要被优化的实现方式，因此，需要对生成的行为树进行调试与修改。

由于生成规模大的行为树的出错概率远高于生成规模小的生成树，在此首先利用大模型进行优化子树的定位，只修改定位到的位置，经过多次调试修改，逐步消除行为树中的漏洞，避免整体生成行为树时因消除某个漏洞时产生更多的漏洞。在实际操作中，将要实现的战术指令 c ，当前被调试的战术行为树 BT ，以及若干行为树与指令数据对作为示例，一同作为输入，使得大模型能够对行为树 BT 进行分析，输出可以被优化的具体子树位置，用

于后续的操作。

3.1.3 行为树的优化：精简完善行为树结构

在保证生成行为树正确、合理的基础上，需要对行为树的整体结构进行优化，实现去除冗余、精简结构等目标。

在行为树的调试过程中，确定了需要被优化的位置，则可对被选定的子树结构进行优化，将行为树、子树位置、指令，以及从数据池中选择的示例一齐作为大模型的输入，使得大模型输出优化后的行为子树表达，替换其在行为树中的位置，并且保持行为树的其他部分不变，大模型可以根据示例数据学习到如何生成更好的行为子树的表达。

3.1.4 行为树的评估：确保行为树合理有效

战术行为树用于航空战术分析，其结果可为飞行员开展战术飞行训练提供参考，因此，必须对其可靠性、安全性等要素进行评估和验证。

评估过程保证行为树不仅在其预定的操作参数范围内有效运行，而且要确保生成的行为树能够符合高质量的要求。如果每一步迭代优化后的行为树，其评估表现比优化前评估更好，则将当前行为树继续进行优化，否则继续使用上一轮的行为树作为优化目标。一方面，评估过程要关注检查大模型生成的行为树是否按照原始的设计正确构建。另一方面，评估检查大模型是否能够输出期望的结果，并且生成的行为树能够有效地执行期望的任务。另外，结合行为树检查、仿真推演等方式检查行为树的性能，以提高生成的行为树的可信度，并进一步调整生成的行为树。可以使用已有的大模型进行生成结果的验证，并且可以根据已有的模拟器进行实际的模拟评估，对生成的结果进行准确的量化。

与现有基于大模型的行为树生成方法相比，本技术框架有以下优势：

(1) 本框架采用迭代优化的方式进行行为树的生成，通过不断评估与改进，减少行为树中的漏洞，规范行为树的表达，能够生成更高质量的行为树，尤其在为复杂指令生成行为树中将更加具有优势。

(2) 本框架维护了一个高质量的<战术指令、行为树表述>数据池，随着行为树生成以及评估结果越来越多，该数据池的规模和质量也会得到提升，进一步提高本框架生成行为树的能力与质量，在大模型的上下文学习中，示例的质量对生成结果有非常重要的影响。

3.2 技术框架落地实现若干考虑

将上述基于大模型的航空战术行为树生成技术框架进行工程实现，需要重点关注两个方面的工程挑战：一是构建航空战术语义理解模型，二是构建战术分析提示

词工程。

其中，航空战术语义理解模型，是基于大语言模型，通过对大量带有标签的航空战术领域数据进行学习，实现对航空战术指令的精确语义理解；战术分析提示词工程，作为连接用户需求与模型响应的关键纽带，依据用户的特定战术指令查询需求，实现从模型中筛选并抽取最贴合要求的战术行为树结构，若模型中未找到相应结构，则自动生成，并提供一个互动界面，允许用户与大模型协作调整战术行为树，直至满足用户的需求，如图7所示。

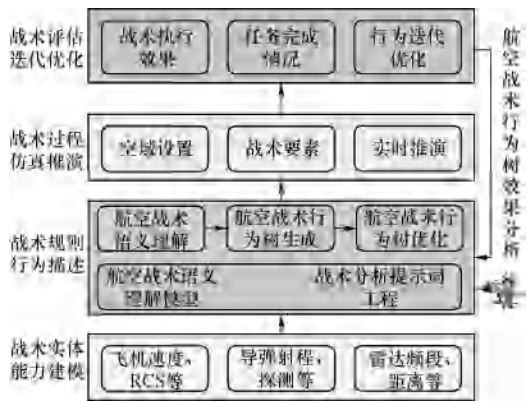


图7 大模型赋能航空战术分析应用示意图

借助这一机制，实现了战术人员通过自然语言指令输入至战术行为树输出的平滑过渡，极大提升行为树构建的效率，同时显著降低对专业领域知识的门槛要求，使得行为树的创建变得更为便捷高效。

3.2.1 航空战术语义理解模型构建

该模型架构主要由两大部分组成：数据工程与模型微调。其中，数据工程聚焦于输入数据的预处理及样本集构建，具体操作包括剔除自然语言中的空行、换行等特殊符号，确保数据的纯净度。同时，这一阶段还负责构建从自然语言到行为树的结构数据样本，明确输入为

自然语言，输出则为描述行为树结构（如 JSON 格式）。

在数据工程的基础上，模型微调阶段则致力于通过利用准备的训练数据来优化模型，旨在让模型具备将自然语言转换成行为树结构的能力。这一环节是整个模型实现其设计目标的关键步骤，确保模型能够准确理解并处理自然语言，进而生成所需的行为树结构。

3.2.2 战术分析提示词工程

战术分析提示词工程，用于连接自然语言理解和行为树的智能生成。其核心机制是：将构建的自然语言与行为树的结构数据格式化并存储于数据库中，形成一个丰富的信息库，当用户提出问题，系统即刻启动其高效的检索引擎，从数据库中快速定位并提取出与问题最为匹配的行为树，这一过程显著减少了大型模型的执行时间，极大地提升了系统的响应速度和运行效率。如果在数据库中未能找到直接匹配的行为树，系统将调用训练的大模型，根据用户的自然语言描述，智能生成全新的行为树，以满足用户的具体需求。此外，在获取到行为树后，还支持用户进行多次对话式的修改和优化，确保最终生成的行为树完全符合用户的期望，实现了人机交互的深度融合和智能化升级。

4 结束语

本文围绕航空战术分析场景，探讨了大模型技术赋能的可行性，并围绕核心的战术行为树自动生成问题，提出了一种基于大模型的战术行为树自动生成技术框架，并围绕其落地实现面临的关键问题进行讨论，可为后续工程落地实现以及相关领域大模型应用提供参考。

参考文献

- 1 PETER D C, JEFFREY A J, et al. Advanced Framework for Simulation, Integration and Modeling (AFSIM) [J]. International Conference on Scientific Computing, 2015.
- 2 刘西, 陈伟, 冯志峰, 等. 双机编队空战仿真模型设计 [J]. 系统仿真技术, 2023.
- 3 赵朝阳, 朱贵波, 王金桥. ChatGPT 给语言大模型带来的启示和多模态大模型新的发展思路 [J]. 数据分析与知识发现, 2023.
- 4 方君, 闫文君, 邓向阳, 等. 基于 Q-学习和行为树的 CGF 空战行为决策 [J]. 计算机与现代化, 2017.
- 5 VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need [J]. Advances in neural information processing systems, 2017, 30.
- 6 DEVLIN J, CHANG M W, LEE K, et al. Bert: Pre-training of deep bidirectional transformers for language understanding [J]. arXiv preprint arXiv: 1810. 04805, 2018.
- 7 LIU Y, OTT M, GOYAL N, et al. Roberta: A robustly optimized bert pretraining approach [J]. arXiv preprint arXiv: 1907. 11692, 2019.
- 8 LAN Z, CHEN M, GOODMAN S, et al. Albert: A lite bert for self-supervised learning of language representations [J]. arXiv preprint arXiv: 1909. 11942, 2019.
- 9 ZHANG Z, HAN X, LIU Z, et al. ERNIE: Enhanced language representation with informative entities [J]. arXiv preprint arXiv: 1905. 07129, 2019.
- 10 SUN Y, WANG S, LI Y, et al. Ernie 2. 0: A continual pre-training framework for language understanding [C] //Proceedings of the AAAI conference on artificial intelligence. 2020, 34 (5): 8968-8975.
- 11 CLARK K, LUONG M T, LE Q V, et al. Electra: Pre-training text encoders as discriminators rather than generators [J]. arXiv preprint arXiv: 2003. 10555, 2020.
- 12 HE P, LIU X, GAO J, et al. DeBERTa: Decod-

- ing-enhanced bert with disentangled attention [J]. arXiv preprint arXiv: 2006. 03654, 2020.
- 13 LEWIS M, LIU Y, GOYAL N, et al. Bart: Denoising sequence-to-sequence pre-training for natural language generation, translation, and comprehension [J]. arXiv preprint arXiv: 1910. 13461, 2019.
- 14 RAFFEL C, SHAZEER N, ROBERTS A, et al. Exploring the limits of transfer learning with a unified text-to-text transformer [J]. Journal of machine learning research, 2020, 21 (140): 1-67.
- 15 GUO J, DU L, LIU H, et al. Gpt4graph: Can large language models understand graph structured data? an empirical evaluation and benchmarking [J]. arXiv preprint arXiv: 2305. 15066, 2023.
- 16 FATEMI B, HALCROW J, PEROZZI B. Talk like a graph: Encoding graphs for large language models [J]. arXiv preprint arXiv: 2310. 04560, 2023.
- 17 CAO Y, LEE C S. Robot behavior-tree-based task generation with large language models [J]. arXiv preprint arXiv: 2302. 12927, 2023.

大模型启发增强的未知混叠雷达信号分选方法**

牛恺锐^{1*} 齐佩汉¹ 李甫¹ 林云²

摘要 针对大模型在复杂电磁环境下的数据需求，提出了一种大模型启发增强的雷达信号分选方法。该方法引入多尺度融合嵌入和掩码增强，并将其应用于构建雷达分选的数据增强集。多尺度融合嵌入对原始信号进行深度时序编码；掩码构建则模拟复杂环境，实现信号的不同程度交织情形。实验表明，在12类雷达信号5dB信噪比场景下，基于该算法生成的高质量训练集支持取得94%的正确分选率，验证了该大模型驱动数据增强方法在电磁领域大模型应用中的有效性。

关键词 大模型启发，数据增强，雷达信号分选，尺度融合

A Data Augmentation Approach Enabling Feature Learning for Large Models in Radar Signal Sorting**

NIU Kai-Rui^{1*} QI Pei-Han¹ LI Fu¹ LIN Yun²

Abstract To meet the data requirements of large models in complex electromagnetic environments, a large model-inspired data augmentation method for radar signal sorting is proposed. This method introduces multi-scale fusion embedding and mask augmentation, and applies them to construct a data augmentation set for radar signal sorting. Multi-scale fusion embedding performs deep temporal encoding on the original signals, while mask construction simulates complex environments and realizes different degrees of signal interleaving. Experiments show that in a 12-class radar signal scenario with 5dB signal-to-noise ratio, the high-quality training set generated by this algorithm enables a 94% correct sorting rate, demonstrating the effectiveness of this large model-driven data augmentation method in large model applications for the electromagnetic domain.

Key words large model inspiration, data augmentation, radar signal sorting, scale fusion

0 引言

在当前人工智能飞速发展的时代，大

模型的浪潮席卷了各个领域^[1-2]。特别是在时序数据处理方面，时序大模型展现出了巨大的潜力^[3]。为了构建一个强大的电

** 国家基础科研项目 (JCKY2023110C099) 和国家自然科学基金面上项目 (62171334) 资助

** Supported by National basic scientific research JCKY2023110C099 and the National Natural Science Foundation of China (62171334)

* 通讯作者

1. 西安电子科技大学 2. 哈尔滨工程大学信息与通信工程学院

1. Xidian University 2. College of Information and Communication Engineering, Harbin Engineering University

磁领域基础大模型,使其掌握电磁信号处理的专业知识和技能,能够应对电磁空间中的各种复杂挑战^[4],如信号调制方式识别^[5]、雷达辐射源识别^[6]、频谱感知^[7]和通信协议理解^[8]等,需要从数据增强的角度为其提供有力支撑。

电磁信号具有高维度、非线性、时变等复杂特征,传统的数据增强方法如旋转、翻转等在这里往往难以奏效^[9]。此外,在复杂电磁环境下获取的信号质量往往参差不齐,存在严重的信号失真、噪声干扰等问题,进一步加大了数据增强的难度^[10]。

以雷达信号分选为例,传统的分选算法在低信噪比、信号交织等复杂场景下性能往往难以满足实际需求。而基于时序大模型的端到端识别分类方法有望突破这一瓶颈,实现智能化、自适应的信号分选^[11-12]。但这也对训练数据的质量和规模提出了更高的要求。

因此,探索电磁信号领域的数据增强新方法,为大模型训练提供有力的数据支撑,是一项意义重大而又充满挑战的课题。这不仅关系到电磁大模型的落地应用,更将助力电磁信号处理技术的智能化发展。

本文聚焦于雷达脉冲信号的分选问题,这是电子侦察领域的一个重要任务。现有的雷达脉冲分选技术在复杂电磁环境下,如高脉冲密度、严重脉冲交叠、低信噪比等情况^[13],以及噪声、环境等因素导致的信号分布、时延的变化会让源模型的表现十分糟糕^[14],其泛化能力往往有限。

针对大模型启发增强的雷达信号分选中的数据增强问题,本文所提方法引入了多尺度融合嵌入和掩码增强技术。其中,多尺度融合嵌入通过深度时序编码,在不同时间尺度上提取原始信号的特征表示。掩码增强则模拟了复杂电磁环境,实现了信号不同程度的交织。通过这种方式,构

建了一个面向雷达分选任务的数据增强集。为了验证所提出方法的有效性,开展了一系列实验,并基于实现雷达脉冲信号分选的同时验证了方法的有效性。

1 问题的提出

1.1 雷达脉冲分选

雷达信号处理通常包括两个关键环节:脉冲分选和调制样式识别。其中,雷达信号分选是指将接收机截获的混合脉冲流分离、归并到其原始发射源的过程。在复杂电磁环境下,接收机往往会捕获来自多部雷达的脉冲信号,它们在时间、频率、空间等域上交织在一起。分选算法的目标就是通过脉冲描述字(PDW)的相似性分析,将同一雷达发射的脉冲聚类在一起,还原出各个雷达源的独立脉冲串^[15]。而对于分选后的单源信号,下一步则是进行调制样式识别,判断该雷达的信号调制方式,如脉冲编码、相位编码、频率捷变等,以进一步推断其功能属性和威胁等级^[16-17]。雷达信号分选流程如图1所示。

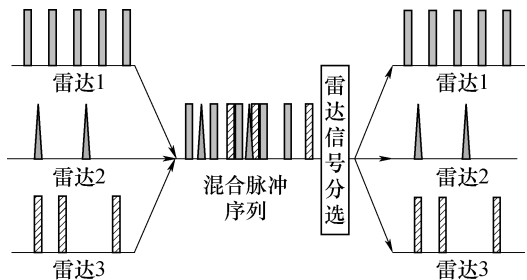


图1 雷达信号分选流程

1.2 雷达脉冲描述字

在雷达信号分选与识别任务中,脉冲描述字(Pulse Descriptive Word, PDW)是一种常用的信号表征形式。雷达信号分

选常选用 PDW 用于信号分选。典型的 PDW 组成如下所示：

$$\{\text{PDW}_i = \theta_{\text{DOA}_i}, f_{\text{RF}_i}, t_{\text{TOA}_i}, \tau_{\text{PW}_i}, A_{\text{PA}_i}\}_{i=0}^N \quad (1)$$

PDW 通过一组关键参数来刻画单个雷达脉冲的特性，其中最常见的五个瞬时参数分别是：

(1) 脉冲幅度 (Pulse Amplitude, PA)：表示脉冲信号的强度或能量大小；

(2) 脉冲到达时间 (Time of Arrival, TOA)：标识脉冲信号被接收机捕获的时间点；

(3) 脉宽 (Pulse Width, PW)：度量脉冲信号持续的时间长度；

(4) 载频 (Radio Frequency, RF)：指脉冲信号的载波频率；

(5) 脉冲到达角 (Direction of Arrival, DOA)：表征脉冲信号到达接收机的空间方位。

式 (1) 中， i 为按照时间先后顺序接收到的雷达脉冲的序号，取值范围从 1 到 N ；其中， N 为在给定时间窗口内截获的脉冲总数。上述五个瞬时参数可以通过雷达接收机的参数检测与测量模块直接获得，是构建 PDW 的基本要素。

在实际的雷达侦察系统中，这些参数的测量通常是自动完成的。当接收机截获到一个脉冲信号后，参数检测与测量单元会实时对其进行分析，提取出 TOA、RF、PW、PA 和 DOA 等关键特征，并将其打包成一个 PDW 向量。

1.3 大模型预训练-微调的训练范式

预训练-微调 (Pre-training and Fine-tuning) 范式在自然语言处理和计算机视觉领域取得了巨大成功^[18]，其核心思想是先在大规模无标注数据上进行自监督

预训练，学习到通用的特征表示，再在特定任务的小规模标注数据上进行微调，实现下游任务的快速适配和性能提升。

这一范式的成功很大程度上归功于掩码语言建模 (Masked Language Modeling, MLM)^[19]和掩码图像建模 (Masked Image Modeling, MIM)^[20]等自监督学习算法的发展。通过随机掩蔽输入数据的一部分，并训练模型预测被掩蔽的内容，这些算法能够让模型学习到数据内在的结构和语义信息，从而获得更加通用、鲁棒的特征表示。

然而，在电磁信号处理领域，特别是雷达信号分选等任务中，由于缺乏大规模标注数据，预训练-微调范式的应用还比较有限。雷达信号数据的获取和标注成本很高^[21]，且真实场景下的信号往往存在严重的噪声、干扰、信号交织等问题，这对预训练算法提出了更高的要求。

为解决雷达信号领域数据不足的问题，本文提出了一种创新的大模型启发增强的雷达数据增强方法。该方法引入多尺度融合嵌入和掩码增强技术，在有限的雷达信号数据基础上，生成大规模、高质量、多样化的增强数据集，为预训练模型提供丰富的训练样本。

借鉴 MLM 和 MIM 的思路，通过对信号的随机掩蔽和重构，模型可以学习到信号内在的时频域特征和调制方式。多尺度融合嵌入将信号映射到高维空间，在不同尺度上提取局部和全局特征，增强了模型对多样化信号的表征能力。

本文在增强数据集上训练的模型，在下游的雷达信号分选任务上取得了显著的性能提升，特别是在低信噪比、信号交织等复杂场景下，展现出了优异的泛化能力和鲁棒性。这证明了数据增强方法能够有效支持模型的预训练-微调范式在电磁信号处理领域的应用。

2 方法

2.1 多尺度融合嵌入

设长度为 L 的 N 维变量 $s_{\text{PDW}} \in \mathbb{R}^{L \times N}$ 是



图2 多尺度融合嵌入流程

M 是最大的模数上界，最大的模数是 $m_{\max} = M/k^1$ ，意味着输入数据值的模 m_{\max} 无信息损失，这里默认 1 是最小的模，因此，需要线性变化输入数据以使得数据的信息能体现在模 $1 \sim m_{\max}$ 的剩余系中。

由于 M 是 k 的 D 指数阶，选择 d 、 k 满足该条件即可，通过以下公式得到宽值域嵌入 $E_{\text{PDW}} \in \mathbb{R}^{L \times N \times D}$ ：

$$E_{\text{PDW}}^{l, n, di+j} = f_{\omega=1} \left(\frac{s_{\text{PDW}}^{l, n}}{M^{di/D}} + \frac{j}{d} \right) \quad (2)$$

$$i \in \{0, 1, \dots, D/d - 1\}$$

$$j \in \{1, 2, \dots, d\}$$

式中， $di + j \in \{1, 2, \dots, D\}$ 为嵌入的一个维度； x 为该输入 token 的值； l 为输入信号长度； n 为输入信号维度。

$f_{\omega=1}(\cdot)$ 是所使用周期为 1 的线性周期函数，表达式如下：

$$f_{\omega=1}(x) = x \bmod 1 \cdot 2 - 1 \quad (3)$$

多尺度融合嵌入等同于把原始信号值通过正整数倍的线性周期函数族进行变换，波长形成了从 1 到 m_{\max} 的正整数 k 倍。通过这种方式，原始信号被嵌入一个高维空间中，不同维度对应着不同尺度下的信

输入的信号， D 是所需的嵌入的维度， $E_i \in \mathbb{R}^D$ 是嵌入，这由所使用的主干网络的输入决定，则可以设置步长 $d_{\text{step}} \in \mathbb{N}^+$ （以下简称为 d ）与缩放系数 $k \in \mathbb{N}^+$ 来控制最大的模数上界 $M = k^{D/d}$ ；反之，由 M 、 k 决定 $d_{\text{step}} = D \cdot \log_k M$ ，如图 2 所示。

号特征。

值得注意的是，由于周期函数的嵌套特性，只有在更大的维度 m （对应更长的波长）上才能捕捉到小尺度下的信号信息。这意味着多尺度融合嵌入是一种跨尺度、层次化的信号表示方法。

从数学角度来看，将一维信号点映射到 D 维向量的过程，可以描述为对原始值进行模运算，其中每一维都使用一个特定的模数。不同维度的模数可以控制该维度捕捉信号细节的粒度。

2.2 掩码交织构建

对多尺度融合嵌入空间进一步处理，将掩码表示为 M ，将掩码区域的填充值表示为 z ，掩码后的嵌入表示为 $M \times x + (1 - M) \times z$ ，如图 3 所示。

通过对多尺度融合嵌入的部分维度进行掩码，已知模 m ，查找进行掩码的最低维度函数 $d_{\text{low}}(\cdot)$ 为：

$$d_{\text{low}}(m) = d \cdot \log_k m \quad (4)$$

根据以上计算结果对 $d > d_{\text{low}}(m)$ 的维度进行掩码，就能近似构建极大极小差值

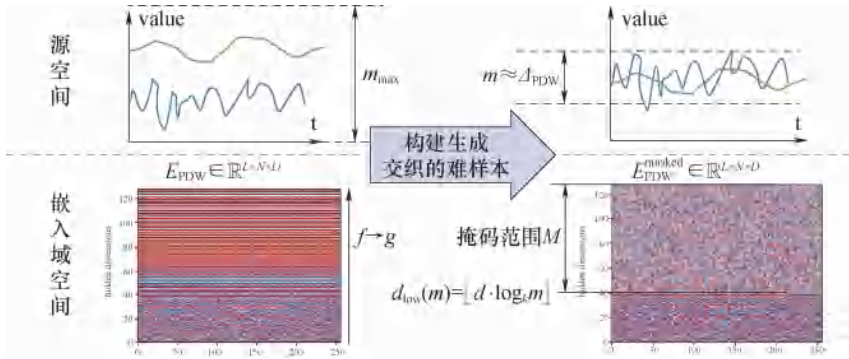


图3 掩码构建交织难样本示意图

为 m 信号的交织情况。

掩码函数定义为 $F_{\text{mask}}(\cdot, d_{\text{low}})$ ，输入前述的多尺度融合嵌入张量 $\mathbf{E}_{\text{PDW}} \in \mathbb{R}^{L \times N \times D}$ ，输出为 $\mathbf{E}_{\text{PDW}}^{\text{masked}} \in \mathbb{R}^{L \times N \times D}$ 。

然后选择合适的掩码方案，以下为三种对于时间维度上掩码的方式，设输入的宽值域嵌入张量为 $\mathbf{E} = [e_1^l, e_2^l, \dots, e_D^l]$ ，这里的 d_{low} 表示为 $d_{\text{low}}(m)$ 的一个随机采样。

均值掩码方式为：

$$F_{\text{mask}}(\mathbf{E}, d_{\text{low}}) = \begin{cases} \sum_{l=1}^L e_d^l \cdot \frac{1}{L} & d \geq d_{\text{low}} \\ e_d & d < d_{\text{low}} \end{cases} \quad (5)$$

随机值掩码方式为：

$$F_{\text{mask}}(\mathbf{E}, d_{\text{low}}) = \begin{cases} \mathcal{R}(e_d) & d \geq d_{\text{low}} \\ e_d & d < d_{\text{low}} \end{cases} \quad (6)$$

式中，函数 $\mathcal{R}(\cdot)$ 为产生一个相同、元素均匀分布在 $[0, 1]$ 之间的张量。

常数掩码方式为：

$$F_{\text{mask}}(\mathbf{E}, d_{\text{low}}) = \begin{cases} \mathbf{0}^{L \times N} & d \geq d_{\text{low}} \\ e_d & d < d_{\text{low}} \end{cases} \quad (7)$$

经实验验证，以上方式都有相似且比较好的效果，但随机值掩码的鲁棒性最强。

以一个概率 P_{hard} 对输入信号 s_{PDW} 的任一特征维度做掩码，称为难样本的难度概

率，这是一个超参数，它控制了对输入特征施加掩码的概率，从而模拟一定比例的“难样本”存在。

具体而言，通过原始数据的极大极小值的差值 Δ_{PDW} 确定加入掩码的范围：

$$\{d \in (\mathcal{R}(d_{\text{low}}(\Delta_{\text{PDW}}), d_{\text{low}}(2\Delta_{\text{PDW}})), D)\} \quad (8)$$

式中，函数 $\mathcal{R}(\cdot)$ 为生成 $[a, b]$ 内均匀分布的离散随机整数变量； d_{low} 为 $d_{\text{low}}(m)$ 的一个随机采样。

掩码函数则决定了具体的掩码方式，如采用均值掩码或随机掩码等。掩码宽值域嵌入作为模型的训练输入，可以提高模型对异常情况和噪声的鲁棒性。

通过在维度上进行掩码，相当于破坏了某些值域区间的信号细节，而保留了其他区间的信息。这种操作在一定程度上模拟了信号在值域上的“交织”现象。在训练时，这种部分观测的状态能够增强模型的鲁棒性，使其学会从残缺的信息中进行推断。

3 仿真实验与分析

3.1 实验参数

本实验利用 pytorch 框架搭建深度学习

网络模型，使用设备 CPU 为 Intel (R) Core (TM) i9-14900k；GPU 为 NVIDIA GeForce RTX 2080Ti 训练模型，采用 Adam 优化器对网络模型参数进行更新，批大小设置为 40，初始学习率设置为 0.005。对数据集按照 7 : 3 的比例划分训练集和验证集。

3.2 数据集

(1) 实验的训练集：设置雷达每种信号类型的持续发射时间为 10s，信号种类标签为 0~11，包含共 12 种信号类型的样本数据，每个训练集文件由一系列时序数据点组成，每个数据点主要由六维特征参数描述，如表 1 所示，从左到右依次为时间戳 TOA、载频 RF、脉宽 PW、脉幅 PA、到达角 DOA、标签 ID。每个文件中只包含该类型无噪声纯净的单类信号（无混叠、丢失、错误及干扰）。

表 1 雷达脉冲描述字数据集组成

No	TOA/s	RF/MHz	PW/ μ s	PA/dB	DOA($^{\circ}$)	Label
1	3.3030859386	9618.00	8.63	-5.52	58.42	1
2	3.3031322860	9618.04	9.05	-4.13	58.16	1
3	3.3031778397	9616.63	8.86	-4.95	57.93	1
.....						

(2) 测试数据：测试数据集如图 4 所

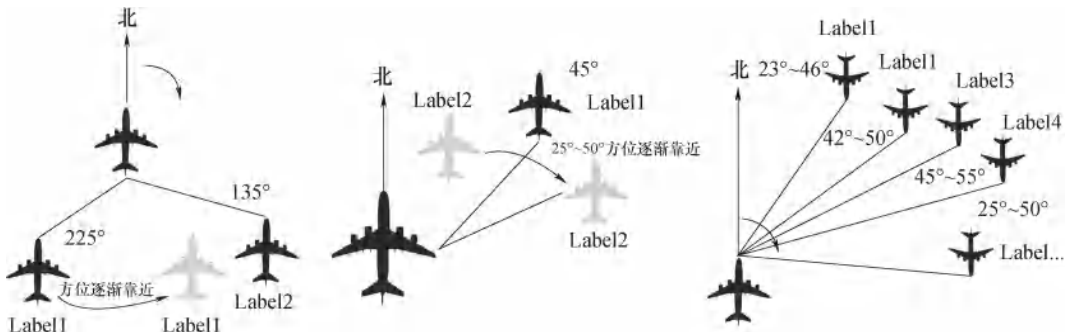


图 4 测试集场景示意图

示，共有简单、一般、复杂三个场景，每个场景中有若干个机载目标，雷达开/关时间各自独立，任意时段内会随机出现时、空、频多域混叠信号，其中包含若干训练集中已知的模板信号，测试集中存在噪声、参数测量误差及极少量参数错误情况，目标方位呈现固定或连续稳定变化。

共设置三种场景的验证数据，每种场景数据存为 1 个 .txt 文件，数据格式与训练数据相同。

实验的测试集有三个，分别验证在若干种混叠信号场景下的雷达分选性能，具体如下：

测试样本 1：4 种混叠信号，信号编号为 0、2、5、7 类型信号的混叠脉冲序列，共 999038 个测试样本。

测试样本 2：8 种混叠信号，信号编号为 0、1、2、4、5、6、7、8 类型信号的混叠脉冲序列，共 1762620 个测试样本。

测试样本 3：所有 12 种混叠信号，共 2579053 个测试样本。

3.3 实验结果与分析

根据前面所介绍的雷达信号分选的数据增强方法，本小节将介绍在复杂雷达脉冲信号分选场景下利用该深度学习网络模型进行识别的工作流程。

(1) 数据采集和预处理。从雷达接收机获取回波信号，转换为脉冲描述字 (PDW)，包括到达时间、工作频率、脉冲宽度、幅值和到达角。将数据划分为训练集和验证集，并进行归一化、去噪等预处理，提高数据质量。

(2) 数据增强。将预处理后的 PDW 数据输入数据增强模块。通过多尺度融合嵌入提取不同尺度的局部和全局特征，利用掩码增强技术随机掩蔽部分信号，模拟复杂电磁环境下的信号交织、丢失等情况，生成大规模、高质量、多样化的增强数据集。

(3) 特征提取和模型训练。将增强后的 PDW 数据输入时序卷积特征融合层提取深层次时频域特征，再输入 MLP 多层感知基因分类器预测雷达信号类别。基于预测结果和样本标签计算损失函数，通过反向传播算法更新模型参数，在验证集上评估模型性能，保存表现最佳的模型。

(4) 模型测试和评估。将训练好的模型应用于测试数据集，对给定窗口长度的脉冲信号序列进行分类，输出每个脉冲信号的标注结果。通过准确率、精确率、召回率等指标评估模型性能。

其中评价维度和指标如下：

信号提取标注准确率：计算所有正确分类的脉冲数量除以总脉冲数量。

信号提取标注精确率：计算每种信号类型的精确率，该类型预测 ID 正确的脉冲数/预测为该类型的脉冲总数，然后所有类型的精确率取平均值。

信号提取标注召回率：计算每种信号类型的召回率，该类型预测 ID 正确的脉冲数/该类型实际脉冲总数，然后所有类型的召回率取平均值。

本文选取了基于 Transformer 的结构和时序卷积结构作为基线，在同一测试集上

进行对比实验。此外，还评估了本文提出的多尺度融合嵌入网络 (Multi-scale Fusion and Masking Embedding Net, MFM-EmbNet) 模型的性能。各模型的识别效果如表 2 所示。

表 2 深度学习算法识别指标对比表

指标	Transformer	TCN 时序卷积	MFM-EmbNet
准确率 (%)	43.21	81.63	94.32
精确率 (%)	52.48	81.70	94.27
召回率 (%)	52.93	81.63	94.32

实验结果表明，MFM-EmbNet 在各项指标上都取得了最佳表现，证明了本文提出的数据增强方法和模型设计的有效性。特别是在低信噪比、信号交织严重的复杂场景下，MFM-EmbNet 展现出了显著的性能优势，体现了其良好的鲁棒性和泛化能力。

结果表明，本文提出的大模型启发增强的雷达数据增强方法，能够有效支撑深度学习模型在雷达信号分选任务中的应用。通过生成高质量、多样化的增强数据，能够训练出更加强健、鲁棒的识别模型，为复杂电磁环境下的信号处理提供可靠的解决方案。

由图 5 可见，本方法在多种雷达脉冲信号交错混叠的情况下表现也十分优秀。相比其他方法能够增强模型训练的稳定性和鲁棒性，从而达到提高模型预测准确性和泛化能力的目的。

实验结果表明，在 5dB 的信噪比场景下，基于算法生成的高质量训练集，模型能够取得 94% 的正确分选率。这一性能显著优于传统方法，证明了数据增强方法能够有效提升模型在复杂环境下的泛化能力。

此外，还探索了不同数据增强策略对模型性能的影响。通过对比实验，发现多

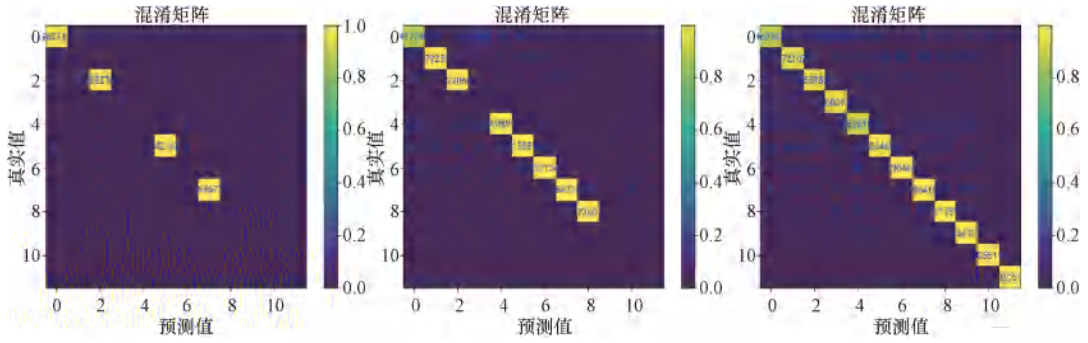


图5 分选混淆矩阵 (4、8 和 12 种混叠信号)

尺度融合嵌入和掩码增强的结合，能够最大限度地提高数据质量，为模型的训练提供了更加多样和鲁棒的样本。

3.4 消融对比实验

通过表 3 所示的消融实验可以验证所提方法中的数据增强以及掩码交织构建的有效性。其中对比的方法在同一种网络结构上进行，消融实验包括：是否使用所提多尺度融合嵌入方法，还是让网络自学习嵌入的特征表征层参数；是否使用掩码构建难样本交织的情形。结果表明，本文所提出的数据增强方法可以有效增强训练数据，有效提升雷达脉冲信号分选模型的鲁棒性。

表 3 消融实验指标对比表

指标	自学习嵌入+无掩码	多尺度融合嵌入+无掩码	多尺度融合嵌入+掩码 (本方法)
准确率 (%)	76.14	82.91	95.01
精确率 (%)	77.29	82.94	94.99
召回率 (%)	76.14	82.91	95.01

这些实验结果充分验证了数据增强方法在雷达信号分选任务中的有效性。我们相信，这一方法不仅可以推广到其他电磁信号处理任务，还能为电磁领域大模型的发展提供新的思路和实践基础。

4 结束语

本文针对大模型在复杂电磁环境下的数据需求，提出了一种创新的大模型启发增强的未知混叠雷达信号分选方法。该方法引入了多尺度融合嵌入和掩码增强技术，通过深度时序编码和复杂环境模拟，可以高效自动化地构建高质量、多样化的雷达信号分选数据增强集。实验结果表明，在包含 12 类雷达信号、不同信噪比场景的数据集上，MFM-EmbNet 模型取得了优异的分选性能，特别是在 5dB 的低信噪比环境下，正确分选率达到了 94%，显著优于传统方法。这证明了数据增强方法能够有效提升模型在复杂环境下的泛化能力。然而，研究仍存在局限性，如模型的计算复杂度较高，在实时处理多通道、大规模的数据时可能面临挑战。未来将开展针对电磁领域基础大模型的异构数据嵌入方法等相关的支撑技术研究。

参考文献

1 CHANG Y, WANG X, WANG J, et al. A survey on evaluation of large language models [J]. ACM Transactions on Intelligent Systems and Technology, 2024, 15 (3): 1-45.

- 2 YIN S, FU C, ZHAO S, et al. A survey on multimodal large language models [J]. arXiv preprint arXiv: 2306.13549, 2023.
- 3 JIN M, WEN Q, LIANG Y, et al. Large models for time series and spatio-temporal data: A survey and outlook [J]. arXiv preprint arXiv: 2310.10196, 2023.
- 4 SHAO J, TONG J, WU Q, et al. WirelessLLM: Empowering Large Language Models Towards Wireless Intelligence [J]. arXiv preprint arXiv: 2405.17053, 2024.
- 5 DOBRE O A, ABDI A, BAR-NESS Y, et al. Survey of automatic modulation classification techniques: classical approaches and new trends [J]. IET communications, 2007, 1 (2): 137-156.
- 6 GUPTA P, JAIN P, KAKDE O G. Deep Learning Techniques in Radar Emitter Identification [J]. Defence Science Journal, 2023, 73 (5).
- 7 ZHENG S, CHEN S, QI P, et al. Spectrum sensing based on deep learning classification for cognitive radios [J]. China Communications, 2020, 17 (2): 138-148.
- 8 ZHANG C, PATRAS P, HADDADI H. Deep learning in mobile and wireless networking: A survey [J]. IEEE Communications surveys & tutorials, 2019, 21 (3): 2224-2287.
- 9 KULIN M, KAZAZ T, MOERMAN I, et al. End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications [J]. IEEE access, 2018, 6: 18484-18501.
- 10 O'SHEA T J, ROY T, CLANCY T C. Over-the-air deep learning based radio signal classification [J]. IEEE Journal of Selected Topics in Signal Processing, 2018, 12 (1): 168-179.
- 11 ZERVEAS G, JAYARAMAN S, PATEL D, et al. A transformer-based framework for multivariate time series representation learning [C] //Proceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining. 2021: 2114-2124.
- 12 ZHOU H, ZHANG S, PENG J, et al. Informer: Beyond efficient transformer for long sequence time-series forecasting [C] //Proceedings of the AAAI conference on artificial intelligence. 2021, 35 (12): 11106-11115.
- 13 隋金坪, 刘振, 刘丽, 等. 雷达辐射源信号分选研究进展 [J]. 雷达学报, 2022, 11 (3): 418-433.
- 14 FARAHANI A, VOGHOEI S, RASHEED K, et al. A brief review of domain adaptation [J]. Advances in data science and information engineering: proceedings from ICDATA 2020 and IKE 2020, 2021: 877-894.
- 15 SUN J, XU G, REN W, et al. Radar emitter classification based on unidimensional convolutional neural network [J]. IET Radar, Sonar & Navigation, 2018, 12 (8): 862-867.
- 16 LIN A, MA Z, HUANG Z, et al. Unknown radar waveform recognition based on transferred deep learning [J]. IEEE Access, 2020, 8: 184793-184807.
- 17 QU Z, WANG W, HOU C, et al. Radar signal intra-pulse modulation recognition based on convolutional denoising autoencoder and deep convolutional neural network [J]. IEEE Access, 2019, 7: 112339-112347.
- 18 QIU X, SUN T, XU Y, et al. Pre-trained models for natural language processing: A survey [J]. Science China Technological Sciences, 2020, 63 (10): 1872-1897.
- 19 DEVLIN J, CHANG M W, LEE K, et al. Bert: Pre-training of deep bidirectional transformers for language understanding [J]. arXiv preprint arXiv: 1810.04805, 2018.
- 20 HE K, CHEN X, XIE S, et al. Masked autoencoders are scalable vision learners [C] //Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2022: 16000-16009.
- 21 LANG P, FU X, MARTORELLA M, et al. A comprehensive survey of machine learning applied to radar signal processing [J]. arXiv preprint arXiv: 2009.13702, 2020.

大模型驱动多智能体的军事需求生成框架

李嘉晖¹ 张萌萌¹ 陈洪辉¹

摘要 联合作战军事需求生成多依赖人为经验且多来源文档，在面对视频、音频等多模态信息时，难以快速有效处理。此外，军事需求生成过程对军事专家的水平要求较高，完备性、精准性难以保证。上述问题直接影响军事需求的生成效率和作战体系的设计质量，因此需要创新军事需求生成方法。文章参考学术界提出的大模型驱动多智能体协作的思路，在军事需求生成领域引入多智能体技术，以改善大模型实际应用问题，模拟人类在解决复杂问题时的决策过程。

首先，文章构建了一个多智能体协作框架，旨在模拟军事需求生成流程中的各个模块。设计的框架包含三个主要模块：用户输入模块、多智能体模块和工具包模块。每个模块的设计思路如下：①用户输入模块负责确定系统目标和输入多模态信息资源，为框架运作提供数据基础。②多智能体模块是框架的核心，由若干智能体组成，智能体通过大模型驱动实现协同工作，共同完成多模态信息获取、模拟专家讨论和生成需求清单等任务。③工具包模块为智能体提供辅助功能，强化智能体在特定领域的能力。该模块包含开源论文库工具、多模态信息处理工具和搜索引擎工具等，智能体由大模型驱动自主选择其中的工具完成任务。

其次，文章采用 Langchain 框架构建多智能体系统，设计了三种类型的智能体：多模态信息获取智能体、军事专家智能体和军事数据分析智能体。框架中各个智能体的设计思路如下：①多模态信息获取智能体：集成了多模态处理工具，能够对视频、音频及文本等多模态数据进行综合处理。借助大型语言模型，该智能体能够深入理解多模态信息内容，并实现对信息的逻辑推理与分析。此外，该智能体还具备思维和记忆功能，能够与用户围绕多模态信息内容进行问答交互。②军事专家智能体：接入互联网搜索引擎工具，能够获取军事领域新闻资讯，并根据新闻资讯产生观点。接入开源论文库，利用大模型理解文献内容，掌握关于军事战略、战术、武器系统等方面的知识。③军事数据分析智能体：接入开源论文库，具有检索和分析开源论文的能力。集成专业搜索引擎和数学工具，在面对搜索任务时，能够迅速识别问题需求，对数据内容表现出高度的敏感性，并能够直接进行数据运算，得出精确的结论。

最后，文章通过实验验证多智能体军事需求生成框架的有效性。在基于多智能体框架的需求生成过程中，用户只需要输入系统目标，提供多模态信息资源，多智能体框架就能利用大模型自动生成提示词，智能体在提示词的驱动下自主调用工具进行协作，最终完成用户设定的目标。实验结果表明，相比传统需求生成方法，该框架显著提升了需求生成的效率，优化了人工操作的时间成本，在处理不同长度的视频和音频资源时，能够节省 80%~95% 的耗时，体现了框架在智能化军事需求生成方面的巨大潜力和实用价值。

关键词 需求生成，多智能体，生成式人工智能，大模型，多模态

1. 国防科技大学信息系统工程全国重点实验室

1. National Key Laboratory of Information Systems Engineering

A Framework for Multi-agent Military Requirement Generation Driven by Large Language Models (Extended Abstract)

LI Jia-Hui¹ ZHANG Meng-Meng¹ CHEN Hong-Hui¹

Abstract The generation of military requirements for joint operations heavily relies on human experience and documents, which struggles to effectively process multi-modal information, such as video and audio. Moreover, the process demands a high level of expertise from military professionals, making it difficult to ensure completeness and precision. These issues directly impact the efficiency of military requirement generation and the quality of combat system design, necessitating innovative approaches to requirement generation. This research draws on the concept of LLMs-driven multi-agent collaboration and introduces multi-agent technology into the field of military requirement generation to address practical application issues of LLMs and simulate the decision-making process of joint operations.

Firstly, this research constructs a multi-agent collaboration framework aimed at emulating the various modules involved in the military requirement generation process. The designed framework consists of three main modules: the User Input Module, the Multi-Agent Module, and the Toolkit Module. The design philosophy of each module is as follows: ①The User Input Module is responsible for defining system objectives and inputting multi-modal information resources, providing a data foundation for the framework's operation. ②The Multi-Agent Module is the core of the framework, composed of several agents that work collaboratively under the drive of LLMs to jointly accomplish tasks such as multi-modal information acquisition, simulation of expert discussions, and generation of requirement lists. ③The Toolkit Module provides auxiliary functions for agents, enhancing their capabilities in specific domains. This module includes tools such as the arXiv API, multi-modal information processing tools, and search engine tools, which agents can autonomously select to complete tasks.

Secondly, this research employs the Langchain framework to construct the multi-agent system, designing three types of agents: Multi-modal Information Acquisition Agent, Military Expert Agent, and Military Data Analysis Agent. The design philosophy of each agent in the framework is as follows: ①Multi-modal Information Acquisition Agents: Integrated with multi-modal processing tools, the agent can comprehensively process multi-modal data such as video, audio, and text. With the aid of LLMs, these agents can understand the content of multi-modal information and perform logical reasoning and analysis. Additionally, the agent possesses thinking and memory capabilities, enabling it to engage in question-and-answer interactions with users regarding multi-modal information content. ②Military Expert Agent: Connected to search engine tools, the agent can learn military domain news and generate viewpoints. It also has access to arXiv, using LLMs to comprehend literature content and gain knowledge about military strategy, tactics, and weapon systems. ③Military Data Analysis Agent: With access to arXiv API, the agent has the ability to retrieve and analyze open access papers. Integrated with professional search engines and mathematical tools, the agent can quickly identify the requirements of search tasks, exhibits high sensitivity to data content, and directly performs data computations to reach precise conclusions.

Finally, this research validates the effectiveness of the multi-agent military requirement generation framework through an experiment. The experimental results demonstrate that when the multi-modal information capacity is within the maximum processing capacity of LLMs, the framework significantly reduces the time consumption for military requirement generation, with video resource time savings accounting for 80% to 85%, and audio resource time savings ranging from 90% to 95%.

Key words requirement generation, multi-agent, generative AI, LLMs, multi-modal

大模型在陆战兵棋推演中的应用研究**

刘大勇¹ 董志明¹ 刘倬立¹ 邱雪欢¹ 冯琦琦¹

摘要 随着人工智能技术的快速发展,特别是大语言模型(Large Language Model, LLM)和多模态大模型的兴起,其在军事领域的应用逐渐成为研究热点。兵棋推演作为辅助指挥决策、指挥对抗训练的重要工具,与大模型的结合展现出巨大的潜力和创新空间。在总结2年来大模型在兵棋推演中的应用现状的基础上,进一步探讨了大模型在陆军战术兵棋推演想定生成、导调管理、人机对抗、智能体建模与训练等方面的应用框架和应用前景,给出基于大模型的AI Agent的通用开发流程,为推动大模型在兵棋推演中的深度应用提供了启示和借鉴。

关键词 陆战兵棋, 想定生成, 智能体建模, 大模型

Research on the Application of Large Models in Army Tactical Chess Simulation**

LIU Da-Yong¹ DONG Zhi-Ming¹ LIU Zhuo-Li¹ QIU Xue-Huan¹ FENG Qi-Qi¹

Abstract With the rapid development of artificial intelligence technology, especially the rise of Large Language Model (LLM) and multimodal large models, their application in the military field has gradually become a research hotspot. As an important tool for deducing complex situations, assisting command decision-making, and conducting training, the combination of military chess deduction with large models demonstrates enormous potential and innovative space. On the basis of summarizing the current application status of large models in military chess deduction in the past two years, this paper further explores the application framework and prospects of large models in army tactical chess deduction scenario generation, guidance management, human-machine confrontation, intelligent agent modeling and training, and provides a rough development process of AI Agent based on large models, providing inspiration and reference for expanding the deep application of large models in military chess deduction.

Key words army tactical chess, scenario generation, intelligent agent modeling, LLM

** 军队高层次人才创新工程项目资助

** Supported by Military High level Science and Technology Innovation Talent Project

1. 陆军装甲兵学院

1. Army Academy of Armored Forces

0 引言

兵棋推演作为模拟真实战争、推演复杂局势、辅助指挥决策的重要工具，在现代战争中扮演重要角色。同时作为一种训练手段，计算机兵棋推演对于提高和扩展高级指挥与决策人员的战略思维与决策能力能收到事半功倍的效果^[1]。至 20 世纪 50 年代萌芽的人工智能技术已经促进了兵棋的发展，但这两年爆火的大模型所具有的语义理解、人机对话、海量知识融合、多场景泛化等强大能力，必将为兵棋推演带来前所未有的重大变革。

为了推动大模型在兵棋中的深度应用，本文着眼兵棋推演需求和大模型突出功能，提出了大模型在兵棋推演中的 4 个应用方向，设计了以大模型为核心的 AI Agent 的构建流程。

1 陆战兵棋环境介绍

陆军战术兵棋是一种模拟陆域旅级规模以下兵力对抗的严肃游戏，通过模拟战场环境、兵力部署、作战行动等，帮助指挥员进行作战方案验证、指挥训练。

1.1 兵棋系统要素构成

兵棋通常包含以下几个核心要素：

(1) 地图与地形。兵棋推演通常在一个模拟的地图上进行，这张地图会详细标注各种地形特征，如居民地、林地、河流等。地形对战斗行动有着重要影响，如起伏地可能会影响部队的行进速度和通视，而河流影响机动路线的选择，如图 1 所示。

(2) 兵力配置。在兵棋推演开始之前，需要根据研究问题的需要为红蓝双方设计兵力构成、部署情况，并在地图上配

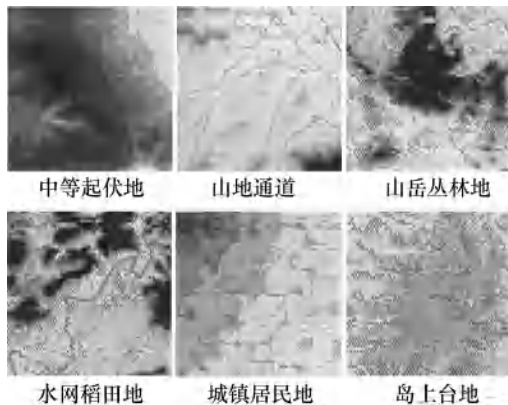


图 1 兵棋系统的地形环境

置各自的兵力。这包括不同类型的作战单位，如步兵、装甲兵、炮兵等，每个单位都有其特定的战斗能力。

(3) 武器装备。不同的作战单位会配备不同的武器装备，这些装备在推演中会影响到单位的战斗效能。例如，装备有先进武器的单位可能在战斗中占据优势。

(4) 作战规则。兵棋推演有一套详细的规则，详细规定了每种算子的机动速度、观察规则、携带武器、射击条件等。这些规则确保了推演的公平性和客观性。

(5) 裁决机制。在推演过程中，需要有一个裁决机制来判断各方的行动是否有效，以及战斗的结果如何，通常由兵棋系统本身来完成。

(6) 态势数据输出和智能体操控接口。现代兵棋系统都预留了态势输出和智能体操控接口。兵棋系统的智能操控接口是兵棋推演系统中关键的一部分，它允许开发者或智能体 (AI) 通过特定的接口与兵棋推演环境进行交互，实现智能决策和行动控制。态势输出接口，用于查询战场态势，以便智能体据此做出决策。态势信息可能包括算子状态、夺控点状态、双方比分等。例如：“庙算”兵棋系统通过 step 函数可以获取每一步的 Observation 信息，如图 2、图 3 所示。



图2 兵棋推演开局态势

```

observation = {
  "actions": [], # 上一步接收到的动作
  "cities": [], # 各个坐标点的信息
  "communication": [], # 通信相关信息
  "jm_points": [], # 侦察点信息
  "judge_info": [], # 裁决信息
  "landmarks": {}, # 地标信息, 雷场, 障碍
  "operators": [], # 算子信息
  "passengers": [], # 乘客信息
  "role_and_grouping_info": {}, # 编队信息和编队信息
  "scenario_id": 0, # 想定ID
  "scores": {}, # 分数
  "terrain_id": 0, # 地图id
  "time": {}, # 时间信息
  "valid_actions": {} # 当前态势下的可操作动作信息
}

```

图3 “庙算”平台态势输出口信息

机动

```

{
  "actor": "int 动作发出者编号",
  "obj_id": "算子ID int",
  "type": 1,
  "move_path": "机动路径 list(int)"
}

```

打击

```

{
  "actor": "int 动作发出者编号",
  "obj_id": "攻击算子ID int",
  "type": 2,
  "target_obj_id": "目标算子ID",
  "weapon_id": "武器ID int"
}

```

上车

```

{
  "actor": "int 动作发出者编号",
  "obj_id": "乘坐算子ID int",
  "type": 3,
  "target_obj_id": "车辆算子ID"
}

```

图4 兵棋系统的命令操控接口等问题。

命令输入接口，用于控制算子（如部队、武器系统等）的行动，这是智能体唯一可以控制兵棋算子的接口，如图4所示。有的兵棋系统还为开发者提供了部分分析功能，辅助开发者快速完成开发，包括态势分析、战术评估等，开发者利用这些工具可以加速智能体的开发。

1.2 传统兵棋推演面临的矛盾问题

然而，传统的陆军战术兵棋推演存在主要依赖人员操控、对操作人员要求较高、组织耗时费力、沉浸感和逼真度不高

(1) 对操作人员技术水平要求较高。兵棋推演要求操作人员具备丰富的军事知识、战略思维能力和决策能力。同时，随着兵棋推演技术的不断发展，操作人员还需要掌握相关的计算机软件和模拟工具的使用方法。这对操作人员的综合素质提出了较高的要求。由于兵棋推演涉及多个学科领域的知识和技能，因此，具备全面素质的专业人才相对短缺。这在一定程度上限制了兵棋推演技术的推广和应用。

(2) 智能体智能水平不高。当前智能体智能水平不高的现状主要体现在其在实际应用中的局限性,如决策能力有限、环境适应性差、学习速度慢等方面。导致这种现状的原因可以从技术、数据、算法以及应用场景等多个维度进行深入分析。从智能体建模方法看,无论是基于知识/规则的智能体,还是基于深度强化学习构建的智能体,还是基于部分优化算法构建的智能体,在特定任务上表现优异,但在面对新任务或新环境时,其泛化能力不足,限制了智能体应用的灵活性和适应性。从算法上看,常规小模型在面对复杂的推理逻辑、态势图认知上,基本上能力很弱或几乎没有能力,不能做到像人一样对敌我双方的态势有整体、宏观的理解和认识。从算力上看,虽然硬件在不断发展,但对于兵棋推演来说,推演一局耗时仍然较长,深度强化学习模型需要推演百万局以上才能见到效果,对于群队级智能体不容易收敛;从数据上看,对于操控小规模算子的智能体,因为奖励稀疏也很难收敛。

(3) 推演自动化程度不高。从想定生成看,目前主要是人为设计、手工编辑,由于推演想定包括推演条件、红蓝双方企图、双方兵力编成、初始态势、战果计算方式等内容要素,编制并录入兵棋系统中,且受到想定编制人员水平的限制,为了保证想定质量往往进行多轮研讨、反复修订完善,耗费时间较长,影响推演效率。对于作战方案计划的制订与评估,仍然需要人工手动把作战方案转换成兵棋系统可识别的数据、代码,需要手动对不同的作战方案进行分析、比较、评估和完善,图形化、可视化、智能化水平不高。对于推演报告的生成,目前仍然采取让专业的推演人员在推演结束后按照一定的模

板手工编辑的办法。

为了提高兵棋推演的效果和质量,这些问题必须得到解决。大模型的出现,为解决上述问题提供了可行途径。

2 大模型在兵棋推演中应用现状

目前,大语言模型在军事对抗推演中的应用尚处于起步探索阶段,公开的案例较少。

美国罗格斯大学的华文越等从兵棋推演的角度,通过模拟“一战”、“二战”和中国战国时期的战争,研究利用大语言模型驱动的智能体来模拟战争方法和技术,验证了基于大语言模型的多智能体在战争推演方面的能力^[2]。

知乎的 Alexander Cheung 利用 GPT 4.0 和 Bing AI 等大语言模型开展美军西太平洋反航母作战兵棋推演。推演过程中, AI 根据输入的详细任务简报和背景信息,生成了完整的作战方案,并对方案中的漏洞进行了自查和改进。这种基于 LLMs 的作战规划决策方式,不仅缩短了筹划时间,还提高了方案的可行性和有效性^[3]。

南京大学智能装备新技术研究中心的研究团队提出了一种基于大语言模型的双层 Agent 任务规划方法。该方法将大语言模型置于决策中心,通过自然语言的交互发出和执行决策指令,并通过兵棋推演模拟环境进行仿真验证^[4]。实验结果表明,大语言模型的智能决策能力明显优于常用的强化学习 AI,且其智能性和可理解性更强。这一研究为兵棋推演的智能化发展提供了新的思路和方法。

上述 3 个案例,均将大语言模型作为决策 Agent 的引擎。前两个案例,仅仅基于纯大语言模型作为推理 Agent,案例 3 在大语言模型的基础上,基于 Lilian Weng 的

Agent 架构^[5]进行了智能体的开发,提高了推演的逼真度和复杂度。

3 大模型在兵棋推演中的应用方向探析

下面,从“需求牵引+技术推动”的角度,以兵棋推演面临的最大挑战和大模型最擅长的功能的交集为重点,分析大模型赋能兵棋推演的着力点。

3.1 应用总体架构

大模型赋能的兵棋推演系统是一个高度智能化的作战模拟与决策支持系统,旨在通过融合先进的人工智能大模型技术,提升兵棋推演的自动化和智能化水平。系统通过构建多层次、模块化的架构,使最基础的算力、数据升华为服务战斗力的各项服务,具体可分为基础层、资源层、平台层、能力层、应用层,如图5所示。

(1) 基础层。基础层是整个系统的基

石,提供了系统运行所必需的基础设施和技术支撑。包括:①高性能计算服务器、存储设备等硬件设施,为系统提供强大的数据处理和存储能力。②操作系统与中间件,支持系统的稳定运行和模块间的通信与协作。③网络环境,确保系统内部以及系统与外部数据源之间的高效数据传输。

(2) 资源层。资源层整合了各类数据资源和知识库,为兵棋推演提供丰富的信息输入。

(3) 平台层。主要包括大模型平台、通用模型平台、知识平台和基于大模型的兵棋推演服务平台,为兵棋推演提供兵棋推演引擎,以及微调好的并外挂知识库的大模型,为推演仿真提供平台支撑。

(4) 能力层。能力层是系统功能的直接体现,瞄准最终应用,在平台层的基础上,通过封装和整合平台层的技术和工具,形成一系列具有实际应用价值的能力。可以构建并训练智能体,依托大模型以及训练好的智能体,进行想定的自动生



图5 基于大模型的兵棋系统总体架构

成导入、人人/机机/人机混合对抗、辅助制订作战方案并评估、自动生成推演报告等。

(5) 应用层。应用层是系统与用户之间的接口，通过提供直观、易用的操作界面和丰富的功能模块，实现基于兵棋推演的作战方案验证与优选、战术战法创新实验、指挥对抗训练、装备效能论证等活动，赋能战斗力提升。

3.2 想定生成

想定是兵棋推演的基础，它定义了推演的环境、条件、参与方和初始态势等。传统上，想定生成依赖于人工编写，这不仅耗时费力，还难以覆盖所有可能的战争场景。而大模型可以根据历史战争数据、战略研究报告等素材，自动生成多样化的想定，可丰富兵棋推演的场景库。大语言模型在辅助想定生成方面的应用可以从以下方面探索：

(1) 生成基于历史战争的想定。通过输入历史战争的数据和背景信息，模型可

以模拟出类似的历史战争场景，为兵棋推演提供逼真的环境。这种基于历史的想定不仅可以帮助参训人员更好地理解 and 应对历史战争中的挑战，还可以作为检验战略和战术有效性的重要工具。

(2) 生成更加贴近实战的情况想定。为了激发参训人员的应变能力和创新思维，常常需要设计一些打破常规、让推演人员意想不到的战争场景。大模型的创新指标可以调整，可以根据输入的关键词和约束条件，生成如贝卡谷地空袭这样的开创性的对抗策略，对于培养参训人员的创新能力、开拓思维具有重要意义。

(3) 定制化生成想定。例如，推演人员可以指定想定的地幅大小、时间范围、双方兵力对比等要素，大模型则根据这些要素生成符合要求的想定，见图6。这种定制化的生成方式可以确保生成的想定更加符合推演要求。以2022年俄罗斯攻占乌克兰安东诺夫机场为例，可以让大模型参照这场战斗生成多个类似想定，便于军事人员研究。

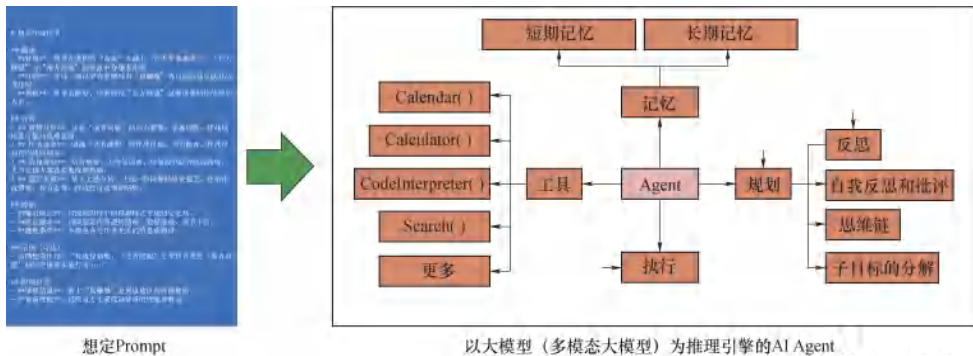


图6 定制化想定生成

3.3 导调管理

在兵棋推演过程中，导调员负责控制推演的节奏、调整规则、解释结果等。这是一个复杂而重要的任务，需要导调员具备丰富的专业知识和敏锐的洞察力。而大

语言模型可以作为导调员的辅助工具，提供实时的数据分析和建议，从而减轻导调员的工作负担并提高推演的效率和质量。

(1) 大模型可以实时分析推演数据并提供建议。在兵棋推演过程中，会产生大量的数据和信息，包括各方的行动、战场

态势的变化等。大语言模型可以实时分析这些数据,识别出重要的趋势和模式,并为导调员提供有针对性的建议。例如,当推演中出现意外情况时,模型可以快速分析原因和影响,为导调员提供决策支持。

(2) 大模型可以根据推演进度和参与者的反馈动态调整规则。在兵棋推演中,有时候需要根据实际情况对规则进行调整以确保推演的公平性和有效性。大语言模型可以根据推演进度和参与者的反馈实时分析规则的有效性,并为导调员提供调整建议。这种动态调整规则的方式不仅提高了推演的灵活性,还使得推演更加贴近实际情况。

(3) 大模型可以提供解说和报告生成。在兵棋推演中及结束后,导调员需要对推演过程和结果进行解释和说明,以帮助参与者理解推演过程和结果。特别是,大模型基于强大的自然语言组织能力,可以根据推演数据和规则生成详细的解释和说明报告,包括各方的行动、战场态势的变化、推演结果的原因等。该项应用可以将兵棋推演组织人员从报告的制定者变成报告的审阅者,可有效提高效率、减轻工作负担。

3.4 人人/机机/人机混合对抗

兵棋推演涉及多种对抗模式,包括人与人、人与机器、机器与机器以及人机混合对抗。这些对抗模式对于检验战略和战术的有效性、培养参训人员的实战能力具有重要意义。而大语言模型在这些对抗模式中发挥着关键作用,为兵棋推演提供了更加逼真和多样化的对抗体验。

(1) 在人机对抗中,大语言模型可以充当蓝方,模拟敌方指挥官的思维和决策过程。通过输入敌方的战略意图、兵力部署等信息,模型可以生成符合敌方指挥员思维模式的行动和决策。这种模拟不仅提高了人机对抗的逼真度,还使得参训人员

能够更好地了解和应对敌方的战略和战术。

(2) 在机机对抗中,大语言模型可以生成复杂的战术和战略方案。通过输入战场态势、兵力部署等信息,模型可以生成多种可能的战术和战略方案,并评估它们的优劣和可行性。这种机机对抗不仅检验了不同算法和策略的有效性,还为战略决策提供了重要的参考。

(3) 在人机混合对抗中,大语言模型可以作为人类参与者的智能助手。通过输入人类参与者的战略意图和行动计划,模型可以生成实时的战略建议和数据分析报告。这种人机混合对抗不仅提高了人类参与者的决策效率和质量,还使得他们能够更好地利用数据和模型进行战略决策。

3.5 决策 Agent 构建和训练

兵棋推演中的智能体需要具备高度的自主性和适应性,以便在复杂的战争环境中做出合理的决策。智能体的决策建模,其实质是模拟人类在 OODA 环的观察、判断、决策过程,需要进行态势初加工、态势理解、态势预测、制定策略等活动,生成具体行动指令等决策产物。

1. 传统决策 Agent 构建范式

目前,战术智能体主要有两种主流的建模范式,如图 7 所示。①基于知识/规则的建模范式,主要是利用有限状态机(Finite State Machine, FSM)、行为树(Behavior Tree, BT)等方法,将人类专家的研究形成的战术战法编程形成计算机代码,或将人类专家的知识经验、战术战法建模形成知识图谱或规则库。优点是可解释性强、推理速度快,难点是对于作战这种大规模、复杂决策空间的复杂系统,由于人类本身对其机理认识不够完全透彻,先期形成的知识经验并不完备,同

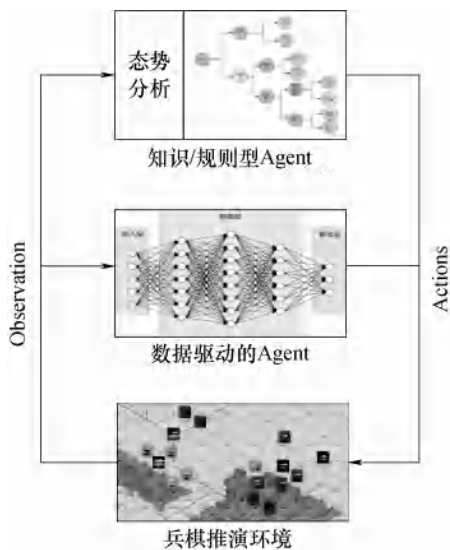


图7 两种传统决策 Agent 构建范式

时由于战争的艺术性，这种固化的知识经验有较大的局限性，在人类选手千变万化甚至是灵光一现、神来之笔的策略面前往往胜算不大。②基于深度强化学习（DRL）的建模范式，让智能体在与战场环境交互中进行试错学习和最优控制，以获得最优的奖励为目标，从而不断优化策略网络参数。常用的算法有单智能体深度强化学习（Deep Reinforcement Learning, DRL）和多智能体

深度强化学习（Multi-Agent Deep Reinforcement Learning, MADRL）。目前存在的问题主要是陆域战术对抗问题状态空间和动作空间巨大，训练时如果训练轮次达不到一定数量很难收敛，目前基于单智能体的深度强化学习研究和训练实践比较丰富，基于多智能体的实践比较缺乏。

2. 基于大模型的决策型 Agent 建模范式

自大模型诞生后，目前最有潜力的是基于大模型推理引擎的 Agent 的建模范式。实验结果表明，大语言模型的宏观决策能力、稳定性和泛化性明显强于强化学习 AI，而且其智能性、繁华性都更出色。表 1 为三种兵棋 Agent 构建范式的比较。

3. 融合型构建范式

从表 1 可以看出，每种智能体构建范式均有各自的优缺点，必须将各种建模方式结合起来，采用融合型构建范式，才能开发出泛化能力强、智能水平高的智能体。图 8 是决策树和大模型融合的智能体构建原理。

表 1 三种兵棋决策 Agent 构建范式优缺点比较

构建范式	优点	缺点	常用模型
基于知识/规则	可解释性强、推理速度快	编程工作量大，基本不具备学习能力，通常与想定紧耦合，智能水平上限难以突破	FSM、BT
基于单智能体深度强化学习/多智能体深度强化学习	探索能力强，更容易找到最优策略，具有一定学习能力	泛化能力弱，对于奖励稀疏问题、状态空间和搜索空间较大的问题，很难收敛	PPO、TRPO、MADDPG
基于 LLM+RAG+知识图谱构建的 AI Agent	泛化能力强，宏观决策能力强	推理速度慢，微观决策能力弱	GPT3.5、GPT4.0, ReAct 框架

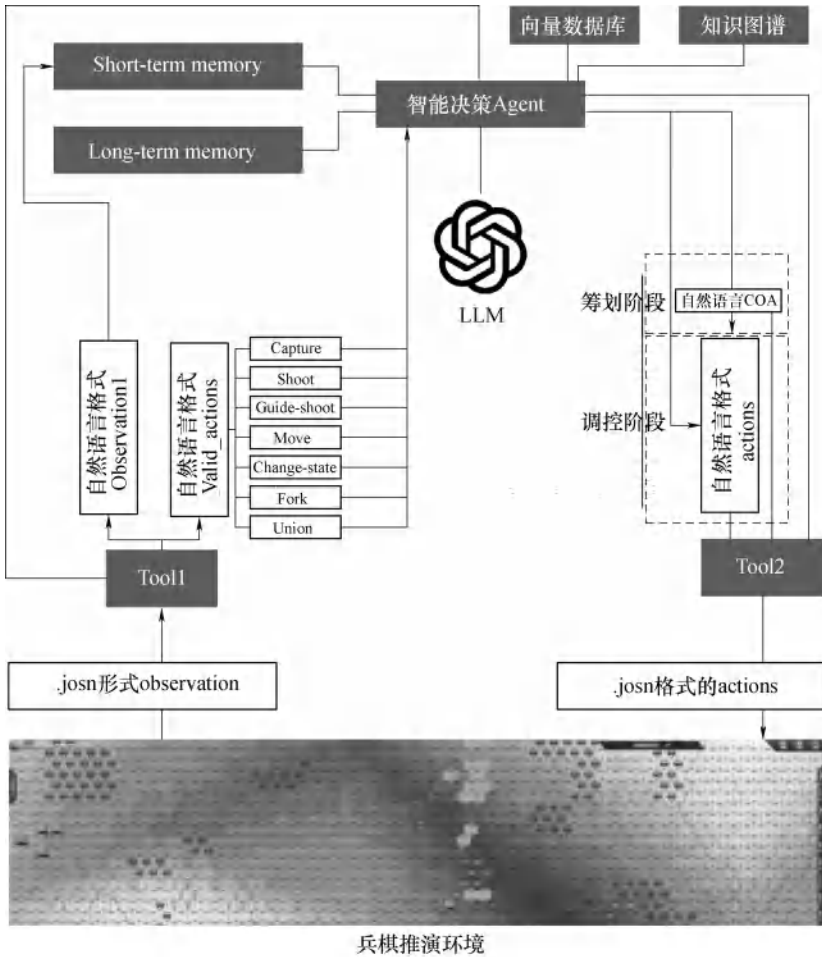


图 8 决策树和大模型融合构建智能体原理

4 兵棋推演大模型和 AI Agent 构建流程

将大模型用于兵棋推演，需要做一些工作，且针对每种功能，需要构建专门的基于大模型内核的 AI Agent，如想定生成 AI Agent、导调 AI Agent。

其构建流程如图 9 所示，具体为：

(1) 选择开源大模型（国内 GLM、Baichuan、Yi、Qwen 系列，国外的 llama3 系列）作为待训练的军事大模型。

(2) 准备军事领域无监督数据集，对选定的预训练大模型，使用预训练工具，如红山开源社区发布的卓识 LLM_Factory，训练行业大模型。

(3) 搜集兵棋推演领域的各种知识、数据，准备 8000~10000 个问答对作为微调数据集，对上面的军事大模型进行微调。

(4) 构建兵棋推演有关各种类型知识（如事实、规则、概念等），按照构建知识库、知识抽取、向量化表示、向量归一化与相似度计算、存储与索引构建、接口设计、支持迭代与优化的流程步骤构建

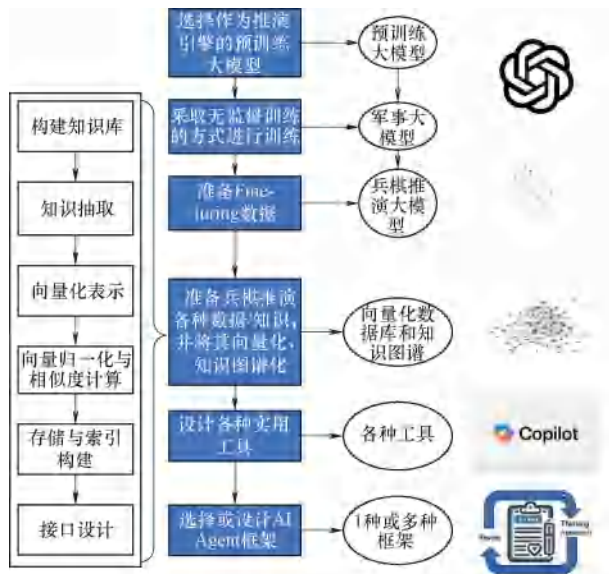


图9 兵棋推演 AI Agent 构建流程

向量化知识库，给大模型提供代 RAG 检索的对象。

(5) 设计或选取各种工具，会调用工具是实现大模型功能扩展的关键。比如，在兵棋推演中，编制 1 个小工具 (Tool) 就可以将 .json 格式的态势数据转变为自然语言格式的态势数据。

(6) 选择 Agent 技术框架。目前，一般选择 Lilian Weng 发表的博文“LLM Powered Autonomous Agent”中给出的包含规划 (Planning)、记忆 (Memory)、工具 (Tools)、执行 (Action) 四大要素的 Agent 架构为起点，设计自己的 Agent 架构。

(7) 编程实现。

5 面临的挑战

尽管大模型在兵棋推演中展现出巨大的应用潜力，但其与兵棋系统的深度融合

仍面临诸多挑战。

(1) 军事大模型的构建。首先，数据获取是一大难题，由于军事领域的特殊性，高质量、合法的训练数据获取难度较大，这直接影响了模型的训练效果和泛化能力。其次，战争场景复杂多变和决策的敏感性，对模型的实时性和准确性提出了极高要求，如何确保模型在复杂战争环境中依然能做出正确决策是一大挑战。此外，军事大模型的研发和应用还涉及伦理、法律等社会问题，如何在确保技术领先的同时，遵守相关国际法和道德标准，也是构建军事大模型时必须考虑的问题。

(2) 适应性的挑战。兵棋系统本身的复杂性和多样性也对大模型的适应性提出了更高要求。不同的兵棋系统可能具有不同的规则、实体和交互方式，而大模型需要能够适应这些差异并进行有效的推演。此外，随着战场环境的不断变化和作战任务的多样化，大模型还需要具备持续学习

和优化的能力。

(3) 闭源数据的挑战。目前军事领域的大模型都是基于开源数据进行的预训练和微调,虽然可以达到一定的智能程度,对于开展研究甚至进行一般的指挥是没有问题的,但是如果站前用于作战方案推演、充当蓝军对手,以及开展作战概念开发等,必须有内部闭源的数据和知识用于对大模型进行微调或进行 RAG 数据库构建。

(4) 大模型“幻觉”带来的可解释性难题。大语言模型的行为由训练数据决定,其技术复杂性和不透明性造成了“黑箱”问题,使用者可能始终无法完全信任其输出的结果,存在人机信任问题和挑战。在兵棋推演中,这一问题将更加凸显,尤其是在进行方案推演时,如果大模型给出的结论或建议不能很好地“说明白”,指挥员是不可能冒较大风险采纳的。

(5) 利用经验和要求创新的平衡难题问题。由于战争指挥是一门创新性的艺术,要求指挥员打破常规,创新战法打法,只有这样才能立于不败之地。但兵棋推演大模型是对人类已有、已经发生的战役战斗的策略、战术的压缩,本身并不会进行创新,并且这种创新不是无原则、无根据的创新,不能像设置 ChatGPT 温度 (temperature) 参数一样来间接影响输出结果的创新性,而必须寻求大模型技术的突破。

6 结束语

大模型在兵棋推演中的应用正处于快

速发展阶段,其在想定生成、人机对抗、智能体建模与训练等方面展现出巨大的应用潜力。为了推动大模型与兵棋系统的深度融合,未来研究应重点关注以下几个方面:首先,需要探索更加高效的大模型建设和训练方法,降低其成本并提高其可用性。其次,需要研究大模型与兵棋系统的接口和交互方式,实现两者的无缝连接和有效协同。此外,还需要开展针对大模型的兵棋推演实验和评估工作,验证其在实际应用中的效果和性能。最后,还需要关注大模型的安全性和可靠性问题,确保其在实际应用中不会对军事行动造成负面影响。

参考文献

- 1 张斌,张跃. 外军、台军兵棋推演的做法及启示 [J]. 军事学术, 2006369 (12): 73-74.
- 2 HUA W, FAN L, LI L. War and Peace (WarAgent): LLM - based Multi - Agent Simulation of World Wars [DB/OL]. (2024-01-30) [2024-06-30]. <https://arxiv.org/abs/2311.17227>.
- 3 Alexander Cheung: 应用 Chat GPT 进行美军西太平洋反航母作战兵棋推演 [DB/OL]. (2023-06-23) [2024-06-30]. <https://zhuanlan.zhihu.com/p/639040303>.
- 4 孙宇祥,赵俊杰,解宇轩,等. 自生成兵棋 AI: 基于大型语言模型的双层 Agent 任务规划 [J]. 控制与决策, 2004.
- 5 WENG L. LLM - powered Autonomous Agents [DB/OL]. (2023-06-23) [2024-06-30]. <https://lilianweng.github.io/posts/2023-06-23-agent/>.

大小模型协同推理在阵地部署 和火力分配中的应用**

黄成琪¹ 梁文谦^{1*} 张勇¹ 家会臣¹ 胡月¹

摘要 多武器对多目标的协同火力分配和阵地部署能够有效地提高作战集群的整体作战效能。传统协同火力打击模型难以直接处理自然语言描述的作战任务，无法快速整合复杂多变的战场信息，而单独使用GPT等大模型无法处理火力分配等比较复杂的计算类任务。结合大模型的深度理解能力与小模型的高效计算优势，文章提出了一种基于大小模型级联的协同推理方法。实验结果表明，该方法可以有效提升决策的效率和准确性，展示了其在军事应用中的巨大潜力。

关键词 大模型与小模型的协同，阵地部署，火力分配，协同推理

Application of Collaborative Reasoning between Large and Small Models in Position Deployment and Firepower Distribution**

HUANG Cheng-Qi¹ LIANG Wen-Qian^{1*} ZHANG Yong¹ JIA Hui-Chen¹ HU Yue¹

Abstract The fire allocation and deployment of multiple weapons can significantly improve the operational effectiveness. Traditional optimization models struggle to directly address combat missions described in natural language and fail to rapidly integrate complex, ever-changing battlefield information. Furthermore, employing large models like GPT independently still can not solve complex problems such as fire distribution. We combine the deep comprehension capabilities of large language models with the computational efficiency of conventional optimization models, proposing a collaborative inference method based on a cascade of large and small models. Experimental results show that our approach can improve decision-making efficiency and accuracy.

Key words collaboration of LLMs and traditional models, positioning deployment, fire distribution, collaborative inference

** 国家科研项目（2019-JCJQ-ZD-002）资助

** Supported by National Scientific Research Project of China (2019-JCJQ-ZD-002)

* 通讯作者

1. 北方自动控制技术研究所

1. North Automatic Control Technology Institute

0 引言

在当今信息化战争时代，军事战略与作战方式正经历前所未有的变革，对指挥决策的智能化与高效性提出了更高要求。阵地部署与火力分配是军事作战中实现战场控制、夺取作战胜利的关键要素，随着科技的发展，战争形态已由传统的线性对抗转变为信息化条件下的非接触、立体化作战，这对军队的作战部署和火力运用构成了新的挑战。

阵地部署与火力分配旨在解决火力单元从集结区域到作战区域的兵力部署决策和火力单元在作战区域的火力分配决策。这两项任务紧密相连，且相互依赖，具体情况如图 1 所示。阵地部署层级将火力单元分配到不同的作战区域，不同作战区域对应不同的目标毁伤概率。火力分配层级为每个火力单元分配打击目标，以最大化作战效益。火力分配任务涉及单层迭代结构，即需要为我方每一个火力单元分配一个最佳打击目标，以实现最优的作战效能。相比之下，阵地部署任务则相对复杂，涉及双层迭代结构，首先需要计算得到各种阵地部署类型下的最优火力分配方案，然后再比较这些方案，以得到最终的最优阵地部署方案。传统的数值优化方法被广泛应用在阵地部署和火力分配任务的求解中，如线性规划、动态规划、遗传算法和粒子群优化等方法^[1-4]。线性规划和动态规划方法在处理确定性问题时表现突出，通过建立数学模型，可以精确地计算出最优解。遗传算法和粒子群优化等智能优化算法则在处理复杂、不确定性问题上显示出独特的优势，能够在大规模搜索空间中快速找到近似最优解。这些方法通过数学模型和算法，能够在一定程度上提高

决策的准确性和效率。以优化算法为基础的小模型在专业领域内表现出色，在特定任务中具备灵活部署和高效计算的优势，能够及时处理相对复杂的战场计算类任务^[5]。这些小模型能在资源有限的情况下提供高效的解决方案，从而提升整体作战效能。

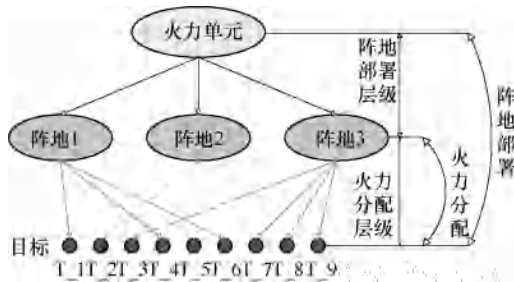


图 1 火力分配与阵地部署任务图

然而对于自然语言描述的火力协同打击任务问题，如图 2 中任务问题示例所示：“在某次作战任务中，敌方在我方根据地外设置了 3 个据点，其威胁程度分别为 (2, 3, 1)。我方计划派遣由 10 个火力单元组成的炮兵部队摧毁敌方据点，根据侦察情报和地势分析，有 3 个作战区域可以作为阵地部署我方火力单元，各阵地对敌方各据点的摧毁概率为：第一个阵地 (0.29, 0.76, 0.55)，第二个阵地 (0.56, 0.39, 0.57)，第三个阵地 (0.45, 0.41, 0.73)。现在需要规划每个作战区域的火力单元部署数量以及确定各火力点的最优进攻策略，以最大程度上摧毁敌方据点”，小模型难以处理示例中自然语言类的非结构化信息，从自然语言信息到结构化数据，再到小模型处理通常需要人工介入提取任务信息，这不仅效率低下，而且容易引入错误。随着技术的发展，作战指令与情报信息的来源日益多元化，包括大量非结构化的自然语言信息，这对新信息的快速理解和小模型的高效求解提出了新的挑战。

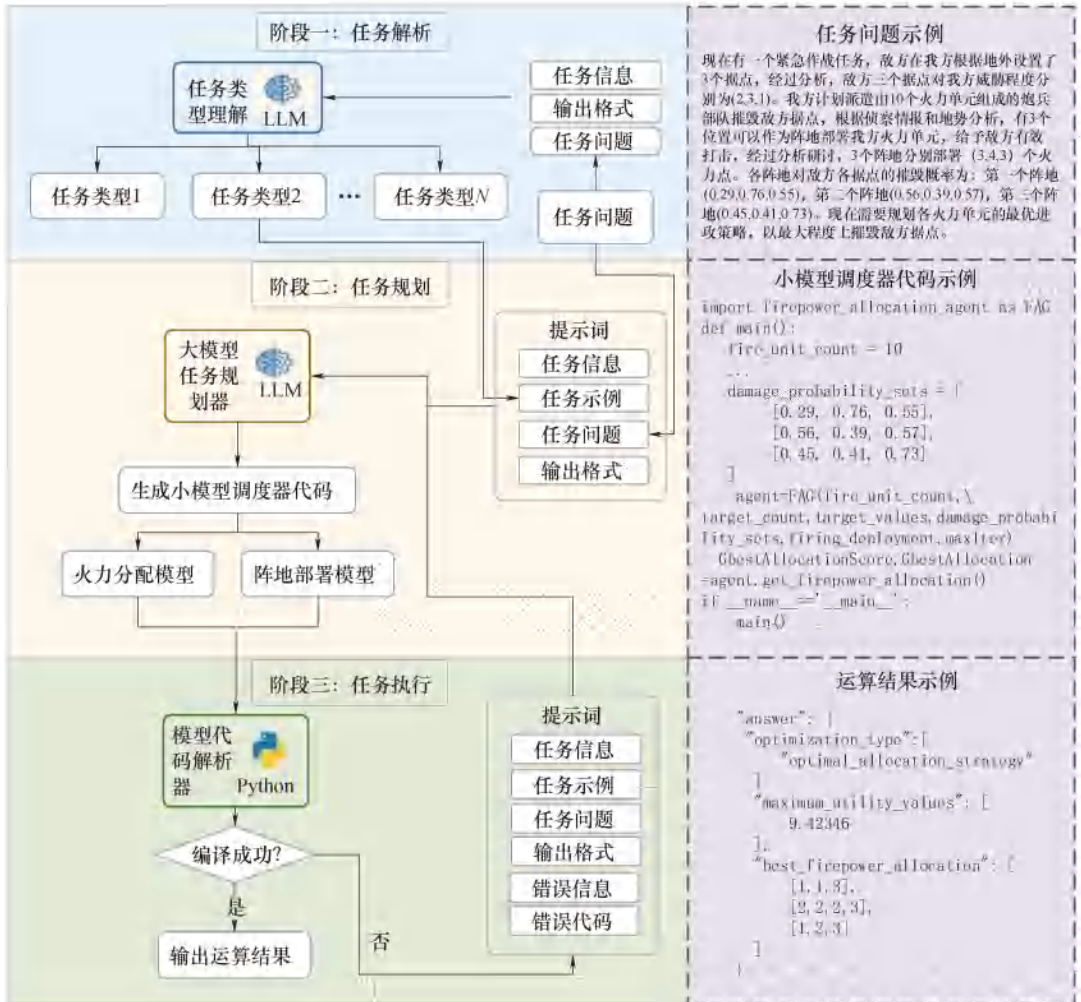


图2 基于大小模型级联的协同推理方法

人工智能技术，特别是自然语言处理领域的突破，为解决上述问题提供了新的方法。大型语言模型（Large Language Models, LLMs）具备进行复杂任务辅助决策的潜力^[6-7]。在军事领域，LLMs 已经被用于战场信息分析、态势感知和决策支持等方面。例如，LLMs 可以帮助指挥官快速理解和处理战场信息，并提供合理的决策建议^[8-11]。LLMs 在自然语言处理领域取得了显著进展，展现出强大的语境理解、生成对话和抽象推理能力。因果推理方

法、知识引导推理及提示工程等方法^[12-16]可以利用 LLMs 处理复杂的逻辑推理问题，这些方向的研究为 LLMs 的落地应用带来更广阔的空间。

然而，当前还无法使用 LLMs 直接处理相对复杂的推理和认知任务，特别是在诸如军事行动范畴内的精密火力分配等高度专门化及计算密集型任务上仍存在局限。虽然 LLMs 能够辅助理解复杂的作战指令和环境描述，但要处理如火力分配这样的精确计算和决策优化问题，还需要与

具备专业计算能力的小型模型算法相结合。因此，如何有效结合 LLMs 的高级认知能力与小型模型在特定任务上的高效计算优势，成为提升军事指挥自动化水平和作战效能的关键。此整合策略不仅要求超越单一模型的能力界限，还需探索两者协同作用的新机制，以期在保持决策智能性的同时，实现运算效率与任务适应性的双重提升。

本文提出了一种基于大小模型级联的协同推理方法——CascadingPlanner，旨在克服单一模型局限性、融合大小模型多元智能优势。该方法通过构建层次化级联结构处理流程，首先利用 LLMs 的广泛知识库和深度理解能力，对复杂及非结构化的自然语言指令进行解析，分辨任务类型和形成结构化数据。随后，这些数据被精确地导向至小模型（轻量级专业模型），这些小模型专注于特定领域任务，如精确火力计算等，进行高效且针对性的处理。小模型凭借其在特定领域的优化算法和快速计算特性，能迅速生成精确的解决方案或建议。在此过程中，大小模型通过智能路由和信息精练机制紧密协作，形成了一个既深且广的协同推理框架，既保留了 LLMs 的泛化和理解优势，又融合了小模型的计算效率和领域专长。

具体而言，本文的创新点包括：

(1) 级联结构的资源优化与效率提升：通过级联结构将知识密集型和计算密集型任务分别交给 LLMs 和小模型，实现了计算资源的高效配置。LLMs 负责理解与策略制定，减少不必要的计算负担；小模型则聚焦于高效执行，确保快速响应，从而整体提高模型处理复杂任务的能力和效率。

(2) 错误反馈机制提升推理计算准确性：LLMs 因其特性会产生预期之外的结

果或错误，为了纠正错误并提高准确性，本文基于 Python 解析器设计了一种错误反馈修正机制，通过这个过程，LLMs 能够自行调整和修正协同推理错误，产生更准确的运行结果，从而提高级联模型的准确性和健壮性。

(3) 模块化框架增强灵活性与可扩展性：该方法以大模型为核心构建了一个模块化的协同推理框架，可根据任务需求灵活插入或替换不同的专业领域小模型，便于不断引入最新的 AI 研究成果，如新型 LLMs 或针对特殊任务优化的小模型，增强协同推理的泛化性和可扩展性。

1 基于大小模型级联的协同推理方法

CascadingPlanner 方法的流程如图 2 所示，通过 LLMs 与小模型级联结构的协同工作，实现对非结构化任务的高效处理。CascadingPlanner 方法分为三个阶段：任务解析、任务规划和任务执行，能够利用 LLMs 的强大自然语言处理能力和小模型独特的计算优势，通过级联的方式让大小模型协同工作，确保任务的高效准确执行。基于大小模型级联的协同推理方法的实现过程伪代码如算法 1 所示。

1.1 阶段一：任务解析

在任务解析阶段，CascadingPlanner 处理的是复杂的非结构化任务问题，任务问题示例如图 2 所示。为了高效解决这一问题，CascadingPlanner 引入了 LLMs，充分利用其卓越的自然语言理解能力，对任务进行深度语义剖析。LLMs 通过其庞大的知识库和精湛的语义理解能力将任务问题映射至预定义的任务类型框架中，每种类型均配有针对性的处理策略与方法。这一

过程中, LLMs 可以快速、准确地理解任务类型, 提高任务解析的效率。Cascading-Planner 会根据 LLMs 分析出的任务类型, 选定用于解决该任务的小模型, 为任务规划阶段提供支持。

算法 1 基于大小模型级联的协同推理方法伪代码

```

01 task = 作战任务
02 prompt_1 = <task, task_msg_1, rule_1>
03 task_type = ask (prompt_1) //询问 LLMs 获得任务类型
04 If task_type = type [i] //某任务类型
05     example = type [i].example //任务类型对应的任务示例
06 prompt_2 = <task, task_msg_2, example, rule_2>
07 code = ask (prompt_2) //询问 LLMs, 生成小模型调度器
08 for i = 1: max_num //尝试执行小模型调度器, 报错后重新生成
09     error_msg = None //初始化错误信息 10
10     try:
11         exec (code)
12     except Exception as error_msg
13         prompt_3 = <task, task_msg_3, example, rule_3, code, error_msg>
14     code = ask (prompt_3) //询问 LLMs, 重新生成小模型调度器
15     If error_msg = None
16         break

```

1.2 阶段二：任务规划

在任务规划阶段, LLMs 依据任务解析阶段得到的任务类型和给定的任务信息, 结合任务示例和规定的输出格式, 构建大模型提示词, 从任务问题中识别出任务的细节和特定要求。如 LLMs 能够识别出涉及的火力单元数量、目标数量等相关参数形成结构化数据。这种能力显著减少

人工处理非结构化信息的需求, 提高任务规划的效率和准确性。LLMs 会根据任务类型选择相应的小模型调度器代码示例模板, 并结合任务的具体信息进行修改后生成新的小模型调度器代码。小模型调度器代码示例如图 2 所示, LLMs 在小模型调度器示例中导入火力分配小模型的工具包, 同时从任务问题中提取火力单元数量等信息形成结构化数据, 最后以调用小模型工具包的方式解决问题。在这一阶段, LLMs 不仅需要理解任务信息, 还需要进行一定的推理和决策, 以调用最合适的小模型。LLMs 在生成调度器时还需考虑调度器的可执行性, 以确保后续任务执行阶段的顺利进行。通过这种方式, 任务规划阶段实现了任务数据的结构化处理, 保证生成的调度器的准确性和适用性, 从而提高任务规划的速度和质量。

1.3 阶段三：任务执行

在任务执行阶段, CascadingPlanner 通过利用 Python 代码解析器执行任务规划阶段生成的小模型调度器代码。在调度器执行过程中, 选定的小模型会被调用并执行复杂的计算过程。具体而言, 当 Python 解析器执行 LLMs 生成的小模型调度器代码时, 会实时监控调度器的执行状态, 确保任务的顺利执行。如果调度器执行成功, 小模型被调用执行并会输出计算结果; 如果调度器执行失败, 则会返回错误信息并触发错误反馈机制。错误反馈机制是 CascadingPlanner 的重要组成部分, 当 Python 解析器在执行 LLMs 生成的小模型调度器代码时发生错误, 错误反馈机制会收集错误信息形成新的提示词, 包括错误代码、错误信息、任务问题、任务示例、任务信息和输出格式。这些信息会被重新输入给 LLMs, LLMs 根据这些反馈信息修改生成

的小模型调度器代码。通过这种反馈循环，不断优化任务执行过程，提高生成调度器的准确性和可靠性。任务执行阶段不仅是调度器的执行过程，还包括对执行结果的分析 and 验证。CascadingPlanner 采用了 LLMs 与小模型的级联结构，将任务理解和计算过程分隔开来，显著提高了任务处理的效率和准确性。这一阶段的任务执行和反馈机制确保了整个过程的稳健性和可靠性，能够应对各种复杂任务的挑战。

CascadingPlanner 方法通过任务解析阶段识别任务类型，决定问题的解决方法；在任务规划阶段，LLMs 提取任务数据并生成小模型调度器调用小模型；在任务执行阶段，小模型进行计算、反馈机制确保整个级联过程的准确性。该方法充分利用了 LLMs 和小模型的优势，实现了复杂任务的高效、精准处理。

2 实验

本研究设置了两组实验。实验一用于验证 CascadingPlanner 方法在三种数据集任务中的有效性和准确性，并设置了两种对比算法。实验二用于验证在控制算力资源的情况下，相比单一的大模型，分析不同参数量的大模型与小模型级联对计算结果的影响。

2.1 实验设置

2.1.1 数据集

由于获取真实的作战数据较为困难，本文通过设定提示词让 LLMs 生成作战任务，并邀请专家对生成的作战任务评估和修正，最终构成实验数据集。其中，火力分配数据集包含 100 条火力分配任务，阵地部署数据集包含 100 条阵地部署任务，混合数据集是包含 50 条火力分配与 50 条

阵地部署的混合任务。

2.1.2 模型配置及设备资源

模型配置：在本文中，设置了一个闭源大模型 GPT-3.5-turbo、两个开源大模型 Llama3 (8B 参数) 和 Code Llama (13B 参数)。其中，闭源大模型 GPT-3.5-turbo 可以通过 OpenAI API 远程访问，开源大模型是将本地服务器作为算力资源，部署 ollama 框架，通过类 OpenAI API 接口实现对开源大模型 Llama3 和 Code Llama 的调用。

设备资源：服务器安装 CentOS 7.9 系统，搭载四块 NVIDIA A800 高性能 GPU，为深度学习、大数据处理提供强大算力支持，确保高效运算。

2.1.3 实验一方案设置

为了验证 CascadingPlanner 的合理性，选择了 Chain of Thought (CoT)^[17] 和 Reason to Act (ReAct)^[18] 作为对比算法，CoT 仅采用 GPT-3.5-turbo 大模型，CascadingPlanner 和 ReAct 采用 GPT-3.5-turbo 大模型+小模型协同的方式，CascadingPlanner 与 ReAct 相比增加了错误反馈机制。三种方案均用于解决火力分配任务、阵地部署任务、火力分配与阵地部署混合任务。

2.1.4 实验二方案设置

实验二设置了四种方案，第一种方案为仅采用 GPT-3.5-turbo 大模型；第二种方案采用 Llama3 大模型+人工蜂群算法小模型；第三种方案采用 Code Llama 大模型+人工蜂群算法小模型；第四种方案采用 GPT-3.5-turbo 大模型+人工蜂群算法小模型。第一种方案通过 CoT 的方法使用，其余三种方案通过 CascadingPlanner 方法使用。四种方案均用于解决火力分配任务。

2.1.5 小模型介绍及超参数选择

人工蜂群算法 (Artificial Bee Colony Algorithm, ABC)^[19] 是一种模拟蜜蜂觅食行为的启发式算法, 有较高的搜索效率和全局优化能力。在火力分配层级, 设定种群大小为 20, 迭代次数为 2000。在阵地部署层级, 设定种群大小为 20, 迭代次数为 10。经过多次实验, 此设定能够在计算精度和时间效率之间取得良好平衡。

2.1.6 实验评价指标

实验一和实验二中各方案均是以“解决自然语言描述的阵地部署和火力分配任务”为目的, 因此, 以“方案对任务求解的作战效能值是最优值”的数量与任务总数量的比值作为评价指标, 这个比值称为正确率, 错误率与正确率相反。最优值的计算方式为: 人工从自然语言任务中提取数据, 并使用穷举算法计算正确结果。穷举算法能够遍历所有可能的解并找出最优解。

2.2 实验结果分析

实验一的结果如表 1 所示。CascadingPlanner 在火力分配、阵地部署和混合任务三种数据集上的正确率分别为 0.95、0.92 和 0.89, 均显著高于 CoT (思维链) 和 ReAct (推理+行动) 在相应任务中的正确率。CoT 的方法处理的正确率均为 0, 说明单一的大模型难以解决复杂的计算任务。这些结果表明, 增加错误反馈机制的 CascadingPlanner 方法在大小模型协同处理任务时, 能有效提升正确率。

实验二的结果如表 2 所示。CascadingPlanner 方法分别采用了 Llama3 和 Codellama 大模型与小模型 ABC 协同工作, 整体计算资源消耗小于 CoT 方法仅使用的 GPT-3.5-turbo, 但在处理该类任务时的正确率分别为 0.41 和 0.44, 显著高于

CoT。这证明了大小模型协同的合理性。CascadingPlanner 使用 GPT-3.5-turbo 大模型协同小模型 ABC, 使得正确率进一步提升至 0.95, 显著优于前述所有结果。这表明, 当大模型本身性能优异时, 大小模型的协同工作能更好地处理复杂计算任务。因此在本文中, 采用性能更优的 GPT-3.5-turbo 作为级联结构中的大模型。

表 1 不同方法在各作战任务处理的正确率

方法	火力分配任务	阵地部署任务	混合任务
CoT	0	0	0
ReAct	0.88	0.82	0.84
CascadingPlanner	0.95	0.92	0.89

表 2 不同大模型在火力分配任务处理的正确率

方法	火力分配任务
CoT (GPT-3.5-turbo)	0
CascadingPlanner (Llama3+ABC)	0.41
CascadingPlanner (Code Llama+ABC)	0.44
CascadingPlanner (GPT-3.5-turbo+ABC)	0.95

针对产生的错误, 本文对混合任务进行了分析, 如表 3 所示。CascadingPlanner 方法的错误率为 0.08, 而 ReAct 为 0.13。这表明反馈机制能够提升级联结构解决任务的正确率。两者计算结果存在偏差的错误率均为 0.03, 这是因为 ABC 在限定时间内计算结果不是最优值。

总体来看, CascadingPlanner 在解决混合任务的表现优于 ReAct。错误反馈机制显著降低了级联过程中错误发生的概率, 为 CascadingPlanner 在任务的解决中提供更高的准确性。

表 3 混合任务中反馈机制对错误率的影响

错误类型	错误原因	CascadingPlanner	ReAct
模型代码未通过解析器	语法错误	0.08	0.13
与准确解存在偏差	ABC 计算大规模数据非最优解	0.03	0.03

3 结束语

本文提出基于大小模型级联的协同推理方法——CascadingPlanner，将任务处理过程分为了任务解析、任务规划、任务执行三个阶段，在后两个阶段中设计了错误反馈机制。以火力分配和阵地部署为例阐述了其应用过程。实验一以 CoT 和 ReAct 方法作为对比，证明了 CascadingPlanner 的有效性，实验二采用了不同参数数量的大模型与小模型协同，证明了大小模型级联的合理性，并且当大模型性能越优，大小模型协同效果越好。

未来的研究将聚焦于几个关键方向以优化该方法。首先，微调小参数数量的开源大模型，使其协同推理能力能匹配上大参数数量的闭源大模型；其次，拓展 LLMs 级联更多不同类型的小模型；最后，通过 LLMs 级联结构收集制作专用数据集，逐步训练微调获取军事领域行业大模型。

参考文献

- 王光源, 李浩民, 陈永展, 等. 基于灰狼算法的多平台火力分配优化模型 [J]. 科学技术与工程, 2023, 23 (23): 10133-10138.
- 夏维, 刘新学, 范阳涛, 等. 基于改进型多目标粒子群优化算法的武器-目标分配 [J]. 兵工学报, 2016, 37 (11): 2085-2093.
- 褚凯轩, 常天庆, 张雷. 基于改进人工蜂群算法的地面作战武器-目标分配 [J]. 兵工学报, 2023, 44 (7): 2171-2183.

- 高春生, 宋业新. 基于嵌套算法的反无人机集群防空部署 [J]. 舰船电子工程, 2023, 43 (8): 31-36.
- 马悦, 吴琳, 郭圣明. 作战任务分配建模及求解方法研究 [J]. 系统仿真学报, 2023, 35 (4): 887.
- JIE C. Analysis of potential Military Applications of ChatGPT [EB/OL]. <http://www.xinyiji.com/news/20221306.html>.
- 瞿崇晓, 郑奇平, 张永晋, 等. GPT 技术原理及其潜在军事应用研究 [J]. 中国电子科学研究院学报, 2023, 18 (7): 624-633.
- ZHOU G X, YAN J. Exploration of the Application of ChatGPT in Command and Control [C] // 2023 9th International Conference on Big Data and Information Analytics, Haikou, China. 2023: 807-811.
- WU J Y, CHE F H, ZHENG X X, et al. Can large language models understand uncommon meanings of common words [J]. arXiv e-prints, 2024. DOI: 10.48550/arXiv.2405.05741.
- BISWAS S. Prospective Role of Chat GPT in the Military: According to ChatGPT [J]. Qeios, 2023. DOI: 10.32388/8wywod.
- MA Y, WU L, GUO S, et al. Research on Modeling and Solution Method of Operational Tasks [J]. Journal of System Simulation, 2023, 35 (4): 887-898.
- CRESWELL A, SHANAHAN M. Faithful Reasoning Using Large Language Models [J]. arXiv, 2022. DOI: 10.48550/arXiv.2208.14271.
- RAMÍREZ G, BIRCH A, TITOV I. Optimising Calls to Large Language Models with Uncertainty-Based Two-Tier Selection [J]. arXiv preprint arXiv:2405.02134, 2024.
- ZHOU D, NATHANAEL S, LE H, et al. Least-to-Most Prompting Enables Complex Reasoning in Large Language Models [J]. arXiv preprints, 2022. DOI: 10.48550/arXiv.2205.10625.
- SHEN Y, SONG K, TAN X, et al. Hugginggpt: Solving ai tasks with chatgpt and its friends in hugging face [C] // In Proceedings of the 37th International Conference on Neural Information Process-

- ing Systems (NeurIPS 2023). 2023: 2734 – 2747.
- 16 ZELIKMAN Y W, GOODMAN N D. Star: Bootstrapping reasoning with reasoning [J]. arXiv preprint arXiv: 2203. 14465, 2022.
- 17 WEI J, WANG X Z, DALE S, et al. Chain – of – thought prompting elicits reasoning in large language models [J]. In Proceedings of the 36th International Conference on Neural Information Processing Systems (NeurIPS 2022), 2022, 34 (7): 2824–2837.
- 18 YAO S, ZHAO J, YU D, et al. ReAct: Synergizing Reasoning and Acting in Language Models [J]. In Proceedings of the Eleventh International Conference on Learning Representations (ICLR 2023), 2023, 32 (5): 336–345.
- 19 MISHRA, BHABANI S P, EUI – WHAN K, et al. Weapon target assignment problem: multi – objective formulation, optimisation using MOPSO and TOPSIS [J]. Int. J. Intell. Def. Support Syst, 2015, 5: 226–252.

大语言模型赋能冲突博弈分析**

顾天阳¹ 葛冰峰^{1*} 黄宇铭¹ 韩思宁¹ 侯泽强¹

摘要 人工智能技术的快速发展，为冲突博弈分析的革新提供了新的契机。冲突分析图模型是进行冲突消解的常用方法。然而，经典的冲突分析图模型在面对复杂冲突局势和海量冲突数据时存在一定的局限性。文章提出了一种基于大语言模型的冲突分析应用框架，旨在利用大模型强大的自然语言理解和生成能力以赋能冲突博弈分析。随后介绍了该框架关键部分的技术实现，展望了该框架对冲突分析领域的潜在能力增强，并分析了可能存在的风险和挑战。

关键词 大语言模型，冲突博弈分析，冲突分析图模型，自然语言处理，智能化决策

Enhancing Conflict Analysis Based on Large Language Models**

GU Tian-Yang¹ GE Bing-Feng^{1*} HUANG Yu-Ming¹ HAN Si-Ning¹ HOU Ze-Qiang¹

Abstract The rapid development of artificial intelligence has provided new opportunities for innovation in conflict analysis. The graph model for conflict resolution (GMCR) is commonly used for conflict resolution. However, traditional GMCR has certain limitations when faced with complex conflict situations and vast amounts of conflict data. This paper proposes a conflict analysis application framework based on large language models (LLMs), aiming to leverage the powerful natural language understanding and generation capabilities of LLMs to enhance conflict analysis. It subsequently introduces the technical implementation of key components, explores the potential enhancements and examines the possible risks and challenges.

Key words large language models, conflict analysis, graph model for conflict resolution, natural language processing, intelligent decision making

0 引言

习近平总书记指出，把新一代人工智能作为推动科技跨越发展、产业转型升级

级、生产力整体跃升的驱动力量，努力实现高质量发展^[1]。随着生成式人工智能的迅速发展，大语言模型（Large Language Models, LLMs）的相关应用领域日益拓宽，越来越多的行业开始探索将大语言模

** 国家自然科学基金（项目编号：71971213、72071206、72231011）资助

** Supported by National Natural Science Foundation of China (Grants Nos. 71971213, 72071206, and 72231011)

* 通讯作者

1. 国防科技大学系统工程学院

1. College of Systems Engineering, National University of Defense Technology

型引入其内部的落地应用场景^[2-6]，以提供更加智能化的服务。

当今，世界正处于百年未有之大变局^[7]，全球战略竞争与地区冲突显著加剧^[8]。冲突各方综合运用军事、经济、政治、外交、舆论等多种对抗手段^[9]，严重阻碍了世界和平稳定发展。冲突分析图模型（Graph Model for Conflict Resolution, GMCR）^[10-11]因其仅需相对较少的信息就能对多方的冲突博弈进行系统有效的建模和分析，已被广泛应用于各种冲突博弈问题的化解^[12-13]。在面对复杂多变的冲突局势时，通常伴随着海量的冲突相关数据，仅靠决策人员往往难以对冲突进行精准建模和快速决策响应。考虑大语言模型在文本检索和知识推理等方面的优势，本文构建了一个基于大语言模型的冲突分析应用框架，旨在赋能冲突分析，实现智能化的冲突消解决策。随后介绍了该框架关键部分的技术实现，分析了在冲突分析领域的应用前景，并讨论了可能存在的风险与挑战。

1 大语言模型及冲突分析概述

1.1 大语言模型

2022年11月，OpenAI公司正式推出了一款人工智能对话聊天机器人ChatGPT^[14]，其出色的自然语言理解与生成能力引起了全世界范围的广泛关注，2个月即突破1亿用户，在国内外掀起了一场大语言模型的浪潮。随着GPT4.0等多模态大语言模型的出现，逐渐显现出了更为成熟的人类思维特征，为人类实现通用人工智能的美好愿景奠定了基础。

大语言模型通常是指基于深度学习方法训练出的具有大规模参数集的神经网络

模型^[15]，如GPT、LLaMA、GLM、QWEN等。通过对海量相关数据的预处理、模型训练和模型评估与应用等步骤，大语言模型能够提供精准的语言理解、生成和分析能力，不仅可以进行文本分类和情感分析，还能够胜任多轮交互式问答、文本多种语言翻译等各项复杂任务。

大语言模型的核心架构是神经网络模型，其通过模拟人类大脑的工作机制和神经元连接，实现了对自然语言的高效处理和生成。常用的神经网络架构有RNN、LSTM和Transformer^[16]，GPT系列大语言模型的基础架构便是Transformer，其模型架构如图1所示。在文本处理时，通常使用词嵌入技术将词汇表中的每个单词映射到一个高维向量空间，这些向量能够捕捉单词之间的语义和语法关系，使得语义上相似的单词在向量空间中的位置更接近。此外，Transformer架构通过自注意力机制^[16]缩短了文本中词语依赖的建模路径，进而增加了模型在大规模语料上的文本建模能力。它允许模型在处理文本时能够关注到输入序列中的不同部分，并根据它们的重要性来分配注意力。

当前，大语言模型的主流应用场景主要集中在智能交互式对话领域，其能够根据用户提供的指令展开多轮对话，展现出了强大的上下文理解与推理决策能力。在基座大语言模型完成预训练后，可以针对特定任务对模型进行微调^[17]，从而适应不同的应用场景。例如，在医学领域^[2-3]，研究人员尝试利用大语言模型进行精准诊断和个性化治疗方案的制订；在教育领域^[5]，大模型有望辅助个性化学习和智能辅导。

1.2 冲突分析图模型

冲突分析图模型^[10-11]，由加拿大学者

基尔戈 (Kilgour) 和希佩尔 (Hipel) 教授等基于经典博弈论的框架提出, 通过系统化的建模和分析过程, 将图论知识运用于解决冲突问题。由于冲突分析图模型仅需各个决策者的相对偏好信息就能进行冲突的定性定量分析, 已被广泛应用于化解现实世界的各种冲突争端和博弈对抗中^[12-13]。

利用冲突分析图模型进行冲突消解分为冲突建模和冲突分析两个阶段, 整个流程如图 2 所示。在冲突建模阶段, 主要包括以下步骤: 确定决策者和策略选项、生成可行状态、识别状态转移以及获取决策者对可行状态的相对偏好信息。在冲突分析阶段, 将基于不同的稳定性定义对所构建的冲突模型进行稳定性分析, 通常包括纳什稳定性 (Nash Stability)^[18]、一般元理性 (General Metarationality, GMR)^[19]、

对称元理性 (Symmetric Metarationality, SMR)^[20] 和序贯稳定性 (Sequential Stability, SEQ)^[21] 四种稳定性定义, 以计算求解冲突可能的均衡方案; 在稳定性分析之后, 将进行后稳定性分析, 包括演化路径分析、灵敏度分析以及其他后续分析。然而, 经典的冲突分析图模型在实际应用中具有一定的局限性。在面临复杂多变的冲突局势时, 仅由专家指定冲突的多方决策者、决策者的策略选项、偏好的表征结构以及相对偏好信息等冲突要素, 往往是主观、不全面的。此外, 在面对海量的冲突相关数据时, 决策人员通常难以在短时间内提取关键有效的冲突信息, 导致无法及时做出决策。因此, 有必要引入大语言模型以辅助冲突分析, 为复杂冲突的消解提供更智能、更全面的战略指导和决策支持。

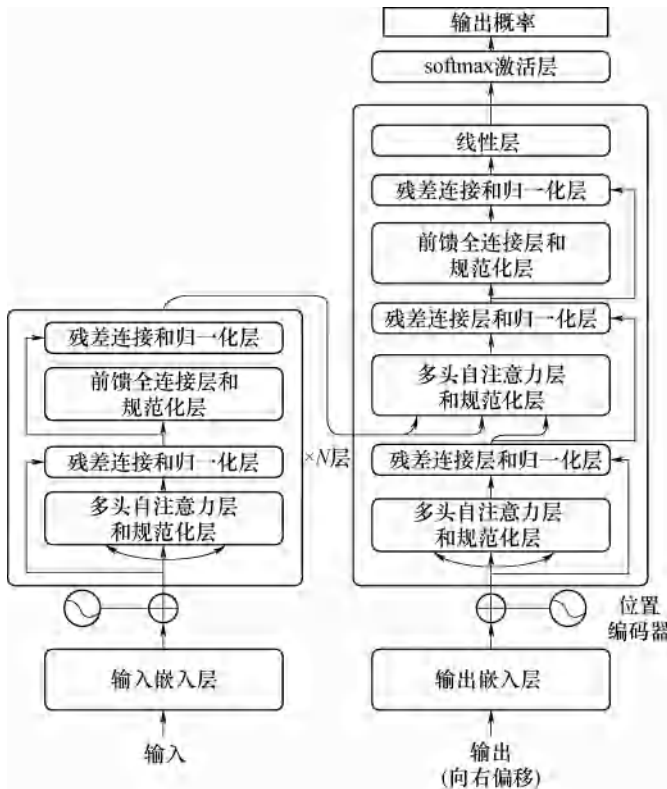


图 1 Transformer 的模型架构

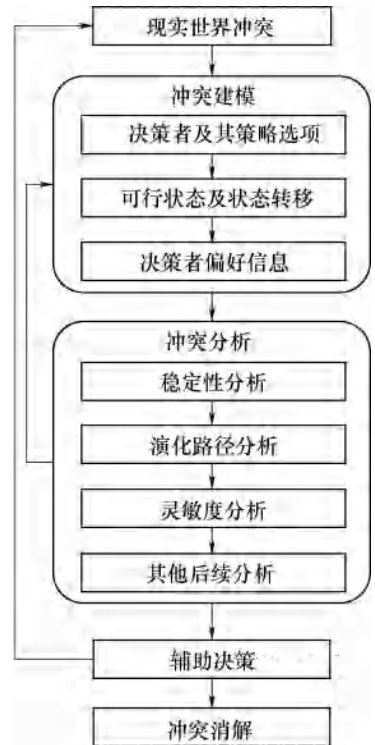


图 2 冲突分析的基本流程

2 基于大语言模型的冲突分析应用框架

基于大语言模型的冲突分析应用框架涉及海量数据处理和领域大语言模型构建等技术，如图 3 所示。该框架自底向上共有五个层次，包括支撑环境层、数据驱动层、模型驱动层、冲突消解层以及态势展示层。

支撑环境层是该框架的基础服务环境，为上层应用提供了必要的支撑，主要

包括计算资源、信息网络、云计算平台以及其他基础服务。计算资源可以提供强大的数据处理能力，以满足应用的计算资源需求，包括高性能的 CPU 和 GPU 资源。信息网络将构建高效的数据传输和通信基础设施，确保数据传输的高效性和安全性，同时支持多样化的数据采集需求。云计算平台则提供弹性的计算和存储资源，支持应用程序的快速部署和弹性伸缩。这些基础设施共同构成了应用框架的资源底座，为上层应用的开发和运行提供了有效的支撑。

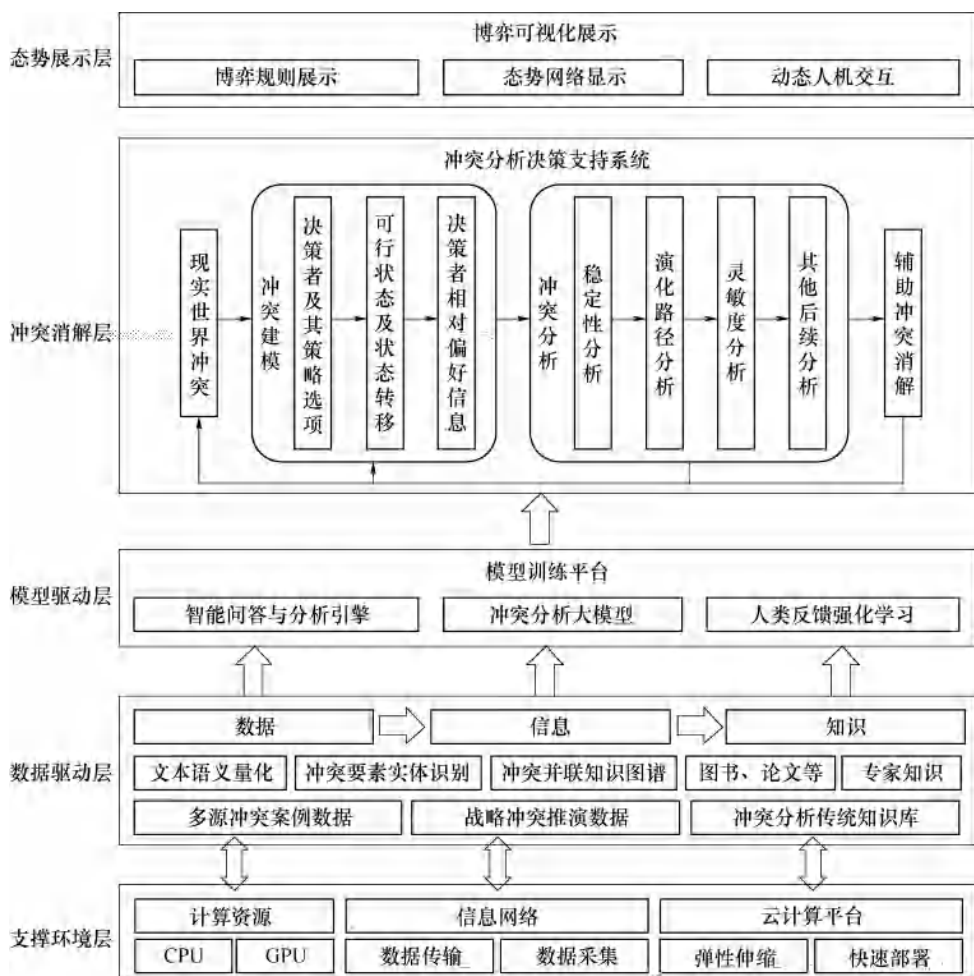


图 3 基于大语言模型的冲突分析应用框架

数据驱动层针对海量的多源冲突案例数据、战略冲突推演数据以及冲突分析传统知识库进行综合分析处理,形成高价值的知识产品。首先,对各种来源的冲突案例数据进行结构化处理,对案例中的实体、冲突要素进行编码和语义识别^[22],在此基础上抽取冲突要素和量化语义,从中自动识别各个关键要素,并通过冲突要素关系挖掘构建冲突的关联知识图谱^[23]。除了整合多源冲突案例数据外,数据驱动层还应涵盖垂直领域的冲突分析传统知识库,如图书、论文、专利等文献类数据,以及领域专家的深度见解和实践经验。引入传统文献数据库和领域专家知识可以显著增强外部知识库构建,为大语言模型提供更丰富和权威的信息来源。构建的知识库能够作为大语言模型的循证依据,极大提高了输出信息的可信度。

模型驱动层是该框架智能化的核心部分,主要包括冲突分析大模型、智能问答与分析引擎以及人类反馈强化学习^[24]。模型训练平台接收数据驱动层传递的海量数据,用于进一步训练构建冲突分析大模型。人类反馈强化学习机制允许专家参与模型的训练过程,专家的偏好被用作奖励信号,以指导模型的训练,实现人机协同的混合增强智能。冲突分析大模型一方面支持智能问答,其能够成为辅助决策人员的“参谋助手”,基于 Prompt 指令的即问即答能显著深化决策人员对于冲突的理解和认识,也可作为学习冲突分析领域知识的工具;另一方面,模型内部的分析引擎用于智能化构建冲突的博弈模型,实现快速确定博弈模型的多方决策者、决策者的策略选项、偏好的表征结构以及相对偏好信息等冲突要素,并能够根据冲突环境的动态变化,自适应地调整博弈模型的相关参数。大模型将提供深入的洞察力和精确

的决策支持,从而辅助决策人员在战略上制订有效的冲突消解方案。

冲突消解层是构建博弈模型和求解均衡方案的关键一层。博弈模型的输入包括决策者及其策略选项、可行状态及状态转移以及决策者相对偏好信息。得益于大语言模型强大的文本检索和知识推理能力,博弈模型的各个要素能够通过冲突分析大模型自动、高效地提取得到。这种方法不仅提高了博弈模型的构建效率,还潜在提高了后续冲突分析的准确性。在冲突分析时,求解计算冲突可能的均衡状态并根据冲突现状预测冲突态势的走向。在决策支持系统和大语言模型分析引擎的双重支撑下,将能够实现战略态势的量化分析和研判,并支持在形势研判基础上的战略预测。稳定性分析过程计算冲突在多种稳定性定义下的均衡状态,进而获得冲突可能的消解方案。此外,为了获得冲突从某个态势到达均衡态势或其他某一态势的演化路径,演化路径分析被用于提供详尽的态势转移路径。而灵敏度分析将检测博弈模型对不同参数变化的敏感性,帮助理解关键参数对冲突最终结果的影响。上述分析方法从不同的角度研究冲突问题的走向,这种预见性的分析可辅助决策人员提出更有指导性的策略。

态势展示层用于展示冲突博弈分析全过程的相关数据,并以大屏的形式进行可视化展现。一方面将展示博弈模型中决策者的策略选项、状态转移规则、相对偏好信息等冲突元素;另一方面将对冲突稳定性分析、博弈态势分析、演化网络分析、演化路径分析、灵敏度分析等的结果予以可视化展示。通过多维度的展示方式,提高了冲突分析过程相关信息的透明度和可读性,确保决策人员能够实时跟踪把握冲突的演进趋势。

综上，基于大语言模型的冲突分析应用框架，是一个模型驱动、人机协同，以多源冲突案例数据、战略冲突推演数据以及传统知识库为基础，以冲突建模和冲突分析为核心，以基于态势的战略决策为表现形式的复杂智能决策活动。

3 关键技术实现

3.1 构建面向战略主题的案例知识图谱

冲突的关联知识图谱，是冲突分析决策支持系统迈向智能化的基础工作，主要完成从海量冲突案例数据到面向特定主题的冲突案例认知的转化，形成案例之间的关系网络。

面向战略主题的案例知识图谱构建流

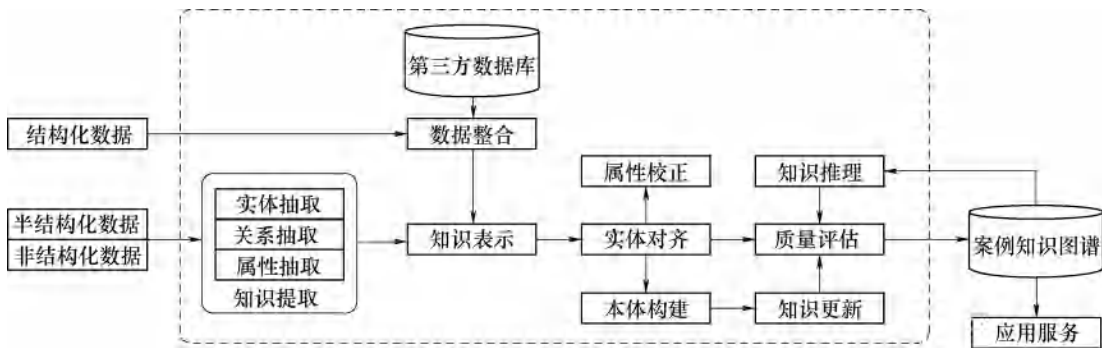


图4 面向战略主题的案例知识图谱构建

3.2 构建面向冲突分析的领域大模型

在基于大语言模型的冲突分析应用框架中，模型驱动层的关键在于构建面向冲突分析的非传统垂直领域通用大模型。针对不同的领域和应用需求，领域大模型的构建方式也各不相同，通常包括以下几种：

(1) 从零开始构建领域大模型。该方

程如图4所示。首先是数据采集，主要包括两种来源：①选定某一战略冲突主题，基于Python网络爬虫技术从各种互联网网页、新闻报道中爬取主题相关的冲突案例数据；②战略冲突推演产生的模拟仿真数据。其次是案例知识提取，包括实体抽取、关系抽取和属性抽取，从描述案例信息的文本中抽取所关注的案例实体并结构化表示，以实体为基本的语义单元，自动抽取实体之间的关联关系，包括因果关系、顺承关系、条件关系等，通过关联关系将实体联系起来，形成网状的知识结构。之后是知识融合，包括共指消解、实体对齐等，以消除矛盾和歧义。通过构建面向战略主题的案例知识图谱，形成了结构化的语义知识库，聚合了大量领域案例知识，从而实现知识的快速响应和推理。

法从领域的应用场景和原始数据出发，依次进行数据预处理、模型架构选择、模型训练、模型评估以及模型部署等步骤，以期构建一个为特定领域量身定制的大语言模型。例如，LaWGPT是基于中文法律知识的大语言模型^[25]，旨在提升模型对法律内容的理解和执行能力。然而，该方法通常依赖于海量的领域高质量数据和专家知识，因此其开发成本和难度相对较高。

(2) 二次预训练构建领域大模型。二次预训练方法是在预训练基座模型^[26]的基础上，使用领域的的数据进一步训练的方法。该方法首先基于海量的通用数据预训练一个基座模型，通常选择已有的通用大模型作为基座模型，如 GPT、LLaMA 和 GLM。之后，将基于特定领域的数据进行二次预训练。该方法不仅可以保持原基座大模型对自然语言强大的理解和生成能力，也能显著提高模型在特定领域内的表现性能。

(3) 微调构建领域大模型。在已经预训练的通用基座大模型上，通过微调^[27]使其适应特定的任务或领域，如图 5 所示。

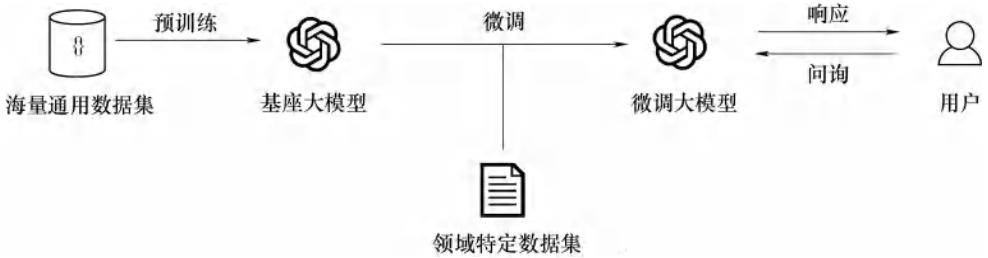


图 5 微调构建领域大模型

这一过程通常是向模型提供领域特定的案例数据和相关指令来实现，从而使模型能够理解和执行特定领域的任务。

(4) 结合向量知识库构建领域大模型。这种方法通过将预训练的基座大模型同外部的知识库相结合，使得模型可以学习到知识库中的相关知识，提高其在特定领域的准确性和可靠性。

对于冲突分析领域而言，考虑到其对通用知识的需求和开发成本，倾向于选择通用基座大模型进行领域内的微调，并融合外部的向量知识库，以增强大模型的可信数据来源，赋予模型更强的循证分析能力。

3.3 人类反馈强化学习增强模型性能

在模型驱动层引入人类反馈强化学习机制，是增强冲突分析大模型性能的关键举措。人类反馈强化学习结合了人类专家指导和机器学习算法，与传统强化学习^[28]通过探索和试错进行学习的方式不同，人类反馈强化学习通过利用人类的偏好信息和专业知识，实现了更快、更有针对性的学习。

人类反馈强化学习的训练过程如图 6 所示。首先是预训练，使用经典的预训练目标和通用数据文本训练一个语言模型，这里还可以使用额外的示范文本或条件对

语言模型进行微调。其次是训练一个奖励模型，该模型接收一系列对比文本并返回对应的标量奖励，在数值上对应于人类的偏好程度；在奖励数值方面，需要专家人工对语言模型生成的不同文本回答进行排名，通过排名可以比较语言模型的多个输出并构建更好的规范数据集。之后，利用奖励模型输出的奖励数值，用强化学习方式微调优化语言模型。这个过程可以被表述为强化学习问题，其策略是接收提示并返回一系列文本或文本的概率分布的语言模型；策略的行动空间是语言模型的词表对应的所有词元；观察空间是可能的输入词元序列；奖励函数则是奖励模型和策略转变约束的结合。通过直接从人类专家的

偏好和决策中学习，人类反馈强化学习可以帮助语言模型更好地理解 and 执行复杂的

任务，从而提升模型在建模和分析具体冲突问题时的性能表现。

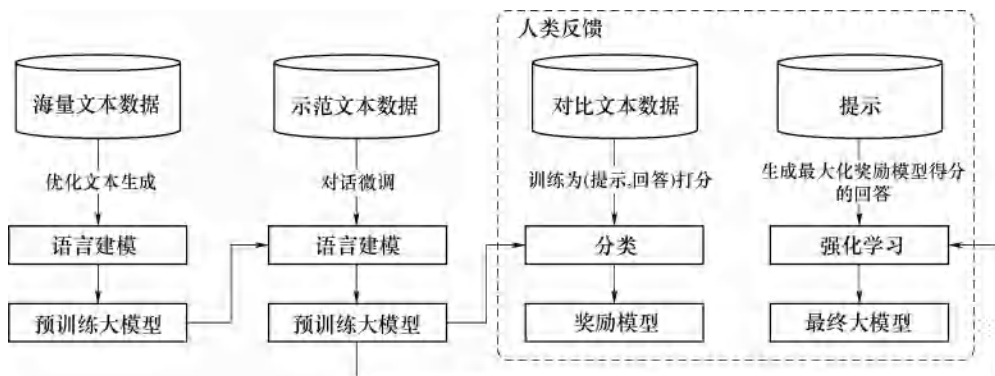


图6 人类反馈强化学习的训练过程

4 对冲突分析的能力增强

基于大语言模型的冲突分析应用框架，将有望作为未来智能化冲突分析的重要理论支撑，将在多个方面赋能冲突分析，提高冲突消解的效率和准确性。

4.1 交互式知识增强能力

大语言模型具有强大的自然语言理解和交互能力，决策人员可以通过自然语言直接与冲突分析大模型进行交互，相较于传统的固定格式输入指令，这极大提高了系统交互的灵活性和实用性。另外，通过与系统的智能交互式问答，决策人员可以快速获取关于历史冲突案例、策略选择以及冲突未来走向的深刻见解。此外，冲突分析大模型还可作为在线的知识学习平台，通过设置合适的提示，决策人员将能够在短时间内学习并掌握冲突分析领域的相关专业知识，以做出更加科学的冲突消解战略决策。总之，这种智能化的交互方式将允许决策人员在复杂多变的冲突局势中做出更快速和更精确的判断，大大提高

了决策效率和质量。

4.2 多源多模态数据融合能力

随着生成式人工智能的持续发展，部分大语言模型目前已具备处理和分析多源、多模态数据的能力，这满足了冲突分析领域在面对海量的多源异构数据时的切实需求。与传统的人工数据收集方法相比，大语言模型的知识检索能力显著提升了冲突案例数据来源的深度和广度。得益于对多源、多模态数据的高效处理能力，大语言模型能够快速地对冲突案例进行初始的全方位描绘和刻画，并构建一个原始的冲突博弈模型，从而为后续的冲突分析奠定了坚实的基础。通过对多源、多模态冲突案例数据的感知，大语言模型显著提升了决策支持系统对于复杂冲突的理解和分析能力，提供了多角度的冲突消解视角。

4.3 动态调整自适应能力

在现实世界中，冲突的局势不是一成不变的，而是时时刻刻在动态变化的。随着局势的演化和目标的调整，大语言模型

需要不断调整博弈模型的相关参数，以适应新的情况，这包括决策者、策略选项、偏好的表征结构以及相对偏好信息等冲突要素。另外，大语言模型本身具备强大的自学习能力，能够通过持续学习和训练，不断优化自身的表现性能。此外，大语言模型可以根据决策人员的使用习惯和反馈信息进行自适应调整，以提供更加个性化的服务。这种智能化的学习和自适应能力不仅提高了冲突消解的效率和效果，也为决策人员在复杂和不断变化的冲突环境下提供了关键的战略决策支持。

4.4 循证审查能力

辅助进行冲突消解的决策支持是冲突分析领域的核心目标，将大语言模型应用于冲突分析能提高决策的智能度和可信度。在冲突消解的具体场景下，确保案例数据来源的可靠性并提供相关证据是至关重要的，不仅能够提高冲突分析的可信度，还能提升语言模型的整体性能。除了开源的冲突案例数据，还有大量的传统文献数据，如图书、论文、专利等，该类数据由于受到知识产权的保护等规定，尚未广泛应用于大语言模型的训练中，因此，包含该类数据的冲突分析大模型将能够提供更深层次的洞见分析。这种方法不仅增强了系统的循证能力，也提升了语言模型的可解释性和鲁棒性。

5 风险和挑战

尽管基于大语言模型的冲突分析应用框架在冲突分析领域的智能化方面有着广阔的应用前景，但由于大语言模型本身存在一定的局限性，在框架落地之前，必须谨慎评估并解决可能存在的风险和挑战。

5.1 数据隐私和安全性问题

当使用大语言模型处理涉及敏感数据的战略军事冲突时，数据隐私和安全性将成为关键问题。这些战略任务常常涉及高度敏感的信息，如政治动态、军事行动以及战略决策等。如果未能妥善管理和保守这些信息，将可能导致机密数据的泄露，这不仅威胁到个人和组织的安全，还会影响到国家安全。因此，在使用大语言模型进行战略冲突分析时，必须实施严格的数据保护措施。这包括采用通信加密技术以保护数据传输，实施严格的机密数据访问控制，以及采用匿名化或伪匿名化处理敏感信息，以减少对数据隐私和安全性的侵犯风险。此外，考虑开发和应用面向隐私保护的大语言模型相关技术，如差分隐私和联邦学习^[29]，进一步加强模型在处理敏感数据时的安全性和可靠性。

5.2 幻觉和可解释性问题

在缺乏充分证据支持的情况下，大语言模型可能会生成看似合理但实际上并不准确的输出，即“幻觉”，从而削弱了输出信息的可信度。不准确的信息可能会导致错误的冲突建模，进而影响到后续的冲突分析和冲突消解。此外，由于无法始终保证大语言模型所学习的开源冲突案例数据的质量，因此，生成的结果可能会存在偏差^[30]，这同样会降低模型输出的可信度。同时，由于神经网络复杂的多层非线性结构和大量参数，大语言模型的内部决策过程往往难以被直观理解和追踪，导致其模型可解释性相对较弱，因此，需要采取措施减少“幻觉”现象和增强模型的可解释性。首先，考虑引入智能外部知识库，并要求模型在输出事实性的论述时，必须提供数据的来源并对其进行引用链

接。其次,可以考虑通过调整模型输出的置信度,以提升模型的整体数据的可靠性。

5.3 数据时效性问题

冲突分析领域高度重视冲突有关信息的时效性,以做出快速响应和精准决策。然而,由于大语言模型训练的时空开销通常较大,且生成流程较为复杂,导致其在数据迭代和新数据学习上存在一定的不足。具体而言,大语言模型需要对海量数据进行长时间的大规模训练,以完善其知识库,且难以迅速接收并融入新知识。因此,确保冲突数据的时效性是使用大语言模型进行有效冲突建模和分析的关键。为了克服数据时效性问题,考虑建立快速响应的数据更新机制,包括自动收集最新的开源案例信息和整合来自冲突局势的实时数据。此外,大语言模型的训练和优化过程也应定期进行,以不断适应新的冲突动态。

6 结束语

随着人工智能技术的快速发展,面对复杂多变的冲突局势,以数据驱动和模型驱动为核心的智能化冲突分析将会成为未来冲突分析领域发展的主流方向。本文提出了基于大语言模型的冲突分析框架,对大语言模型在冲突分析领域的应用做了积极的理论框架探索,有效解决了经典的冲突分析方法在面对复杂冲突态势和海量冲突数据时的局限性。随后,本文介绍了该框架关键部分的技术实现。此外,还着重讨论了大语言模型对冲突分析领域的能力增强及其潜在的风险和挑战。然而,该理论框架需要进一步的实践验证,随着关键技术的不断突破和落地,可以预见智能化的冲突分析将在决策效率和准确性上实现

更为显著的提升。

参考文献

- 1 牛铨瑶. 习近平大数据观研究 [D]. 南昌: 江西财经大学, 2020.
- 2 THIRUNAVUKARASU A J, TING D S J, ELANGO VAN K, et al. Large language models in medicine [J]. *Nature medicine*, 2023, 29 (8): 1930-1940.
- 3 阮彤, 卞俣昂, 余广涯, 等. 医学大语言模型研究与应用综述 [J]. *中国卫生信息管理杂志*, 2023, 20 (6): 853-861.
- 4 吴武清, 赵煜东, 赵越, 等. GPT等大语言模型在会计与审计中的应用 [J]. *国际商务财会*, 2023 (22): 81-87.
- 5 张春红, 杜龙飞, 朱新宁, 等. 基于大语言模型的教育问答系统研究 [J]. *北京邮电大学学报 (社会科学版)*, 2023, 25 (6): 79-88.
- 6 韩旭, 孙亚伟, 赵璐. 体系化人工智能与大语言模型在智能情报场景中的应用 [J/OL]. *北京邮电大学学报*, 1-9 [2024-07-10].
- 7 吴心伯. 论中美战略竞争 [J]. *世界经济与政治*, 2020, 5: 96-130.
- 8 HIPEL K W, FANG L, KILGOUR D M. The graph model for conflict resolution: Reflections on three decades of development [J]. *Group Decision and Negotiation*, 2020, 29 (1): 11-60.
- 9 董艺博, 葛冰峰, 黄宇铭, 等. 基于概率强度偏好的冲突分析图模型方法 [J/OL]. *系统工程与电子技术*, 1-10 [2024-07-10].
- 10 KILGOUR D M, HIPEL K W, FANG L P. The graph model for conflicts [J]. *Automatica*, 1987, 23 (1): 41-55.
- 11 FANG L P, HIPEL K W, KILGOUR D M. Conflict models in graph form: Solution concepts and their interrelationships [J]. *European Journal of Operational Research*, 1989, 41 (1): 86-100.
- 12 黄宇铭, 葛冰峰, 侯泽强, 等. 基于冲突分析图模型的多无人机协同空战博弈 [J]. *系统工程理论与实践*, 2023, 43 (9): 2714-2725.
- 13 于晶, 张飞羽. 基于决策成本的军事冲突图模型 [J/OL]. *系统工程理论与实践*, 1-10

- [2024-06-17].
- 14 KASNECI E, SEBLER K, KÜCHEMANN S, et al. ChatGPT for good? On opportunities and challenges of large language models for education [J]. *Learning and individual differences*, 2023, 103: 102274.
 - 15 ZHAO W X, ZHOU K, LI J, et al. A survey of largelanguage models [J]. *arXiv preprint arXiv: 2303. 18223*, 2023.
 - 16 VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need [J]. *Advances in neural information processing systems*, 2017, 30.
 - 17 张钦彤, 王昱超, 王鹤羲, 等. 大语言模型微调技术的研究综述 [J/OL]. *计算机工程与应用*, 1-22 [2024-07-10].
 - 18 NASH J. Non-cooperative games [J]. *Annals of Mathematics*, 1951, 54 (2): 286-295.
 - 19 HOWARD N. Paradoxes of rationality: Theory of metagames and political behavior [M]. Cambridge, MA: MIT Press, 1971.
 - 20 RÊGO L C, VIEIRA G I. Symmetric sequential stability in the graph model for conflict resolution with multiple decision makers [J]. *Group Decision and Negotiation*, 2017, 26 (4): 775-792.
 - 21 HAN Y, XU H Y, Ginger Y K. Construction and application of hyper-inverse conflict models based on the sequential stability [J]. *EURO Journal on Decision Processes*, 2020, 8: 237-259.
 - 22 LI J, SUN A, HAN J, et al. A survey on deep learning for named entity recognition [J]. *IEEE transactions on knowledge and data engineering*, 2020, 34 (1): 50-70.
 - 23 黄恒琪, 于娟, 廖晓, 等. 知识图谱研究综述 [J]. *计算机系统应用*, 2019, 28 (6): 1-12.
 - 24 OUYANG L, WU J, JIANG X, et al. Training language models to follow instructions with human feedback [J]. *Advances in neural information processing systems*, 2022, 35: 27730-27744.
 - 25 ZHOU Z, SHI J X, SONG P X, et al. LawGPT: A Chinese Legal Knowledge-Enhanced Large Language Model [J]. *arXiv preprint arXiv: 2406. 04614*, 2024.
 - 26 孙凯丽, 罗旭东, 罗有容. 预训练语言模型的应用综述 [J]. *计算机科学*, 2023, 50 (1): 176-184.
 - 27 郝博文, 柳溢菲, 李立耀, 等. 基于多模态推荐指令的大语言模型指令微调 [J/OL]. *北京邮电大学学报*, 1-7 [2024-06-17].
 - 28 李茹杨, 彭慧民, 李仁刚, 等. 强化学习算法与应用综述 [J]. *计算机系统应用*, 2020, 29 (12): 13-25.
 - 29 刘艺璇, 陈红, 刘宇涵, 等. 联邦学习中的隐私保护技术 [J]. *软件学报*, 2022, 33 (3): 1057-1092.
 - 30 徐磊, 胡亚豪, 潘志松. 针对大语言模型的偏见性研究综述 [J/OL]. *计算机应用研究*, 1-14 [2024-06-17].

多智能体决策新范式：强化学习与大模型 融通演进技术分析及其军事应用展望**

张伊丹^{1,2} 陈展^{1,2} 赵新昱^{1,2*} 王磊^{1,2} 贾婕^{1,2} 刘晓暄^{1,2}

摘要 随着人工智能技术的飞速发展，多智能体决策技术作为作战规划、军事决策等任务的有力支撑，正逐步向强化学习与大模型融合的新范式演进。这一技术通过结合 GPT-4 等大语言模型，显著提升了智能体在复杂军事环境中的感知、认知和决策能力。相较于传统强化学习方法，新范式在适应性和决策效率方面优势显著。文章在剖析多智能体决策技术原理及传统方法局限性的基础上，深入分析强化学习与大模型的融合演进技术，并对其军事应用潜力进行展望。

关键词 多智能体决策，大语言模型，强化学习，强化学习与大模型融通演进

A New Paradigm in Multi-Agent Decision: Analyzing the Integration of Reinforcement Learning with Large Language Models and Exploring Military Application Prospects**

ZHANG Yin-Dan^{1,2} CHEN Zhan^{1,2} ZHAO Xin-Yu^{1,2*}
WANG Lei^{1,2} JIA Jie^{1,2} LIU Xiao-Xuan^{1,2}

Abstract With the rapid advancement of artificial intelligence technology, multi-agent decision has become crucial for military decision making and combat planning, evolving into a paradigm integrating reinforcement learning with large language models (LLMs) like GPT-4. This integration significantly enhances agents' perception, cognition, and decision in complex military environments, surpassing traditional methods in adaptability and efficiency. This paper examines the principles and limitations of traditional multi-agent decision methods, analyzes the integration of reinforcement learning with LLMs, and explores its potential military applications.

Key words multi-agent decision, large language models, reinforcement learning, integration of reinforcement learning with large language models

** 中国科学院重点实验室基金 (CXJJ-23S032)、中国科学院空天信息研究院科学与颠覆性技术研究基金 (2024-AIRCAS-SDTP-03) 资助

** Supported by the Key Laboratory Fund of the Chinese Academy of Sciences (CXJJ-23S032) and the Disruptive Fund of Aerospace Information Innovation Research Institute (2024-AIRCAS-SDTP-03)

* 通讯作者

1. 中国科学院空天信息创新研究院目标认知与应用技术重点实验室 2. 中国科学院空天信息创新研究院网络信息体系技术重点实验室

1. Key Laboratory of Target Cognition and Application Technology (TCAT), Aerospace Information Research Institute 2. Key Laboratory of Network Information System Technology (NIST), Aerospace Information Research Institute

0 引言

随着智能化时代的到来，现代战争的节奏不断加快，复杂性亦随之攀升。在战争这一充满“不确定性”的领域内，仅凭传统作战原则和指挥员直觉，寻求有效决策方案的难度日益加大。随着人工智能技术的兴起，早期强化学习智能体技术开始在辅助决策等任务上得到应用，由于其高度关联模型训练环境，难以应对快速变化的真实决策场景。随着大语言模型的出现，凭借大语言模型通识理解、推理能力，多智能体决策技术开始具备复杂环境中的自主感知、认知和对抗能力，为充分探索战争决策空间提供了新的视角。它能够助力指挥员发现和锚定决策点，以更高的效率制订和优化行动方案。

本文聚焦多智能体决策技术，在回顾传统强化学习智能体、新兴大语言模型智能体方法的基础上，重点探讨强化学习与大模型融合演进技术，并对其在军事辅助决策、兵棋仿真推演等领域的应用进行了分析与前瞻性展望。

1 多智能体决策简述

1.1 概念简述

智能体，通常被定义为具备自主性、反应性、主动性和社交能力的计算实体。它能够感知周围环境，并据此采取行动以实现预设目标。例如，在复杂多变的战场环境中，无人机能自主协调，执行侦察和精准打击任务。

这些智能体普遍具有以下核心特性：

(1) 自主性：智能体能够独立行动，无须外界的直接控制或人为干预。

(2) 反应性：面对环境中的突发变化，智能体能够迅速响应，并做出相应调整。

(3) 主动性：智能体不仅对环境变化做出反应，更能主动设定并追求目标。

(4) 交互性：智能体之间能够进行信息交换与协作，以实现共同的目标。

智能体的运行过程涵盖了感知、决策与行动三个关键阶段。首先，通过感知来收集环境信息；其次，基于当前状态生成决策方案；最后，执行决策所确定的行动。

多智能体决策则是指多个智能体在复杂多变的环境中，通过相互协作或竞争，结合自身的局部决策集合和感知到的环境信息，共同决定最优解决方案的过程。其核心在于，在复杂多变的环境下，多智能体如何制定出最优决策策略以最大化决策效益。

1.2 技术发展简述

为实现多智能体决策效益的最大化，如图 1 所示，当前的研究主要可以分为 3 类，包括强化学习多智能体技术、大语言模型多智能体技术和强化学习与大模型融通演进多智能体技术。

强化学习多智能体技术通过构建环境-智能体交互反馈机制，促进智能体的学习和演进；大语言模型多智能体技术则依托于大模型的知识储备和推理能力，以实现高效的决策制定；进一步地，将强化学习与大语言模型的优势相结合，可提升多智能体决策的可靠性，并深化对军事等特定领域的理解能力，这是当前的热点研究方向。



图1 多智能体决策技术发展及相关工作

$$R: S \times A \rightarrow [0, 1] \quad (2)$$

$$O: S \times A \times \Omega \rightarrow [0, 1] \quad (3)$$

2 传统多智能体决策技术原理

2.1 强化学习多智能体技术

强化学习 (Reinforcement Learning, RL)^[1], 又称为增强学习, 其核心思想是试错机制, 即让智能体在与环境的交互中, 通过执行动作并接收环境反馈的“奖励”来自我学习。智能体在与环境的交互过程中不断尝试、修正动作, 以获得最大的累计奖励。

多智能体强化学习 (Multi Agent Reinforcement Learning, MARL)^[2] 通常可以被描述为马尔可夫决策过程 (Markov Decision Process, MDP)^[3]。鉴于在多数实际应用场景中, 智能体往往无法直接获取环境的完整状态信息, 因此, 它们更多地被建模为部分可观察马尔可夫决策过程 (Partially Observable Markov Decision Process, POMDP)^[4]。一个 POMDP 由七元组 $(S, A, T, R, \Omega, O, Y)$ 定义, 其中 S 表示状态集合, A 表示动作集合, T 表示状态转移概率矩阵 $T(s'|s, a)$, R 表示奖励函数 $R(s, a)$, Ω 表示观察集合, O 表示观察概率函数 $O(o|s', a)$, Y 表示折扣因子。主要变量数域范围如下:

$$T: S \times A \times S \rightarrow [0, 1] \quad (1)$$

在此基础上, 如表 1 所示, 根据多智能体学习方式的不同, 强化学习多智能体技术可划分为独立学习和联合学习两类方式。

(1) 独立学习: 每个智能体独立与环境互动, 仅依赖自身观测和奖励值来更新策略, 缺乏智能体间交流, 效果有限。其中, 深度确定性策略梯度 (DDPG)^[5] 使用深度神经网络直接学习确定性策略, 近端策略优化 (PPO)^[6] 通过调整目标函数限制策略更新的步长, 从而提高训练的稳定性, 软演员-评论家算法 (SAC)^[7] 则提出行动-评价机制, 优化在各种连续动作任务上的表现。

(2) 联合学习: 智能体间通过显式、隐式通信模块和信息共享模块实现信息与知识交互, 整合了更多的状态、动作信息, 但运行效率有待提升。多智能体深度确定性策略梯度 (MADDPG)^[8] 在单个智能体决策中引入对合作智能体的动作预期, 优化了综合策略目标, 价值混合算法 (QMIX)^[9] 构建全局-个体混合价值函数, 将全局动作分解为单个智能体的动作, 星际争霸 2 智能体 (AlphaStar)^[10] 则同时采用有监督回放学习和强化学习机制, 大幅提高智能体的潜在学习空间。

通过独立学习和联合学习方式，强化学习多智能体技术已广泛应用于围棋、游戏、仿真控制等目标明确且能够交互的应用场景。

表 1 近年主流强化学习多智能体方法

类别	方法	年份	特点
独立学习	DDPG ^[5]	2016	使用神经网络直接学习策略
	PPO ^[6]	2017	目标函数限制更新步长
	SAC ^[7]	2018	行动-评价机制
联合学习	MADDPG ^[8]	2017	合作智能体动作预期
	QMIX ^[9]	2018	全局-个体混合价值函数
	AlphaStar ^[10]	2019	有监督回放学习+强化学习

2.2 优势与局限性分析

基于强化学习的多智能体决策技术，其优势明显。与传统的监督学习不同，它无须预先定义的标签，而是依赖智能体与环境间的互动，通过执行动作并接收环境反馈的“奖励”来实现自我学习。这一独特机制，使得该技术能够摆脱对大量数据样本的依赖，进而更好地适应真实世界中标签稀缺的场景。更为重要的是，这种学习模式更贴近实际决策过程，智能体能够探索更广泛的策略-动作空间，并擅长学习那些复杂且稀有的策略。

然而，强化学习的方法亦有其局限性。由于主要依赖奖励来指导多智能体的行为，其生成的策略缺乏直观的可解释性。此外，强化学习多智能体对交互环境高度依赖，这使得跨环境和跨任务的迁移变得尤为困难，难以在小样本或零样本情况下实现有效的泛化。这些限制无疑对多智能体决策技术的广泛应用构成了挑战。

3 大语言模型多智能体技术

随着 ChatGPT 的惊艳亮相^[11]，大语言

模型在人工智能领域取得了里程碑式的成功。与传统的强化学习方法不同，大语言模型并不依赖于孤立或受限的环境来获取知识。相反，它们通过深度挖掘海量的训练数据，并巧妙运用庞大的模型参数，积累了大量的世界通用知识。这些知识的表达不仅具有高度的可解释性，还展现出了对小样本甚至零样本学习场景的非凡适应性。基于这一强大能力，前沿研究开始积极探索，采用大语言模型构建自主智能体（LLM-based Agent），以获得类似人类的决策规划能力。

然而，大语言模型在转化为能够自主决策的多智能体时，仍面临一系列挑战。具体而言，这些模型尚需明确指定在特定任务或场景中的角色身份，以及增强记忆和动作执行能力。为了解决这些问题，当前研究工作已经开发出一系列增强模块，以拓展大语言模型多智能体的能力边界，如表 2 所示。

(1) 身份模块：通过手动指定、大语言模型生成和数据集对齐等方式设定智能体身份，优化智能体决策背景。其中 MetaGPT^[12]通过模拟组织内不同岗位的角色划分，大幅提高了软件工程的开发效率与代码生成质量。

(2) 记忆模块：存储和利用交互历史信息进行决策优化，增强智能体决策的稳定性。其中，航行者智能体（Voyager）^[13]在世界游戏中通过构建可访问的历史技能库，大幅提高了智能体面对重复相似场景的决策稳定性和可靠性。

(3) 规划模块：利用大模型的规划能力进行任务分解和任务路径规划，提高智能体决策的可执行性。其中，思维链（CoT）^[14]技术对单个任务构建分步骤多轮推理机制，大幅提高多轮决策准确性。

(4) 动作模块：将大语言模型（LLM）

的决策转换为具体的行动与控制指令，便于进行动作执行。其中，工具变压器算法 (Toolformer)^[15]通过在监督训练目标序列中融入控制应用程序接口 (API)，提升了智能体在动作控制上的可靠性。

表 2 近年主流大语言模型多智能体相关方法

方法	年份	特点
MetaGPT ^[8]	2023	直接指定智能体身份，智能体间职责拆分
Voyager ^[9]	2023	可存储访问历史策略
CoT ^[10]	2022	单个决策拆解成多步推理
Toolformer ^[11]	2023	融合文本、控制输出指令

尽管大语言模型多智能体以其广泛的世界知识和卓越的推理技能广受认可，然而，由于其在训练过程中采取的完全无监督学习方法以及主要依赖于可公开访问的互联网文本作为训练语料，当面临特定领域或场景，如军事作战辅助决策、无人机群协同作战时，实现对多智能体行为的精确控制和决策生成的挑战依然显著。

4 强化学习与大模型融通演进技术

4.1 基于强化学习对齐的大语言模型智能体技术

为解决大语言模型智能体在军事决策、作战规划等特定领域应用的挑战，将擅于“试错和探索”的强化学习与大语言模型进行融合，成为一种备受瞩目的解决方案。强化学习可以作为一项工具，减少大语言模型与特定领域之间的差异，并通过指令微调和偏好对齐方法，确保智能体与人类偏好以及特定应用场景的需求保持一致。

ChatGPT 采用了一种创新的人类反馈强化学习 (Reinforcement Learning from Human Feedback, RLHF)^[16] 机制。RLHF 技术通过整合人类的反馈，构建了一个奖励神经网络模型，用以生成奖励信号。这些信号指导多智能体的学习过程，有效对齐了人类偏好与模型的优化目标。

自我博弈偏好优化 (Self-Play Preference Optimization, SPO)^[17] 技术专注于更细致地调整大语言模型智能体以适应特定领域的任务。通过在训练过程中引入多样化、细粒度的对齐策略，并执行多轮微调，SPO 显著增强了智能体在特定应用场景中的决策能力。

然而，鉴于大语言模型主要通过语言进行交互，必须将智能体的状态、动作和环境奖励转化为自然语言形式，才能驱动大语言模型智能体进行有效决策。

4.2 大模型增强的强化学习多智能体技术

相较于依赖语言驱动的大语言模型智能体技术，结合大语言模型、视觉模型来增强强化学习多智能体决策能力，正逐渐成为研究领域的新趋势。这些大模型充当了强化学习多智能体的大脑、感官等，通过有效注入真实世界的知识，显著提升了决策的效率和能力。

Du 等^[18] 的研究表明，通过将大语言模型集成到强化学习多智能体的“大脑”中，可以利用其丰富的先验知识和推理能力来生成更加精确和稠密的奖励信号。这种方法能引导智能体进行高效的探索，减少了学习可行策略所需的交互次数，提高了样本的利用效率。

Cao 等^[19] 与 Carta 等^[20] 则提出利用大语言模型辅助构建智能体奖励函数，通过优化智能体的决策目标，使强化学习框架

具备更高的学习空间，减少智能体面对小概率事件的不确定性。

DeepMind 公司则提出一种统一的智能体架构 U-Agents^[21]。在大语言模型的基础上，U-Agents 还融合了视觉大模型作为智能体的“感知器官”，使其能够处理多模态信息，进而完成环境感知—任务分解—策略优化等任务。

将大模型作为强化学习多智能体的“大脑”和“手脚”，已成为当前研究的前沿趋势。这一方法不仅有助于解决强化学习中奖励稀疏和样本效率低下的难题，还为强化学习多智能体在实际任务中的大规模应用提供了有力支持。

总体而言，如表 3 所示，多智能体决策技术正朝着强化学习与大模型深度融合的新范式演进。通过运用大模型编码的通用知识，结合强化学习的策略优化范式，能够打造出高效解决具体决策任务的 AI 智能体。这一趋势不仅为人工智能的发展注入了新的活力，还有望成为解锁人工智能在军事决策等领域广泛应用的关键所在。

表 3 强化学习与大模型融通演进相关工作

类别	方法	年份	特点
基于强化学习对齐的大语言模型智能体技术	ChatGPT-RLHF ^[16]	2022	通过强化学习将大语言模型智能体与指定领域的需求对齐，指定领域决策能力强
	DPO ^[17]	2024	
	SPO ^[17]	2024	
大模型增强的强化学习多智能体技术	ELLM ^[18]	2023	将大模型作为强化学习多智能体的“大脑”和“手脚”，决策效率高、泛化性强
	U-Agents ^[21]	2023	
	RL4Sugg ^[22]	2024	

5 军事应用与展望

在人工智能技术的浪潮中，以强化学习、大语言模型为核心的多智能体决策技术，为军事领域注入了新的活力与机遇。

这些技术在军事辅助决策、兵棋仿真推演、武器装备组合选择以及无人机编队控制等方面展现出显著优势，预示着军事领域将迎来更加智能化和高效化的未来。

5.1 典型军事应用

军事辅助决策：美国大数据分析公司 Palantir 推出的人工智能平台产品（Artificial Intelligence Platform, AIP），利用大语言模型协助军事规划，可被用于自动目标识别及监视、战场分析等。相比于早期军事辅助 AI 系统强依赖于历史决策数据标注，AIP 能够凭借更广泛的通识知识，理解自然语言查询，使得指挥官能够以对话的方式与系统交互，获取定制化的决策支持^[23]。

兵棋仿真推演：美国国防高级研究计划局（Defense Advanced Research Projects Agency, DARPA）的“兵棋推演 2025”项目结合了强化学习多智能体算法和大数据分析技术，通过模拟未来战场情景，评估新兴技术对战争形态的影响。瑞典国防研究机构开发的“多域兵棋”（Multi-Domain Wargame）也是一个值得关注的案例，它模拟陆、海、空、天、电等多域作战环境，帮助军事分析师和指挥官理解跨域协同作战的复杂性。

武器装备组合选择：美国空军研究实验室（AFRL）开发的“武器优化工具”（Weapon Optimization Tool, WOT）是一个基于人工智能的决策支持系统。该系统运用强化学习算法，能够根据战场环境、敌我双方的装备性能参数和预期的作战目标，智能推荐最优的武器装备组合方案。此外，WOT 还能预测敌方可能的反制措施，为指挥官提供更为全面的决策依据。

无人机编队控制：美国海军研究办公室（ONR）推出的“低成本无人机蜂群技

术” (Low-Cost UAV Swarm Technology, LOCUST) 项目, 利用强化学习技术实现了无人机编队的自主控制^[24]。该项目开发的无人机通过强化学习多智能体算法, 能够根据实时战场信息自我调整飞行路径和战术动作, 以适应复杂的战场环境和敌方的防御措施。

5.2 未来展望

随着技术不断落地应用, 强化学习多智能体技术在军事领域的应用已日渐广泛, 大语言模型多智能体技术也在辅助决策、任务规划等方面展现出巨大的潜力。然而, 大语言模型多智能体技术仍面临数据稀缺与安全性的双重挑战。军事环境的对抗性、欺骗性和谋略性要求数据集必须具备高质量和多样性, 而当前数据集构建的难度与潜在的“杂质”问题不容忽视。此外, 数据驱动的大模型在应对战场的快速变化时, 可能存在响应延迟和决策失误的风险。

进一步地, 作为新兴的决策范式, 强化学习与大模型融通的多智能体技术虽处于初期阶段, 但其在游戏仿真与机器人模拟领域中的成功实践已经预示着在军事领域的巨大应用潜力。特别是在开放式战场环境和复杂任务中, 该技术展现出较大的前景。

展望未来, 强化学习与大模型融通演进的新范式将逐步赋能无人作战、人机协同作战等领域, 推动军事决策向智能化和自动化的更高阶段发展。

参考文献

- 1 Kaelbling L P, Littman M L, Moore A W. Reinforcement learning: A survey [J]. Journal of artificial intelligence research, 1996, 4: 237-285.
- 2 DORRI A, KANHERE S S, JURDAK R. Multi-agent systems: A survey [J]. IEEE Access, 2018, 6: 28573-28593.
- 3 PUTERMAN M L. Markov decision processes [J]. Handbooks in operations research and management science, 1990, 2: 331-434.
- 4 LILLICRAP T P, HUNT J J, PRITZEL A, et al. Continuous control with deep reinforcement learning [J]. arXiv preprint arXiv: 1509. 02971.
- 5 SCHULMAN J, WOLSKI F, DHARIWAL P, et al. Proximal policy optimization algorithms [J]. arXiv preprint arXiv: 1707. 06347.
- 6 HAARNOJA T, ZHOU A, ABBEEL P, et al. Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor [C] // International conference on machine learning. PMLR, 2018: 1861-1870.
- 7 LOWE R, WU Y I, TAMAR A, et al. Multi-agent actor-critic for mixed cooperative-competitive environments [J]. Advances in neural information processing systems, 2017, 30.
- 8 RASHID T, SAMVELYAN M, DE W C S, et al. Monotonic value function factorisation for deep multi-agent reinforcement learning [J]. Journal of Machine Learning Research, 2020, 21 (178): 1-51.
- 9 VINYALS O, BABUSCHKIN I, CZARNECKI W M, et al. Grandmaster level in StarCraft II using multi-agent reinforcement learning [J]. Nature, 2019, 575 (7782): 350-354.
- 10 BROWN T, MANN B, RYDER N, et al. Language models are few-shot learners [J]. Advances in neural information processing systems, 2020, 33: 1877-1901.
- 11 HONG S, ZHENG X, CHEN J, et al. Metagpt: Meta programming for multi-agent collaborative framework [J]. arXiv preprint arXiv: 2308. 00352, 2023.
- 12 WANG G, XIE Y, JIANG Y, et al. Voyager: An open-ended embodied agent with large language models [J]. arXiv preprint arXiv: 2305. 16291, 2023.
- 13 WEI J, WANG X, SCHUURMANS D, et al. Chain-of-thought prompting elicits reasoning in

- large language models [J]. Advances in neural information processing systems, 2022, 35: 24824–24837.
- 14 SCHICK T, DWIVEDI-YU J, DESSÌ R, et al. Toolformer: Language models can teach themselves to use tools [J]. Advances in Neural Information Processing Systems, 2024, 36.
- 15 CHRISTIANO P F, LEIKE J, BROWN T, et al. Deep reinforcement learning from human preferences [J]. Advances in neural information processing systems, 2017, 30.
- 16 RAFAILOV R, SHARMA A, MITCHELL E, et al. Direct preference optimization: Your language model is secretly a reward model [J]. Advances in Neural Information Processing Systems, 2024, 36.
- 17 SWAMY G, DANN C, KIDAMBI R, et al. A min-maximalist approach to reinforcement learning from human feedback [J]. arXiv preprint arXiv: 2401.04056, 2024.
- 18 DU Y, WATKINS O, WANG Z, et al. Guiding pretraining in reinforcement learning with large language models [C] //International Conference on Machine Learning. PMLR, 2023: 8657–8677.
- 19 CAO Y, ZHAO H, CHENG Y, et al. Survey on large language model – enhanced reinforcement learning: Concept, taxonomy, and methods [J]. arXiv preprint arXiv: 2404.00282, 2024.
- 20 CARTA T, ROMAC C, WOLF T, et al. Grounding large language models in interactive environments with online reinforcement learning [C] //International Conference on Machine Learning. PMLR, 2023: 3676–3713.
- 21 DI P N, BYRAVAN A, HASENCLEVER L, et al. Towards a unified agent with foundation models [J]. arXiv preprint arXiv: 2307.09668, 2023.
- 22 WANG Z, GAN B, SHI W. Multimodal Query Suggestion with Multi – Agent Reinforcement Learning from Human Feedback [J]. arXiv preprint arXiv: 2402.04867, 2024.
- 23 王明程, 王高开, 李勇男. 基于大模型智能体的安全风险态势感知框架构建 [J/OL]. 情报理论与实践: 1–13 [2024–06–17]. <http://kns.cnki.net/kcms/detail/11.1762.G3.20240325.1635.002.html>.
- 24 樊琼剑, 杨忠, 方挺, 等. 多无人机协同编队飞行控制的研究现状 [J]. 航空学报, 2009, 30 (4): 683–691.

基于 PP-LCNet 微调的电子器件文档解析

吴栢畅¹ 陈泓材^{1*}

摘要 工程师设计电路时通过翻阅大量文档来获得电子器件的信息,效率低,工作量大,通过人工智能自动解析文档可大幅提升工程师效率,但是当前的文档布局分析模型针对的是各种类型的文档,并不适用于电子器件文档,文章使用 PP-LCNet 网络来实现用于文档分析的大模型中的文档布局分析功能,利用自己创建的电子器件文档的数据集进行训练,获得了适用于电子器件文档的模型,能够将电子器件文档内的内容分为 21 类,并且拥有不错的平均精度以及平均召回率,大大提高了模型的检测速度。

关键词 布局分析, 电子器件, 大模型, PP-LCNet 网络

Electronic Device Document Analysis Based on PP-LCNet Fine Tuning

WU Long-Chang¹ CHEN Hong-Cai^{1*}

Abstract When designing a circuit, engineers can obtain information of electronic devices by browsing a large number of documents, which is of low efficiency and heavy workload. Automatic document parsing by artificial intelligence can greatly improve engineers' efficiency. However, the current document layout analysis model is aimed at various types of documents and is not suitable for electronic device documents. In this paper, PP-LCNet network is used to realize the document layout analysis function in the large model for document analysis, and the data set of electronic device documents created by myself is used for training, and a model suitable for electronic device documents is obtained, which can divide the contents of electronic device documents into 21 categories while having a good average accuracy and average recall rate. It also greatly improves the speed of model detection.

Key words layout analysis, electronic devices, large models, PP-LCNet networks

1 背景

电子器件文档是用于电路设计的必备材料,但工程师在设计电路时需要从海量器件文档中提取信息,工作量大且耗时长,借助大模型来解析电子器件文档是一

种新方法。而电子器件文档因其内容的复杂性和重要性,不适用于当前已有的大模型。

1.1 电子器件文档的复杂性与重要性

电子器件文档解析的复杂性主要体现

* 通讯作者

1. 东南大学自动化学院

1. School of automation, Southeast University

在以下几个方面。①电子器件种类繁多，外形各异：目前已知的电子器件种类数以万计，且外形尺寸、形状、颜色、标记等都存在差异。这给文档的识别带来了很大的困难。②电子器件文档信息繁杂：电子器件文档通常包含器件型号、参数、规格、功能等多种信息，这些信息往往以文本、符号、表格等多种形式呈现。如何准确提取和理解这些信息是解析的关键挑战之一。

①电子器件文档的特殊性：电子器件文档通常包含大量图表、符号、表格等非文本信息，且排版布局较为复杂。现有的文档布局分析大模型主要针对文本为主的文档进行训练，难以有效识别和理解电子器件文档中的非文本信息。②多模态信息融合困难：电子器件文档中的信息往往以多模态的形式呈现，如文本、图像、表格等。

尽管电子器件文档解析面临着诸多挑战，但其重要性仍然不容忽视。①提高电子器件信息检索效率：可以帮助快速检索和定位电子器件信息，提高工作效率。②降低人工成本：可以减少人工识别电子器件信息的成本，特别是对于大规模的电子器件文档处理任务。③提高电子器件维修效率：可以帮助快速识别故障电子器件，提高维修效率。

1.2 当前文本布局分析的发展

近年来，随着深度学习技术的快速发展，基于大模型的文档布局分析取得了显著的进展。然而，现有的文档布局分析大模型主要针对通用文档进行设计，对于电子器件文档的分析仍存在一些局限性。

当前主流的针对文档布局分析的大模型主要有 LayoutLMv、PaddleDetection 模型^[1]以及 Dit 模型。

LayoutLMv3 是多模态转换器架构，以统一的方式结合了文本和图片嵌入。文档图像不依赖卷积神经网络进行图像嵌入，而是表示为图像块的线性投影，然后将其线性嵌入并和文本标记对齐。但它的计算资源需求高，数据需求大。

PaddleDetection 是一个全栈式的物体检测平台，涵盖了从数据预处理、模型训练到部署的全过程，提供了多种经典的和最新的检测算法，如 YOLO、Faster R-CNN^[2]、Mask R-CNN^[3]、PP-LCNet 等，并不断更新以跟进研究前沿。虽然其支持多种模型，但某些特定任务可能需要定制化的修改或调整，这可能需要深入理解底层框架和模型结构。

Dit 利用 Transformer 架构的全局自注意力机制，对文档图像进行编码和理解。其核心思想是通过 Transformer 的强大建模能力捕捉文档图像中的复杂关系和特征。但其计算复杂且数据依赖程度高。

另外，由于电子器件文档的特殊性，现有的文档布局分析大模型主要针对通用文档进行设计，对于电子器件文档的分析仍存在一些局限性。在对电子器件文档进行分析时主要将文档分为文字 (text)、标题 (title)、表格 (table)、图片 (figure) 以及列表 (list) 五类，然而对于电子器件文档的分析来说，文档内的各种图对于电子器件的理解有着至关重要的作用，因此，将图片进行细分是非常重要的内容，另外，图片以及表格的题注部分也对图片和表格的分析有着指导作用，但在主流的大模型中总会将其归类为文本部分。

2 方法介绍

PaddleDetection 提供了多种经典的和最新的检测算法，如 YOLO、Faster R -

CNN^[2]、Mask R-CNN^[3]、PP-LCNet，其中，PP-LCNet 是一个基于 MKLDNN 的加速策略轻量级卷积神经网络，是一个能应用于多任务的轻量级模型。图 1 为 PP-LCNet 网络的基本构造。

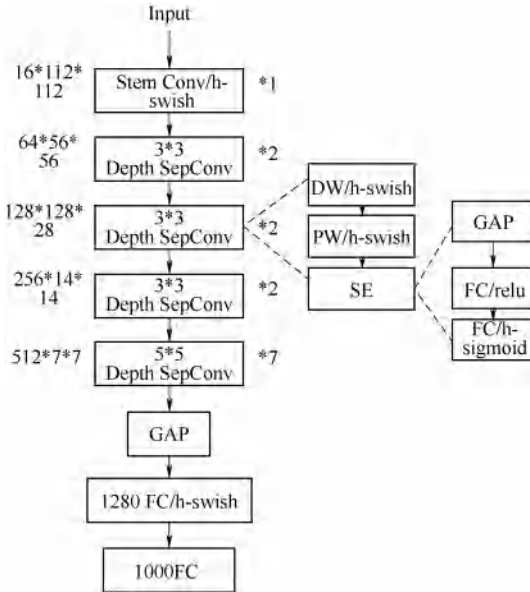


图 1 PP-LCNet 网络基本构造

2.1 H-Swish 激活函数

一般而言，经常使用的激活函数不外乎 tanh、Relu、Sigmoid，还有 bert 中的 Gelu 函数，这里本文使用了一种比较新颖的激活函数 H-Swish^[4]。它是对 Swish 激活函数的改进。公式如式 (1)、式 (2) 所示。

$$H-Swish(x) = x * ReLU6(x + 3)/6 \quad (1)$$

$$ReLU6(x) = \min(\max(0, x), 6) \quad (2)$$

与 Swish 函数相比，H-Swish 引入了一个额外的线性分段函数来近似 Swish 函数的形状。这个线性分段函数使得 H-Swish 具有更简单的计算形式，并且在一定程度上减少了计算量。H-Swish 函数具

有以下特点：在输入为负时，H-Swish 函数保持为线性关系，避免了信号的过度抑制；在输入为正时，H-Swish 函数接近于 Swish 函数，具有非线性特征，可以更好地捕捉输入的特征。

2.2 SE 模块

SE (Squeeze-and-Excitation) 模块是一种用于增强卷积神经网络特征表示能力的模块，它可以自适应地调整通道之间的相互依赖关系。SE 模块最初是在图像分类任务中提出的，但也可以应用于其他计算机视觉任务，如目标检测和语义分割^[5]。

SE 模块的核心思想是通过学习得到每个通道的权重，然后利用这些权重对通道特征进行重新加权。它包含两个主要步骤，如图 2 所示。

压缩阶段 (Squeeze)：在这一步骤中，SE 模块通过全局平均池化操作（或者使用自适应平均池化）将输入特征图的空间维度压缩为一个通道维度的向量。这个向量表示了每个通道的全局信息。激励阶段 (Excitation)：在这一步骤中，SE 模块通过两个全连接层（或者卷积层）对压缩后的向量进行处理。第一个全连接层用于降低维度，第二个全连接层用于生成每个通道的权重。这些权重通过激活函数（通常是 Sigmoid 函数）进行归一化，以表征每个通道的重要性。

最后，SE 模块将这些通道权重与原始特征图相乘，从而实现通道级别的特征重新加权。这样做可以提高网络的表达能力，使得网络更加关注重要的特征通道，抑制不重要的通道，进而提升网络的性能。

SE 模块的引入可以有效地提升模型在各种视觉任务中的准确性。它是一种轻量级且可嵌入不同网络架构中的模块，因此在实践中被广泛采用。

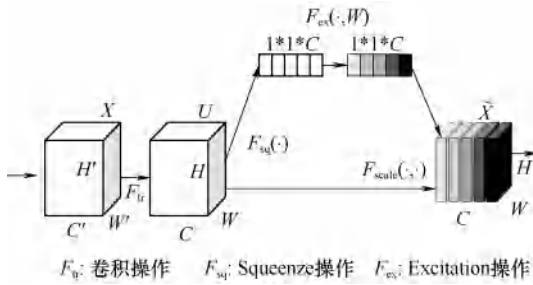


图2 SE 模块

2.3 卷积核

卷积核的大小会影响到网络的性能，在同一层卷积中混合使用大小不同的卷积核会增加预测时间，所以这里在同一层中只使用一种大小的卷积核。在模型中，全局平均池化层后面的维度很小，直接在它后面添加分类层会损失很多特征信息，为了增强模型的鲁棒性，在两者之间添加了1280维、大小为 1×1 的卷积核，这使得模型鲁棒性更好，但只有一点的预测时间提高。

3 实验内容

3.1 数据处理

本文的数据是自己处理电子器件文档数据集，通过对3796张来自电子器件文档的图片进行分析，获得了类别为文本、标题、列表、表格、图片五种类别的输出结果，并在这个基础上进行人工处理，将图片内容进行细分，针对图片功能的不同，本文将图片分为功能框图、流程图、特性曲线图、时序图、电路图、引脚图、工程尺寸图、采样图、3D示意图、引脚名称图、标记图、外观图、功能注册图、布局图、数据结构图、其他部分图16个种类。以下是各种类别的图片的主要作用：

(1) 功能框图：展示了电子器件的功能组成部分和它们之间的关系，用于说明整体架构和功能模块的划分。

(2) 流程图：展示了电子器件或系统中的流程、操作序列或算法的步骤，用于说明工作流程或控制逻辑。

(3) 特性曲线图：显示了电子器件特定参数随着输入或其他条件变化而变化的曲线，用于说明器件的性能和特征。

(4) 时序图：描述了电子器件或系统中不同信号的时间顺序和相对时序关系，用于说明时序逻辑和时序要求。

(5) 电路图：展示了电子器件内部的电路连接和元件的布局，用于说明电路设计和连接方式。

(6) 引脚图：展示了电子器件的引脚和引脚功能的布局，用于说明器件与外部设备的连接方式。

(7) 工程尺寸图：展示了电子器件的物理尺寸和外部结构，用于说明器件的尺寸规格和安装要求。

(8) 采样图：显示了电子器件输出信号的采样数据，用于说明信号波形和信号质量。

(9) 3D示意图：以三维图形形式展示了电子器件的外观或内部结构，用于提供更直观的器件形状和结构信息。

(10) 引脚名称图：展示了电子器件引脚的编号和对应功能的说明，用于帮助用户正确连接器件。

(11) 标记图：为电子器件的各个部分或功能添加标记，用于增加可读性和理解性。

(12) 外观图：展示了电子器件实际外观的照片或图像，用于辅助辨识和外观检查。

(13) 功能注册图：描述了电子器件内部寄存器的功能和位域，用于说明寄存

器的配置和操作方法。

(14) 布局图：展示了电子器件内部元件的布局 and 连接方式，用于说明电路板的布局 and 线路走向。

(15) 数据结构图：描述了电子器件内部数据的组织和关系，用于说明数据的结构和访问方式。

而对于题注部分，针对于大部分题注的标注方式特点，以及会将题注识别为文本的特点，将几何中心与最近的 text 文本视为该图片的题注，但是如果 picture 较长，会出现将图片左右两侧的文本视为图例的可能。因此，增加了 figure 和 text 的中心点的横坐标差值不超过图片长度的十分之一的条件。

在调整好上述过程之后，输出的图片以 json 的形式输出，并将其转换为 COCO 数据集的格式。

COCO 数据集的注释文件通常分为几个主要部分：images、annotations、categories。每个部分都包含特定的信息，并以字典嵌套的方式表达。

其中，images 部分包含图片名称、长宽信息以及图片 id。anntations 表示标注文件中目标物体的标注信息列表，每个元素是一个目标物体的标注信息，包含元素分割标注、区域面积、所处图片的 id、位置信息、元素 id、元素对应的类别 id。categories 包含所有类别名称以及对应 id。值得注意的是，元素的位置信息中包含的是元素左上角像素坐标以及元素的长宽，以一个数组的形式表现出来： $[x1, y1, w, h]$ 。

3.2 模型训练结果

本研究将所获得的 json 文件转化为 COCO 形式的数据集之后，放入 PaddleDetection 对 PP-LCNet 网络进行训练，训练的结果如表 1、表 2 所示。实验的目标检

测结果用平均精度和平均召回率来进行评估，平均精度 (AP) 主要反映了模型在考虑误检 (False Positives) 的情况下，能够正确检测到目标的能力。高 AP 值意味着模型在多个置信度阈值下都能维持高精度。平均召回率 (AR) 主要评估了模型在不同检测数目限制下，能够找到实际存在的目标的能力。高 AR 值意味着模型在不同的检测数目下都能找到大多数的目标。

表 1 平均精度结果表

最大检测数	IoU	区域大小	平均召回率
100	0.50 : 0.95	All	0.665
100	0.50	All	0.711
100	0.75	All	0.686
100	0.50 : 0.95	Medium	0.73
100	0.50 : 0.95	Large	0.666
100	0.50 : 0.95	Small	-1.000

表 2 平均召回率结果表

最大检测数	IoU	区域大小	平均召回率
1	0.50 : 0.95	All	0.655
10	0.50 : 0.95	All	0.915
100	0.50 : 0.95	All	0.916
100	0.50 : 0.95	Medium	0.784
100	0.50 : 0.95	Large	0.916
100	0.50 : 0.95	Small	-1.000

从表中可以发现，在 IoU 阈值为 0.50 时，平均精度为 0.711，而在 IoU 阈值为 0.75 时，平均精度为 0.686。这表明在更高的 IoU 阈值下，模型的性能略有下降。平均召回率在不同最大检测数下表现良好，当最大检测数为 100 时，平均召回率达到了 0.916，说明模型能够有效地检测到大部分目标。

对于中等大小的目标 (medium)，模型的表现最好，平均精度达到了 0.730。平均召回率在不同目标大小下表现一致，都接近

0.9, 表明模型在各个目标大小上都有较好的检测能力。对于小目标, 模型未能提供具体的性能数值, 可能是因为文本布局分析中小目标较少或者不存在导致的。

模型与常用的 Faster R-CNN 以及 Mask R-CNN 进行了对比, 发现模型的精度、召回率都得到了提升, 但提升的效果有限, 但是最重要的是它大大提高了训练的速度以及预测的速度, 如表 3 所示。

表 3 不同模型在 IoU=0.50 : 0.95, area=all 的情况下的表现

模型名称	平均精度	平均召回率	预测时间
Faster R-CNN	0.612	0.816	12.3s
Mask R-CNN	0.634	0.852	15.6s
PP-LCNet	0.613	0.844	1.2s
PP-LCNet	0.665	0.916	1.2s

同时, 本研究将本模型的预测结果与当下主流的模型进行对比, 可以发现本模型与 LatoyLMv3 模型、Dit 模型, 以及 PaddleDetection 原模型的预测结果相差不大, 而本模型更是将图片的细分种类准确地识别了出来, 在与 Faster R-CNN 网络的对比中, 精度明显更高。另外, 更重要的是, 在预测过程中, 本研究发现, 对于每张图片来说, 本模型所需要的时间大约为 1.2s, 远小于其他的几种模型。

综合来看, 模型在检测和定位目标方面表现良好, 但精度仍没有达到较高的结果, 可能是由于数据集数量较少的原因, 但是可以达到其他模型达不到的图片细分的效果, 且在预测速度方面遥遥领先。

4 结束语

本文对基于 PaddleDetection 框架的目

标检测模型进行了重新训练和评估, 旨在细化电子器件文档布局分析中的具体目标类别。实验结果表明, 该模型在多个评估指标上表现出色, 展示了良好的检测能力。

首先, 从平均精度 (AP) 来看, 在所有目标类别、所有尺寸和 IoU 阈值范围 (0.50 : 0.95) 内, 模型取得了 0.665 的平均精度, 这表明模型在综合考虑不同的 IoU 阈值时, 仍能保持较高的检测准确性。在特定的 IoU 阈值下, 模型在 IoU = 0.50 时的平均精度为 0.711, 在 IoU = 0.75 时的平均精度为 0.686, 进一步验证了模型在宽范围的 IoU 阈值下的稳定性和可靠性。

对于不同尺寸的目标, 模型在中等大小目标上的表现尤为突出, 平均精度达到了 0.730, 而在大目标上的平均精度为 0.666。然而, 对于小目标, 模型未能提供具体的性能数值, 可能是由于文档布局分析中小目标较少导致的。

从召回率 (AR) 的角度看, 模型在最大检测数为 100 时, 于各个 IoU 阈值范围 (0.50 : 0.95) 内的平均召回率达到了 0.916, 表明模型能够有效地识别出大多数的目标。在最大检测数为 1 和 10 时, 模型的平均召回率分别为 0.655 和 0.915, 显示出在不同限制条件下, 模型的召回能力仍然保持较高水平。特别是对于大目标, 模型的平均召回率同样达到了 0.916, 而中等目标的平均召回率为 0.784, 再次证明了模型在更大目标上的出色表现。

同时经过对比能够发现, PP-LCNet 模型在平均精度以及平均召回率上对比于 Faster R-CNN 以及 Mask R-CNN 有着一定程度的提升, 在训练以及每张图片的预测的时间长度上有着显著的减少, 这对于多页数的电子器件文档的分析来说, 有着非

常重要的作用。同时，本模型将图片细分为 16 类，并能够准确地预测出不同类别的信息，在对电子器件文档进行进一步的分析时，这细分的类别将能够更好、更快地让模型对电子器件的性能进行分析。

综上所述，本研究的目标检测模型在电子器件文档布局分析中展示了强大的检测能力和鲁棒性，尤其是在中等和大目标的检测上表现优异。后续为了进一步提高模型的精度，可能不断增加数据集的数量。此外，通过集成更多的领域知识和优化模型架构，有望进一步提高模型在复杂文档布局分析任务中的应用潜力。

参考文献

- 1 HUANG Y, LV T, CUI L, et al. LayoutLMv3: Pre-training for Document AI with Unified Text and Image Masking [C] //Proceedings of the 30th ACM International Conference on Multimedia. 2022.
- 2 谌颀, 张袖斌, 肖斌, 等. 基于 Faster-RCNN 深度学习算法的图像识别技术研究 [J]. 机器人产业, 2024 (3): 98-102. DOI: 10.19609/j.cnki.cn10-1324/tp.2024.03.019.
- 3 ZHOU Y, HUANG Z, LIU X, et al. Water leakage detection and its application of turbine floor equipment based on MaskRCNN [C] //2022 4th International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM), Hamburg, Germany. 2022: 567-572. DOI: 10.1109/AIAM57466.2022.00114.
- 4 CHOI K, KIM S, KIM J, et al. Hardware-Friendly Approximation for Swish Activation and Its Implementation [C] //in IEEE Transactions on Circuits and Systems II: Express Briefs. DOI: 10.1109/TCSII.2024.3394806.
- 5 WANG D, SONG D, TANG G, et al. A Fault Diagnosis Method for Rotating Machinery Based on Compressed Sensing and Deep Convolutional Neural Network with SE Block [C] //2022 Global Reliability and Prognostics and Health Management (PHM-Yantai), Yantai, China. 2022: 1-6. DOI: 10.1109/PHM-Yantai55411.2022.9942124.

基于大模型 RAG 微调与增强的智能运维方法

林 白¹ 高锦杰¹ 李宏伟¹

摘要 针对装备业务数字化、信息化、智能化管理升级的迫切需求,装备业务管理信息系统可运用基于大模型的智能运维方法提升管理效率和水平,采取在开源大模型基础上微调并用专家知识增强的范式。然而大模型垂直领域微调不足以激发知识检索增强效果,需要将大模型微调时的指令与知识检索增强服务时的指令对齐,训练运维指令跟随、运维专业知识融入理解和可行方案生成能力。因此,提出了一种基于大模型 RAG 微调与增强的智能运维方法。实验证明,通过离线 RAG 微调能大幅提升线上大模型知识检索增强的效果。

关键词 智能运维, 大模型, 微调, 知识检索增强

Intelligent Operation and Maintenance Method Based on RAG Fine-tuned and Enhanced LLM

LIN Bai¹ GAO Jin-Jie¹ LI Hong-Wei¹

Abstract In response to the urgent need for upgrading the digitalization, informatization, and intelligent management of equipment business systems, the equipment business management information systems can use intelligent operation and maintenance methods based on large models to improve management efficiency and level, adopting the comprehensive paradigm of fine-tuning and expertknowledge on the basis of the open-source large models. However, specific domain fine-tuning is not sufficient to stimulate the effectiveness of RAG for the LLM. It is necessary to align the instructions in the fine-tuning stage of the LLM with the instructions in the RAG application stage, for training to develop the ability of the LLM to follow the instructions, understand the professional knowledge retrieved and then embedded in context, and generate feasible solutions. Therefore, an intelligent operation and maintenance method based on RAG fine-tuned and enhanced LLM is proposed. Experimental results have shown that offline RAG fine-tuning for the LLM can significantly improve the effectiveness of online RAG application.

Key words AIOps, LLM, Fine-tuning, RAG

0 引言

随着装备业务管理数字化、信息化、

智能化升级需求日益迫切,装备业务管理信息系统可利用大模型手段,解决管理中的精准决策、精准规划、精准部署、精准落实、精准检验问题。鉴于网络负载及复

1. 军事科学院系统工程研究院系统总体研究所

1. Institute of Systems Engineering Academy of Military Sciences

杂性的提升,保障业务系统的可靠运行变得越来越重要。因此,当业务系统出现异常故障时,快速有效地进行故障定位与恢复具有重要意义。然而,故障定位与恢复是一项艰巨且耗时的任务,需要大量的专家知识检索与理解操作^[1]。故障定位与恢复要求在有限的时间内快速全面地收集分析日志、指标、故障单等信息,并给出正确的处理措施^[2-3]。传统方法中,面对这些巨量信息,运维工程师需要花费大量的时间来检索和分析数据,因此延误了解决事件和恢复系统功能的时机。同时,运维工程师掌握的专业知识往往具有局限性和时效性,这也会阻碍他们从整体上准确理解和解决故障。此外,采集的故障信息本身存在大量噪声,这会进一步增加故障定位与恢复的难度。

典型的人工智能方法可以用来简化数据分析工作,但运维工程师仍然需要在筛选信息、解释数据、识别根因、制订方案方面投入大量的人力工作^[4]。2022年人工智能大模型方向取得了重大突破,杰森(Jason Wei)等研究发现,当模型达到一定规模时,大模型智力水平出现“涌现”现象^[5],国内外先后发布了一系列先进的大模型,如OpenAI公司的生成式预训练转化器(GPT)、清华大学的一般语言模型(GLM)、阿里巴巴公司的通义千问、百度公司的文心一言等,它们的语言理解能力、生成能力和逻辑推理能力达到人类水平。在系统运维和故障解决领域,系统日志记录了各系统或设备的关键状态和异常告警信息,运维人员积累了大量的专业知识和故障分析与解决案例。大语言模型可以解析大体量数据、识别关键信息,并输出简洁全面的内容,显著减轻运维工程师手动筛选巨量故障信息的负担^[6],这为业务系统的故障定位与恢复提

供了一种有效的途径^[7-8]。

大模型要在运维领域落地应用,无须从零训练,只需在开源的大模型基础上利用垂直领域语料进行微调即可^[9]。同时,针对大模型通常存在“幻觉”、专业知识不足的问题,可通过知识检索增强的方法弥补^[10]。将模型参数微调和RAG知识检索增强生成两种手段相结合^[11],能够快捷地提高大模型在垂直领域的专业理解和生成能力。

凭借大模型的理解与生成能力实现自动理解日志告警、自动检索专家知识与经验、自动生成解决方案,从而提高智能运维效率和水平。为此提出了一种基于大模型RAG微调与增强的智能运维方法^[12]。区别于传统的RAG知识检索增强方法,本文事先进行大模型的RAG知识检索增强微调以提升大模型的RAG上下文理解与生成能力,然后直接从日志异常出发,经过大模型知识检索增强,自动生成运维故障的解决方案。智能运维大模型底座采用清华大学GLM3-6B^[13],并构造RAG运维知识增强问答样本进行了指令监督微调;智能运维系统的日志告警则会自动触发运维大模型搜索报错异常信息、专家知识和案例,通过RAG增强生成得到故障解决方案。对实际运维故障处理案例进行专家评估,结果显示RAG知识检索增强微调对于基于RAG知识增强的大模型运维系统来说是必要的,它能提升大模型在运维领域的专业知识理解与生成能力,大幅提升大模型生成运维方案的可靠性。

1 理论方法

引入基于大模型知识检索微调与增强的智能运维框架(图1)。大模型检索增

强微调方法是利用预先训练的大语言模型（LLM）并在特定数据集上进行进一步训练的过程；大模型检索增强服务是集成检索能力的 LLM 文本生成方法。大模型智能运维系统由运维大模型底座和运维大模型服务两部分组成，并且在大模型训练阶段采取知识检索增强微调措施来提高大模型服务阶段的知识检索增强能力。

1.1 大模型检索增强微调方法

为了克服传统大模型检索增强生成存在的上下文知识理解与使用程度低的问题，考虑在大模型微调阶段，采用 LLM 大模型辅助生成的方法构造 RAG 知识检索增强微调样本，训练大模型的运维指令跟随、运维专业知识融入理解和可行方案生成能力。

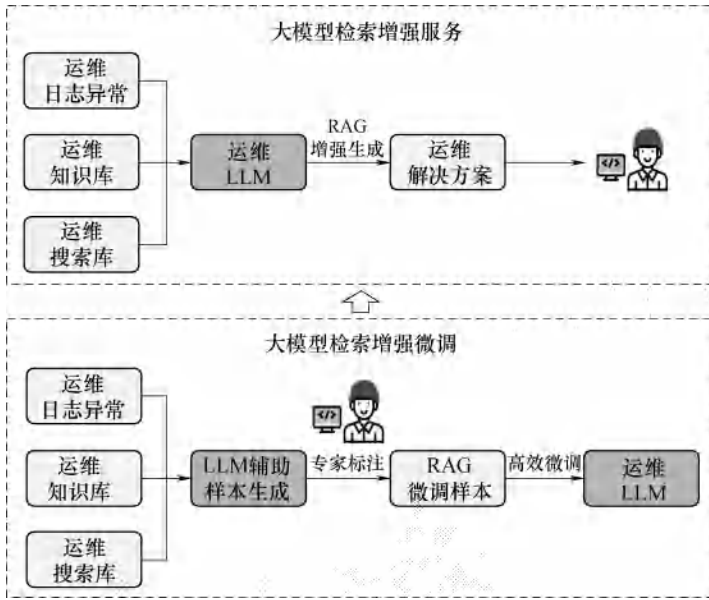


图 1 智能运维系统架构图

1. 微调样本构造

基于历史错误级别的日志异常，通过互联网搜索或知识库检索，收集故障解决知识和案例经验，构造 RAG 检索样本。引入 LLM 大模型通过 Prompt 指令生成最优的参考答案，运维专家进一步修正和标注，构成指令问答对，基于此，构造知识检索增强微调样本示例如下：

Instruction :

你是一个高级运维开发工程师，可以根据报错日志和报错日志相关的专家知识库给出详细的解决方案；如果有多种解决方案的话，将

方案根据可靠性从高到低排序输出；存在多种类似的解决方案，可以对这些方案去重，整理再输出。

错误日志内容如下：

###

1251-Client does not support authentication protocol requested by server; consider upgrading MySQL client

###

报错日志相关的专家知识库，参考如下：

###

专家知识来源 1：

①升级 navicat 驱动；②把 mysql 用户登录密码加密规则还原成 mysql_native_password。方式②需要 Win+R，输入 cmd 打开命令行，进入 MySQL 的 bin 目录，然后输入 mysql -u root -p，输入密码登录。按照以下命令修改即可。

```
ALTER USER 'root'@'localhost' IDENTIFIED BY 'password' PASSWORD EXPIRE NEVER; #修改加密规则
```

```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password'; #更新一下用户的密码
```

```
FLUSH PRIVILEGES; #刷新权限
```

专家知识来源 2:

方法一

修改 root 加密方式

1. 查看 root 或其他用户信息的加密方式

```
[root@centos7 ~] # mysql -u root -p # 登录 mysql
```

```
mysql> use mysql; # 切换 mysql 数据库
```

```
mysql> select user, plugin from user where user='root'; #查看 root 的加密方式
```

2. 改变加密方式

```
alter user 'root'@'%' identified with mysql_native_password by '123456';
```

```
mysql> select user, plugin from user where user='root';
```

方法二

添加用户，同时设置登录加密方式为 mysql_native_password，并且给它远程访问权限，完成后这个用户也可以访问。

添加远程登录用户

```
CREATE USER 'mjh'@'%' IDENTIFIED WITH mysql_native_password BY '123456'; GRANT ALL PRIVILEGES ON *.* TO 'mjh'@'%';
```

###

请根据报错日志相关的专家知识库中的不同知识来源对错误日志提供解决方案。

Output:

根据提供的错误日志和专家知识库，以下是针对“1251-Client does not support authentication protocol requested by server; consider upgrading MySQL client”错误的解决方案，按照可靠性从高到低排序：

方案一：修改 MySQL 用户密码加密规则（最高可靠性）

这个方案通常能够解决客户端和服务端认证协议不匹配的问题。

1. 登录到 MySQL 服务器

```
mysql -u root -p
```

输入密码后进入 MySQL 命令行。

2. 切换到 MySQL 数据库

```
use mysql;
```

3. 修改现有用户的加密方式（如 root 用户）

```
ALTER USER 'root'@'localhost' IDENTIFIED BY 'password' PASSWORD EXPIRE NEVER;
```

```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';
```

这里的 'password' 需要替换为实际的 root 用户密码。

4. 刷新权限

```
FLUSH PRIVILEGES;
```

方案二：创建新用户使用 mysql_native_password 加密（次高可靠性）

如果修改现有用户加密方式不可行，可以创建一个新用户。

登录到 MySQL 服务器上（步骤同上）。

创建新用户并设置密码和加密方式。

```
CREATE USER 'new_user'@'%' IDENTIFIED WITH mysql_native_password BY 'new_password';
```

这里的 'new_user' 和 'new_password' 需要替换为你想创建的用户名和密码。

给新用户授权

```
GRANT ALL PRIVILEGES ON *.* TO 'new_user'@'%';
```

```
FLUSH PRIVILEGES;
```

方案三：升级 MySQL 客户端（可靠性取决于具体情况）

如果上述方案都无法解决问题，可以考虑升级 MySQL 客户端。

对于 Navicat 等第三方工具，升级到最新版本。

对于命令行客户端，确保安装了与 MySQL 服务器版本兼容的客户端版本。

注意：

在实际操作中，建议首先尝试方案一和方案二，因为这些操作不需要升级客户端，对现有环境的影响较小。

方案一和方案二本质上是一致的，只是方案一针对现有用户，方案二是创建新用户。在这里，为了避免重复，只列出了两个主要方案，并进行合并和整理。

按照这个优先级排序，应该能够解决大多数认证协议不匹配的问题。如果问题仍然存在，可能需要进一步检查客户端和服务器的配置以及网络连接情况。

2. 高效微调方法

研究表明，大语言模型在针对下游任务进行微调后，权重参数矩阵通常具有很低的本征秩，即高维度的参数矩阵中存在冗余^[14]。由此，研究人员假设模型微调时权重更新的那部分参数矩阵也是低秩的，并提出多种参数高效微调方法。LoRA (Low-Rank Adaptation) 是其中一种典型的高效微调方法，可以在降低模型微调参数数量和显存占用的同时，使训练后的模型具有与全量微调相当的性能^[15]。LoRA 模型架构图如图 2 所示。

图中左边部分 W_0 是预训练大模型的参数矩阵，右边部分是 LoRA 增加的可训练权重参数 ΔW ，分为 A 、 B 两个低秩分解矩阵，秩为 r 。其中， A 矩阵使用随机高斯分布进行初始化，维度为 $r \times k$ ，负责将输入数据维度降至 r 维； B 矩阵使用 0 进行初始化，维度为 $d \times r$ ，负责将数据维度

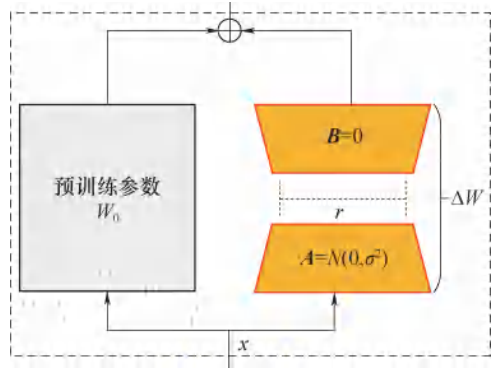


图 2 LoRA 微调模型架构

升至 d 维。LoRA 模型最后的输出为预训练参数部分与可训练参数部分的叠加：

$$h = W_0 x + \Delta W x = W_0 x + B A x \quad (1)$$

LoRA 微调模型降低了微调参数量，且没有引入额外的推理延迟，可以显著改善微调大模型“灾难性遗忘”的问题，是一种高效的参数微调方法。本文选用 LoRA 方法，基于大模型检索增强微调样本对 GLM3-6B 模型进行参数高效微调，构建面向故障定位与恢复领域的基于大模型 RAG 微调与增强的智能运维系统。

1.2 大模型检索增强服务

智能运维系统线上日志异常处理模块会自动触发运维大模型进行分词搜索和向量检索，召回与对应日志故障分析解决密切相关的文档，并综合文档的相关度、质量、有效性等因素对参考文档进行排序。通过 Prompt 指令将最相关的文档资料作为上下文进行大模型 RAG 增强生成，直接得到可靠的解决方案。

2 实验分析

2.1 大模型 RAG 微调分析

为了对基于大模型 RAG 微调与增强的

智能运维方法进行性能分析测试，设计了三个对比模型。第一个模型是没有经过大模型 RAG 微调的原始 GLM3-6B 模型，第二个模型是经过大模型 RAG 微调的 GLM3-6B 模型，第三个模型是经过大模型 RAG 微调与检索增强的 GLM3-6B 模型。使用 OpsEval^[16] 中提出的基于人工打分的专家评估 (Expert Evaluation) 方法确定输出信息的流畅性、准确性、证据量等作为本文分析的评判指标，各项分值范围为 0~5，分数越高，模型性能越好。由 3 名运维领域专家对每个模型的 100 条样本数据问答信息进行打分，取全部打分的平均值作为该模型最终得分，实验结果见表 1。

表 1 专家评估结果

模型	专家评估平均分			
	流畅性	准确性	证据量	总分
GLM3-6B	2.98	2.83	2.16	7.97
RAG 微调模型	3.53	3.98	4.14	11.65
RAG 微调与检索增强模型	3.99	4.45	4.51	12.95

表 1 中的 GLM3-6B 表示清华大学发布的原始 GLM3-6B 模型，RAG 微调模型表示经过大模型 RAG 微调的 GLM3-6B 模型，RAG 微调与检索增强模型表示经过大模型 RAG 微调与检索增强的 GLM3-6B 模型。由表 1 可以看出，经过 RAG 微调与检索增强后的 GLM3-6B 模型在流畅性、准确性、证据量方面显著优于原始 GLM3-6B 模型和经过大模型 RAG 微调的 GLM3-6B 模型。这表明 RAG 微调方法可以增强大模型对专业领域业务问答数据的理解和生成能力，生成更流畅、准确的答案，并提供充足的证据。而通过融合知识检索增强方法，可以进一步增强大模型的专业领域知识，生成更加准确且符合业务要求的分析结果。

2.2 线上效果评测

大模型 RAG 微调后对线上日志告警处理提供服务支撑，由报错日志出发，大模型自动检索相关知识和方案进行 RAG 增强，生成故障解决方案。例如，系统报错如下：

```
ERROR Exiting Kafka due to fatal exception
during startup. (kafka.Kafka$)

kafka.common.InconsistentClusterIdException:
The Cluster ID CaoegNzgQImpR9G-dpg7SQ doesn't
match stored clusterId Some (HyzbmmDkQi-
K8Ai1XFgiaA) in meta.properties. The broker is
trying to join the wrong cluster. Configured zoo-
keeper.connect may be wrong.
```

触发大模型处理流程，生成结果如下：

根据提供的错误日志和专家知识库，以下针对 Kafka 启动时遇到的 InconsistentClusterIdException 异常的解决方案，按照可靠性从高到低排序：

方案一：修改 meta.properties 中的 Cluster ID (最高可靠性)

1. 根据错误日志提示，找到 Kafka 的 server.properties 配置文件中的 log.dirs 配置项。
2. 在指定的 log.dirs 路径下，查找 meta.properties 文件。
3. 打开 meta.properties 文件，找到 cluster.id 属性。
4. 将 cluster.id 的值修改为错误提示中的 Cluster ID (即 CaoegNzgQImpR9G-dpg7SQ)。
5. 保存文件并退出编辑器。
6. 重新启动 Kafka 服务。

方案二：清理 Kafka 日志目录 (次高可靠性)

如果方案一无效，或者你不确定如何准确修改 Cluster ID，可以尝试以下步骤：

再次确认 log.dirs 配置项指定的路径。

删除该路径下的所有文件和文件夹。注意，这个操作将删除所有 Kafka 数据，请谨慎操作。

删除完毕后，重新启动 Kafka 服务。

方案三：检查 Kafka 启动脚本和配置文件路径（中等可靠性）

确保启动 Kafka 时使用的是正确的配置文件。

从 Kafka 的根目录运行启动脚本：

```
bin/kafka - server - start.sh config/server.properties
```

确认 zookeeper.connect 配置项是否指向正确的 Zookeeper 集群。

方案四：升级 JDK 版本（最低可靠性）

检查当前的 JDK 版本是否与 Kafka 兼容。

如果 JDK 版本过旧，尝试升级到更高的版本。注意，这应该是最后考虑的解决方案，因为 JDK 升级可能会影响其他服务。

注意：

方案一和方案二是针对错误日志中提到的具体问题的直接解决方案。

方案三和方案四则是一些辅助性的检查和调整，可能在某些特定情况下有所帮助。

在实际操作中，建议首先尝试方案一，因为它直接解决了 Cluster ID 不一致的问题。

根据以上分析，解决方案已经去重并整理输出。如果问题仍然存在，可能需要进一步检查 Kafka 和 Zookeeper 的配置一致性，以及网络连接和防火墙设置。

按照方案指引操作故障恢复成功。

经过对 200 个日志故障解决方案进行验证和评估，结果表明，经过知识增强微调和大模型能提供出色的解决方案，表现在以下方面：

可靠性：大模型生成的解决方案可靠性高，成功解决率达到 95.5%。

效率：大模型自动生成解决方案，大量节省了运维人员的时间，显著提高了故障处理的效率。

可解释性：大模型从专家知识库中提取了多种解决方案，并能识别可靠性高的解决方案，这在实际操作中得到了验证，

第一方案在绝大多数情况下能够解决问题。

3 结束语

通用 LLM 大模型在运维领域快速应用落地采用“业务域微调+知识检索增强”范式。在通用预训练 LLM 大模型基础上进行业务域微调，可选用 LoRA 高效微调方法，拟合业务问答数据特征，建立面向垂直领域的理解和生成能力。知识检索增强能弥补大模型专业领域知识的不足，消除大模型的“幻觉”现象，对垂直领域的可控生成是至关重要的。

本文将离线业务域微调与线上大模型服务中的知识检索增强结合在一起，做对应的知识检索增强微调，训练运维指令跟随、运维专业知识融入理解和可行方案生成能力，能够提升线上知识检索增强的效果。

由日志出发，大模型自动关联查询分析专业知识和专家经验、自动生成解决方案，为智能运维开辟了一条新思路，为端到端故障自愈奠定了基础。

参考文献

- 1 MA M, YIN Z, ZHANG S, et al. Diagnosing root causes of intermittent slow queries in cloud databases [J]. In Proceedings of the VLDB Endowment, 2020, 13 (8): 1176-1189.
- 2 HE S, ZHANG X, HE P, et al. An empirical study of log analysis at microsoft [C] //In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2022: 1465-1476.
- 3 GANATRA V, PARAYIL A, GHOSH S, et al. Detection is better than cure: A cloud incidents perspective [C] //In Proceedings of the 31st ACM Joint European Software Engineering Confer-

- ence and Symposium on the Foundations of Software Engineering. 2023: 1891-1902.
- 4 CHEN J, ZHANG S, HE X, et al. How incidental are the incidents? characterizing and prioritizing incidents for large - scale online service systems [C] //In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering. 2020: 373-384.
 - 5 WEI J, TAY Y, BOMMASANI R, et al. Emergent Abilities of Large Language Models [J]. Transactions on Machine Learning Research, 2022.
 - 6 AHMED T, GHOSH S, BANSAL C, et al. Recommending root - cause and mitigation steps for cloud incidents using large language models [C] //In Proceedings of the 45th International Conference on Software Engineering. 2023: 1737-1749.
 - 7 SHETTY M, BANSAL C, UPADHYAYULA S P, et al. Autotsq: learning and synthesis for incident troubleshooting [C] //In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2022: 1477-1488.
 - 8 JIN P, ZHANG S, MA M, et al. Assess and summarize: Improve outage understanding with large language models [C] //In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2023: 1657-1668.
 - 9 王婷, 王娜, 崔运鹏, 等. 基于人工智能大模型技术的果蔬农技知识智能问答系统 [J]. 智慧农业 (中英文), 2023, 5 (4): 105-116.
 - 10 田永林, 王兴霞, 王雨桐, 等. RAG-PHI: 检索增强生成驱动的平行人与平行智能 [J]. 智能科学与技术学报, 2024, 6 (1): 41-51.
 - 11 GUU K, LEE K, TUNG Z, et al. REALM: retrieval - augmented language model pre - training [C] //In Proceedings of the 37th International Conference on Machine Learning. 2020: 3929-3938.
 - 12 GAO Y, XIONG Y, GAO X, et al. Retrieval - augmented generation for large language models: a survey [EB/OL]. (2024-03-27) [2024-06-05]. <https://arxiv.org/abs/2312.10997>.
 - 13 ChatGLM3 [EB/OL]. [2024-06-05]. <https://github.com/THUDM/ChatGLM3>.
 - 14 AGHAJANYAN A, ZETTLEMOYER L, GUPTA S, et al. Intrinsic dimensionality explains the effectiveness of language model fine-tuning [C] // In Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing. 2021: 7319-7328.
 - 15 HU E J, SHEN Y, WALLIS P, et al. LoRA: low - rank adaptation of large language models [C] //In Proceedings of the 10th International Conference on Learning Representations. 2022.
 - 16 LIU Y, PEI C, XU L, et al. opsEval: a comprehensive task-oriented aiops benchmark for large language models [EB/OL]. (2024 - 02 - 16) [2024 - 06 - 05]. <https://arxiv.org/abs/2310.07637>.

基于大模型检索增强的情报智能认知技术研究

栾真¹ 王又辰^{1*} 李楠² 刘宝琪³ 冯帆¹

摘要 文章面向情报分析领域中的军事要报生成、处置方案推荐等任务,开展基于大模型检索增强技术的研究,构建包括融合历史案例、处置规定等内容的知识库,通过多模态数据统一表征技术、跨模态索引库的提示增强技术,提升外部知识库在大模型检索中的效能,解决领域内的模型幻觉问题,并探索该技术在作战场景下的应用模式,提升情报处理及决策效率,有效支撑作战场景下的关键情报上报及处置应对。

关键词 情报分析,大模型,检索增强生成,知识库,方案生成,方案推荐

Intelligence Cognitive Analysis Technology based on Retrieval-Augmented Generation

LUAN Zhen¹ WANG You-Chen^{1*} LI Nan² LIU Bao-Qi³ FENG Fan¹

Abstract This research mainly focus on military information analysis such as report generation and plan recommendation scenarios. In this article, we have developed a large language model based information retrieval paradigm, which include a knowledge base about historical events and regulations. By using multimodal data unified representation and cross-modal indexing, the method is able to strengthen the external knowledge availability factor. The information retrieval paradigm is optimized to improve the efficiency of intelligence processing and decision-making, supporting intelligence management, analysis and response in real world scenarios.

Key words intelligence analysis, large language model, retrieval augmented generation, knowledge base, solution generation, solution recommendation

0 引言

当前,大模型在情报领域的应用方兴未艾,而其在军事场景应用落地过程中,仍存在领域数据不足、模型可解释性低等

诸多挑战,为了提高大模型技术在领域中的应用效能,本文基于大模型技术开展面向军事场景的异构情报关联融合、多模态知识库构建、检索增强方案生成等一系列模型方法,提出“作战情报感知—军事要报生成—处置方案推荐”的作战场景下情

* 通讯作者

1. 北京计算机技术及应用研究所 2. 中国人民解放军 639369 部队 3. 军事科学院军事科学信息研究中心

1. Beijing Institute of Computer Technology & Application 2. Unit 639369 of the PLA 3. Military Science Information Research Center, Academy of Military Science

报认知及分析模式构想,突破当前情报大模型在作战场景下应用面临的重点难题,提升情报处置决策效率,实现关键情报需求的快速响应和处置应对。

1 问题的提出

1.1 领域案例及处置规则数据缺乏

大模型在情报领域的应用中,领域案例的缺乏使得其在自我改进和学习时缺乏有效的反馈机制,造成准确率降低、泛化能力不足等问题,在面对新场景时由于缺乏相关背景知识及具体操作指南,难以提供准确的信息。维护包含案例信息、处置规定等内容的知识库可以帮助模型在特定任务中不断优化其处理策略,尤其在面对复杂问题时,体系化的案例知识及处置规则中可能隐藏着多种场景的关键要素及解决方案,辅助模型生成相应场景下更符合答案,优化大模型在情报领域的表现。

1.2 情报大模型的可解释性问题

大模型虽然在生成的性能上表现优异,但其决策过程往往是暗箱操作,难以被用户理解和解释,而在军事应用中,决策透明度和可解释性是至关重要的,在军事情报分析和战场指挥等高风险场景中,指挥员和操作人员需要对智能系统的建议有充分的理解,故亟须探索检索增强等技术辅助大模型定位信息来源,增强决策的透明度和可解释性。

2 基于作战场景的大模型架构设计

报大模型^[1] (MultiModel Large Language Model, MLLM) 的假设下进行,针对情报分析中的军事要报生成及处置方案推荐任务,构建融合历史案例、处置规定、专家知识等内容的知识库,研究基于知识库的跨模态检索增强技术,并探索其在作战场景下的应用模式。具体技术架构如图 1 所示。

在作战场景下的军事要报生成及处置方案推荐任务一般需涉及情报感知、作战业务、知识服务三个类别的信息系统之间的实时交互,其中情报感知类系统进行多模态情报数据的采集与处理;作战业务类系统需进行对于情报数据的分析、上报、处置等业务处理;知识服务类系统则为其他业务系统提供知识支撑;除此之外,各系统均需依赖通用的多模态情报大模型。

首先对于知识服务类系统,需动态构建面向作战场景的知识库^[2],包括事件库及规则库,丰富情报数据集并提供实时更新能力,作为外部的知识库支撑动态检索相关信息;其次研究基于知识库的跨模态大模型检索增强生成技术^[3],借助事件库中的最佳匹配得到事件单元上下文信息及对应处置规则,进行大模型的提示词设计,辅助大模型生成更高质量的情报上报报告和处置分析结果,降低大模型生成任务存在的幻觉问题,并定位信息来源增强决策的可解释性;最后开展基于大模型检索增强的情报分析技术研究,利用情报大模型的处理支撑能力,打通情报感知类、作战业务类及知识服务类系统对于情报大模型的调用链路,减轻各类系统之间信息交互的壁垒^[4],构建“作战情报感知—军事要报生成—处置方案推荐”的情报智能协同处置能力,为情报认知与处理提供更高的效能。

本文的研究在已建设通用的多模态情

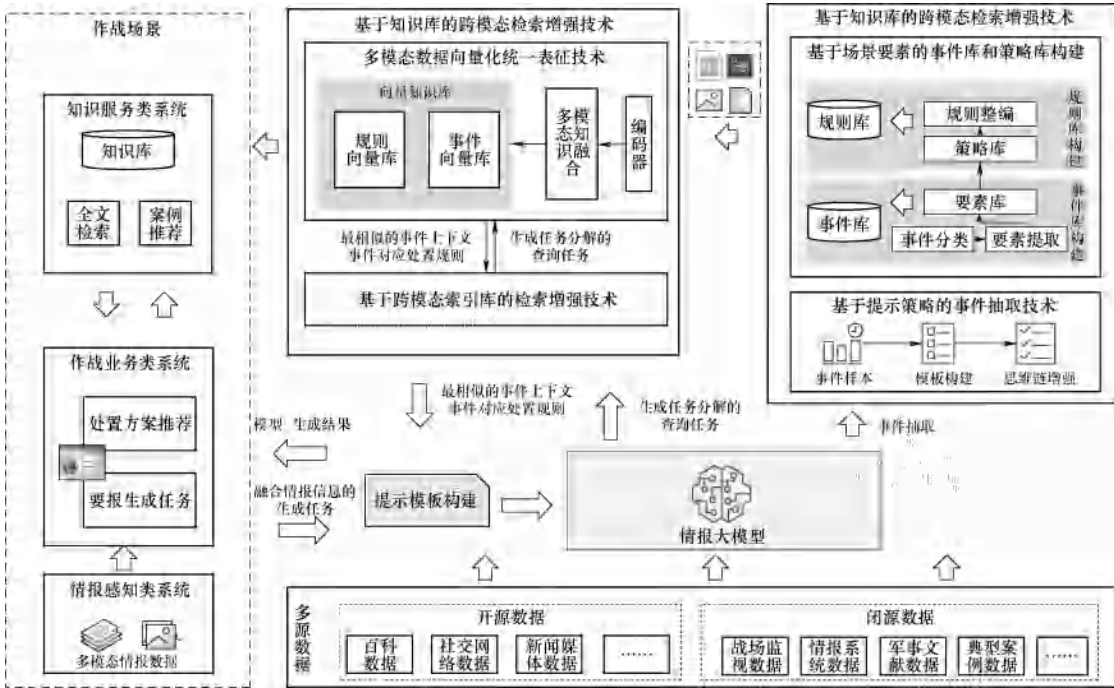


图1 基于检索增强大模型的多系统联动模式技术设计

3 关键技术

3.1 面向作战场景的知识库构建

军事要报生成及处置方案的推荐是面向作战场景的一个重要研究方向,而处置方案的制订需要有丰富的情况处置案例做支撑。本文首先对情报大模型进行提示策略设计以实现从海量多源数据中的初步事件检测及抽取,其次通过对事件知识的处理、提取、分类等操作构建事件库,并借助专家知识采用“抽取+审核”的方式构建用于辅助形成事件处置方案的规则库,事件库和规则库共同构成支撑整体的外部知识库,用以辅助最终的场景应用。

3.1.1 基于提示策略的事件抽取技术

应用通用的多模态情报大模型实现对于海量多源数据的事件抽取任务,需要设

计适合的提示策略。本文采用上下文学习方法来构建提示策略,首先根据业务规则及专家知识构建少量的面向作战场景的事件样本,包括任务描述和示范的任务样例拼接起来作为提示增强的一部分,在任务样例的构建过程中,通过添加思维链^[5]提示来增强大模型的推理能力,采用自动的思维链方法将推理逻辑加入描述当中形成样例集^[6],然后引导情报大模型在新的信息抽取要求下生成预测结果,该方法根据输入的面向作战场景的少量提示,就能解决对应场景下的新问题。

具体处理方式如下,情报大模型生成的输出可以用以下公式来表示:

$$MLLM(I, D_k, f(x_{k+1}, _)) \rightarrow \hat{y}_{k+1} \quad (1)$$

$$D_k = \{f(x_1, y_1), \dots, f(x_k, y_k)\}$$

式中, I 为给定某个特定抽取任务的描述; $D_k = \{f(x_1, y_1), \dots, f(x_k, y_k)\}$ 作为由 k 个样例组成的一组示范; $f(x_k, y_k)$ 为将

任务样例转换为提示内容的函数； x_{k+1} 为新的查询输入； \hat{y}_{k+1} 为大模型的预测结果。

在形成样例集后，将其整合为对情报大模型的提示，按照预定义的模板将样例的输入输出对进行实例化，最后对测试问题进行上下文学习，得到最终的抽取结果。

3.1.2 基于场景要素的事件库和策略库构建

本文通过模型的推理及生成能力实现

对事件要报及处置方案的生成及推荐，需首先构建覆盖历史案例经验的知识库作为模型的外部支撑，主要知识类别可分为事件内容本身及处置规则知识两类，故构建事件库和规则库以实现对于知识源的维护，其中事件库汇总海量历史数据中形成的事件案例知识，规则库则是对各类事件进行要素拆分后，将对应处置策略进行梳理形成的规则集^[7]。具体架构如图 2 所示。

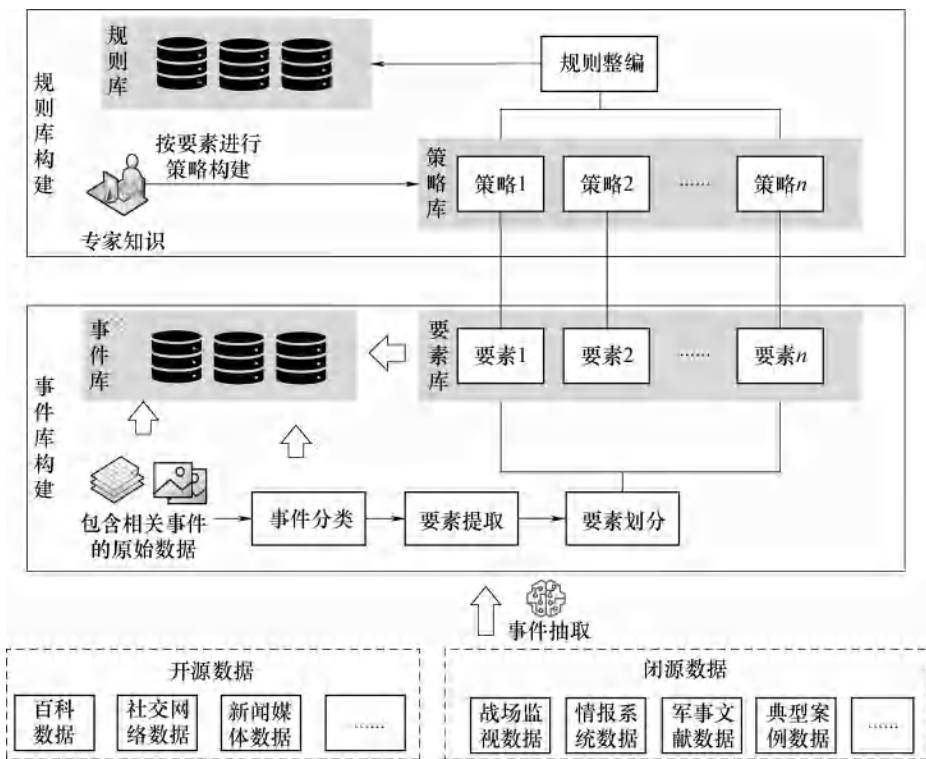


图 2 基于场景要素的事件库和策略库构建技术

在这一架构下，首先，借助情报大模型的事件抽取能力从海量多源数据中识别包含事件的数据，并将原始数据汇入事件库。其次，考虑到事件的处置往往包含较多的影响要素，难以直接找到相似事件并参考其处置规则进行处理，故本文按照关注的业务角度进行事件分类及要素提取，

并融合专家知识进行要素划分构建要素库，将包含事件的数据按要素库的分类切分为更小的单元，以按单元进行处置策略单元的梳理，并按照一定的整编方案进行处置规则的整编形成规则库^[8]。最后，当新的事件出现，将该事件进行要素提取后与要素库中的最小单元进行匹配，

再对匹配排名较高的规则单元进行筛选及组合,可更好地对新事件提出有针对性的处置方案,同时将处置规则汇入规则库,对知识库形成不断的增量维护。

3.2 基于知识库的大模型检索增强技术

为了避免出现由于大型模型生成能力不足以及情报领域知识覆盖不全所导致的生成结果错误问题,本文通过结合已有的情报领域知识,采用检索的方法来生成指令所对应的回答,充分利用领域内的专业知识,检索与用户输入相关的文本、图像等知识来辅助大模型进行最终答案的生成,这一过程有效地利用了大模型在通用领域上的指令和语义理解能力。知识库可以作为模型的补充,使得模型在面对特定领域的问题时能够获得更准确、全面的答案,从而为大语言模型的应用提供一种灵活、高效的解决方案,克服当前通用大模型在情报领域应用时存在的结果生成不符合领域认知的问题。

3.2.1 多模态数据向量化统一表征技术

本文构建的知识库包括结构化数据、文本数据、图片、视频等多模态数据类型,无法直接被情报大模型调用。多模态数据向量化统一表征技术研究针对不同类型数据进行统一向量化表征并构建索引,利用自然语言处理技术、计算机视觉技术对文本、图像等多模态情报数据进行向量化表示,以有效的方式组织和存储跨模态数据,建立对应的索引结构,构建形成知识向量库^[9]。在索引过程中,数据被解析、转换和组织,以便进行高效的检索,索引充当数据的结构化表示,使得在运行时能够进行更快速的检索操作,如图3所示。

1. 多模态知识表示

采用自然语言处理技术及计算机视觉

技术对多模态知识进行分别处理,编码映射入向量空间,结构化数据有着高度组织化和字段明确的特性,可采用独热编码或利用关系网络进行关系表示学习转化为向量形式,文本数据可采用词嵌入模型、上下文感知模型等方法进行编码;图像数据可利用卷积神经网络提取图像的层次化视觉特征进行数据编码^[10];视频编码则利用3D卷积神经网络处理视频的空间和时间维度,并通过长短期记忆网络来捕捉时间序列信息等方式映射入向量空间^[11]。

2. 多模态知识融合

在获得初步编码的多模态知识后,通过模态融合技术使这些知识合成为统一形式,本文采用基于注意力机制的多模态数据融合方法,运用复杂的算法和模型架构,深入探索和利用不同模态间的相互关系及其动态交互,并且在处理一个模态的数据时专注于另一个模态中的关键部分,通过动态调整不同模态间的注意力权重^[12-13],实现不同模态信息的高效融合,增强信息的全面性,消除知识歧义,提升模型预测的准确性和鲁棒性。

3. 多模态向量库设计

向量知识库需自身具备从异质数据源中快速定位和抽取有质量的情报信息的能力,本文采用一种高效的多模态向量索引技术,对数据进行适当的预处理以确保其质量和一致性,通过 k 均值聚类算法来对编码后的多模态嵌入向量进行有效的空间划分,通过倒排索引技术将查询向量与聚类后的各质心向量进行匹配,定位目标簇族以缩小数据搜索范围。对于已经缩小的搜索空间,进一步应用最大内积搜索技术,以最终实现在庞大的数据集上进行快速且准确的近似最近邻搜索。

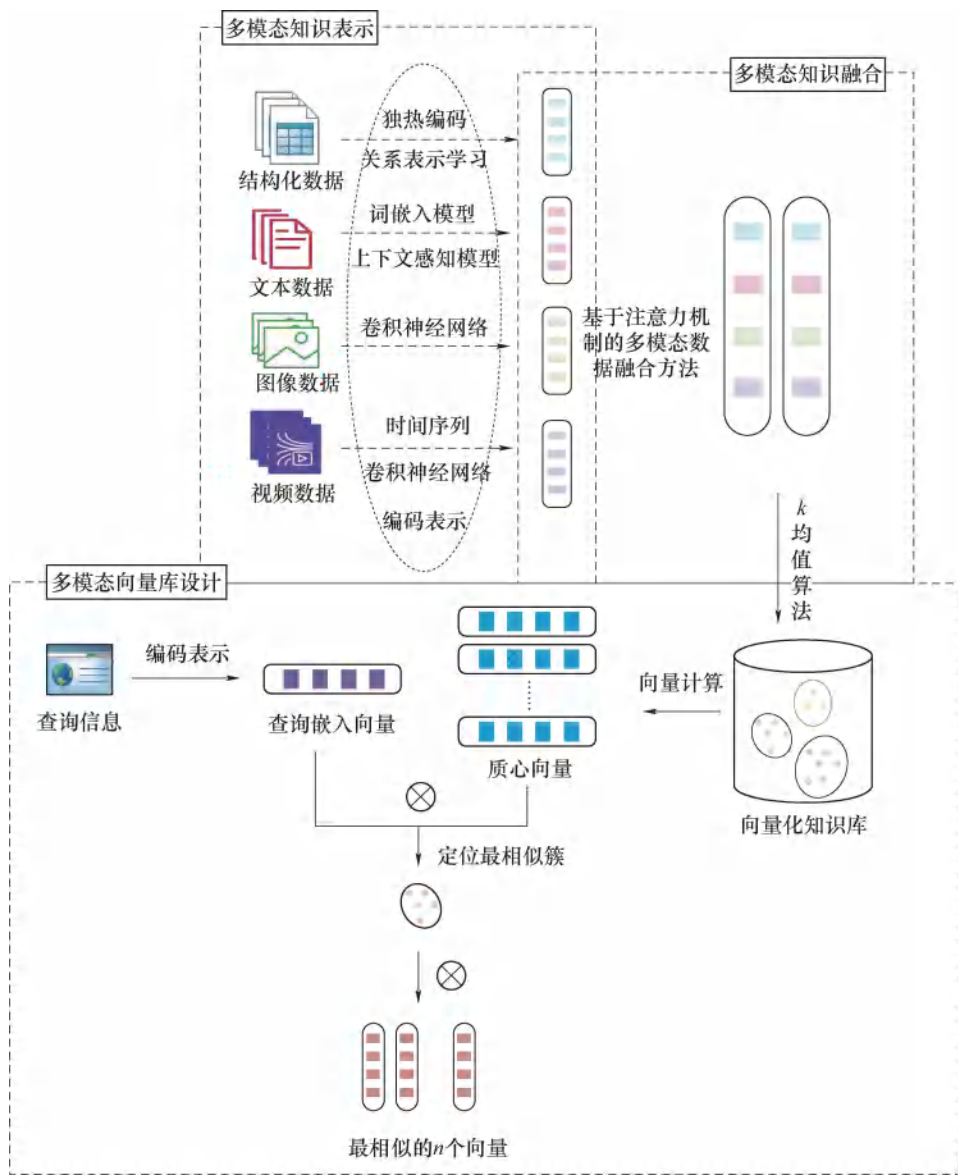


图3 多模态数据向量化统一表征技术

3.2.2 基于跨模态索引库的检索增强技术

基于跨模态索引库的检索增强技术旨在通过用户意图与知识向量库之间的语义匹配，在海量知识向量库中快速精准地匹配到与用户提问相关的文本、图像等信息，并根据上文对于知识库的设计将相关处置规则数据统一检索出来，生成阶段将

这些数据按照一定的规则生成提示模板，并传递给情报大模型进行进一步的处理和生成，根据检索到的数据和用户查询内容对于情报大模型的生成内容进行增强，如图4所示。

本文将一个检索模型和生成模型结合在一起执行相应任务^[14]，该方法依赖内部

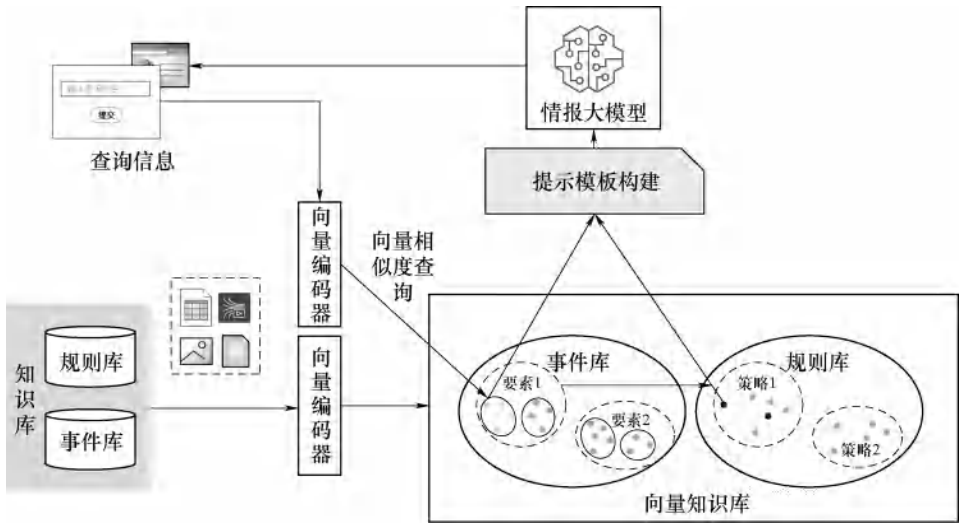


图4 基于跨模态索引库的提示增强技术

知识高效的修改方式，不需要对整个模型进行重新训练，故非常适合军事场景的应用。检索增强生成方法的关键：一是在于检索阶段依赖的知识库的质量，此处已经在前文中构建相应的知识库；二是在生成阶段要着重考虑提示模板的设计，提示模板是生成语言模型提示的预定义方式，从最终用户那里接收一组参数并生成提示，在构建模板时需要充分与作战场景结合，识别在作战任务中起关键作用的信息块，包括问题的关键词、关注点、上下文等。

当给定一个生成任务时，该方法生成一个查询问题，检索模型将经过编码后的查询问题与已构建的事件库中的事件单元进行对比，找到相似性最高的 k 个事件单元，将对应的规则库中的策略单元进行组合后形成规则知识，将问题、事件单元的上下文数据、对应的规则知识经过提示模板格式化后一起传递给情报大模型，降低大模型幻觉^[15]，最终增强答案生成。

检索增强生成同时利用生成式模型和检索式模型，使得模型能够融合两者的优势。通过检索外部知识库，检索增强生成

模型能够获取更丰富的信息，从而生成更准确、更丰富的文本。有助于解决生成式模型在缺乏背景知识时可能出现的模糊或错误的问题。检索到的结构化知识提供了生成文本的背后逻辑和依据，增强了模型的解释性。用户能够更好地理解生成结果的来源和合理性。此外，通过更换不同的知识库或更新外部知识，检索生成模型能够灵活适应任务的变化。这使得模型能够及时反映实际环境和任务需求的变动。模型更加全面、灵活地处理自然语言生成任务，提高了生成文本的质量和适用性。

4 基于大模型检索增强的情报分析模式探索

本文主要面对战场突发事件的要报生成及处置应对的场景，研究作战场景下基于大模型检索增强的情报分析模式，在这里考虑情报感知类、作战业务类、知识服务类三类信息系统，构建“作战情报感知—军事要报生成—处置方案推荐”的智能协同处置方案。各系统交互的流程如图5所示。

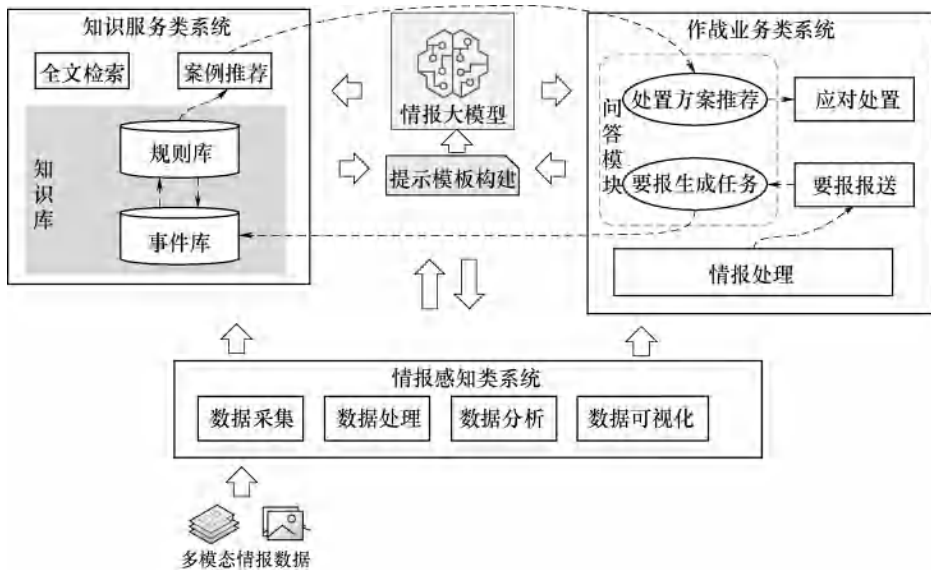


图5 基于大模型检索增强的情报分析架构

情报大模型作为智能处理能力的基础底座，为各系统提供文本抽取、图像抽取、视频提取、事件检测、文本生成等智能处理支撑。

情报感知类系统提供数据的采集和处理能力，接收到情报信息，对多模态的情报数据进行处理、分析，并将处理后的数据提供给作战业务类系统和知识服务类系统。

知识服务类系统提供知识的管理与检索推荐能力，汇聚了从情报感知类系统收集的情报数据，以及专家知识、文献数据等，借助情报大模型的智能处理能力，构建包括事件库及规则库等的知识库，一方面可作为情报大模型的外部知识源提供检索增强能力，另一方面可为作战业务类信息系统提供全文检索及案例推荐功能，增强系统决策的透明度。

作战业务类信息系统是面向作战指挥人员的主要业务处理的窗口，在本文设计的情报认知及分析模式中，由作战业务类系统作为任务发起方，采用问答式的交

互，将收到的情报信息转化为要报生成任务，向情报大模型提出生成请求，情报大模型调取知识服务类系统内置的知识库进行检索查询，匹配到相似事件案例及其对应的处置规则，将检索到的知识信息与原始查询任务一起构建提示模板送入情报大模型，最终由情报大模型返回生成的要报信息，同时将模型在知识服务系统中匹配到的相似案例及处置方案回传给作战业务系统，作为情报大模型生成内容的依据，增强系统可信性。

5 结束语

本文设计了一种基于大模型检索增强的情报智能认知模式，首先动态构建面向作战场景的知识库，包括事件库及规则库，丰富情报数据集并提供实时更新能力；其次研究基于知识库的跨模态大模型检索增强生成技术，借助事件库中的最佳匹配得到事件单元上下文信息及对应处置规则，辅助大模型生成更高质量的情报报

告和分析结果；最后研究了一种基于大模型检索增强的新一代情报分析模式，构建“作战情报感知—军事要报生成—处置方案推荐”的智能协同处置方案，为情报处理及分析提供了更高的效能。

参考文献

- 1 FEIH, YAO Y, ZHANG Z. From Multimodal LLM to Human-level AI: Modality, Instruction, Reasoning, Efficiency and Beyond [C] //In Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024): Tutorial Summaries.
- 2 唐明伟, 苏新宁, 王昊. 突发事件应急响应情报体系案例解析: 以公共安全事件为例 [J]. 情报科学, 2019, 37 (1): 105 - 111. DOI: 10. 13833/j. issn. 1007-7634. 2019. 01. 017.
- 3 LEWIS P, PEREZ E, PIKTUS A, et al. Retrieval-augmented generation for knowledge-intensive nlp tasks [J]. Advances in Neural Information Processing Systems. 2020, 33: 9459 - 9474.
- 4 胡德强, 李先能. ZZ 指挥决策情报分析大模型 [C] //国防科技大学系统工程学院. 第五届体系工程学术会议论文集——数智时代的体系工程. 大连理工大学经济管理学院. 2023: 2. DOI: 10. 26914/c. cnkihy. 2023: 056270.
- 5 WEI J, WANG X Z, DALE S, et al. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models [C] //Advances in Neural Information Processing Systems (Volume 35). 2022: 24824-24837.
- 6 NAI Z, NIANMIN Y, JIAN Z, et al. Rule-based adversarial sample generation for text classification [J]. Neural Computing and Applications, 2022, 34 (13): 10575-10586.
- 7 唐明伟, 苏新宁, 姚兴山. 本体驱动的突发事件案例知识库 [J]. 情报理论与实践, 2016, 39 (9): 123-127. DOI: 10. 16353 //j. cnki. 1000-7490. 2016. 09. 022.
- 8 唐明伟, 苏新宁, 肖连杰. 面向大数据的情报分析框架 [J]. 情报学报, 2018, 37 (5): 467-476.
- 9 蹇松雷. 基于复杂异构数据的表征学习研究 [D]. 长沙: 国防科技大学, 2019. DOI: 10. 27052/d. cnki. gzjgu. 2019. 000004.
- 10 杜鹏飞, 李小勇, 高雅丽. 多模态视觉语言表征学习研究综述 [J]. 软件学报, 2021, 32 (2): 327-348. DOI: 10. 13328 /j. cnki. jos. 006125.
- 11 张德, 王子玮, 张峰. 基于语义空间统一表征的视频多模态内容分析技术 [J]. 电视技术, 2017, 41 (Z2): 131-133. DOI: 10. 16280/j. videoe. 2017. h7. 027.
- 12 曹申健. 基于多模态信息融合的目标识别研究与实现 [D]. 成都: 电子科技大学, 2022. DOI: 10. 27005/d. cnki. gdzku. 2022. 002 446.
- 13 张炳力, 潘泽昊, 姜俊昭, 等. 基于交叉注意力机制的多模态感知融合方法 [J]. 中国公路学报, 2024, 37 (3): 181 - 193. DOI: 10. 19721/j. cnki. 1001-7372. 2024. 03. 009.
- 14 SETH E. What executives need to know about knowledge management, large language models and generative AI [J]. Applied Marketing Analytics, 2023, 9 (3): 215-229.
- 15 LI H, SU Y, CAI D, et al. A survey on retrieval-augmented text generation [J]. arXiv preprint arXiv: 2202. 011 10. 2022.

基于大语言模型的复杂问题分解流程 自动生成方法

李敏¹ 牛婵¹ 闫林¹ 樊志强¹ 夏晓凯¹

摘要 该方法旨在利用大语言模型将复杂的体系设计相关业务问题自动分解细化为具体的子问题和处理步骤文本，之后抽取文本中的实体要素及衔接关系，最终形成业务流程图模型。文章提出了一种基于大语言模型的复杂问题分解流程自动生成方法，采用基于三级文本摘要的资源数据存储、基于问题规则要素的问答交互、基于大模型集合的实体关系抽取与结果评估等思路进行方法实现。最后，结合具体案例进行了实验，结果显示利用该方法能够有效实现复杂问题的分解流程自动生成。

关键词 复杂问题分解，流程自动生成，大语言模型

Automatic Generation of Complex Problem Decomposition Flow Based on Large Language Model

LI Min¹ NIU Chan¹ YAN Lin¹ FAN Zhi-Qiang¹ XIA Xiao-Kai¹

Abstract This method aims to use the large language model to automatically decompose the complex system design-related business problems into specific sub-problems and processing step text, and then extract the entity elements and cohesive relations in the text, and finally form the business flow diagram model. In this paper, an automatic generation method of complex problem decomposition process based on large language model is proposed. Resource data storage based on three-level text summary, question and answer interaction based on question rule elements, entity relationship extraction and result evaluation based on large model set are adopted to implement the method. Finally, experiments are carried out with a concrete case, and the results show that this method can effectively realize the automatic generation of decomposition flow for complex problems.

Key words complex problem decomposition, automatic process generation, large language model

0 引言

面向体系设计领域^[1]，复杂问题分解能够对体系设计过程中的难点、重点业务

问题提供答案参考和分解推荐，能够有效辅助专家的体系设计工作。问题复杂性促使人们考虑到应结合多种智能方法来支持问题的求解，因此出现了将各类算法、技术与基于符号知识的专家系统进行融合来

1. 中国电子科技集团公司信息科学研究院

1. Information Science Academy of China Electronics Technology Group Corporation

进行产品概念设计的方法。主要存在三个方面的问题：①以往的方法本质上都强调机器智能的融合，孤立了机器智能与人类智能的融合，没有考虑到如何直接结合人类智能与机器智能来进行复杂问题分解。②难以解决大量无法用数学模型表达的复杂问题。在人工智能还没有达到完美表达人类发散性思维的情况下，人在复杂问题分解中的地位始终是无法替代的。③利用深度学习方法理论上能够有效实现复杂问题分解，但对于体系设计领域缺少有效的高质量的训练数据，故此方法也只停留在理论和实验阶段。

1 复杂问题自动分解技术研究


1.1 问题定义

本文聚焦于复杂问题分解方法在体系

设计领域的应用，主要包括、业务流程、能力分解、系统组成设计等方面。致力于利用检索增强技术，结合大语言模型的文本生成能力和信息抽取能力辅助用户针对一个具体的体系设计需求，快速生成体系设计业务问题的分解思路，最后提取节点实体及实体关系要素，并利用图形控件显示出来预期效果，如表 1 所示。

利用大语言模型进行复杂问题分解流程自动生成时面临以下问题和挑战：①通用大语言模型缺少体系设计相关领域的业务数据训练环节，故生成的文本对于领域专家来说不够专业，此外，无法实时融合新的知识信息。②用户输入的复杂问题不够具体、要素不够齐全，影响大模型对问题的理解。③大语言模型虽然能够生成文本，但当需要精确的 JSON（Java Script Object Notation）输出格式时，它们并不总是按照指示执行。

表 1 预期效果

复杂问题输入	期望输出
体系设计需求： 怎样进行情报保障工作 工作流程的设计。 相关知识信息： 《美军联合战役情报保障问题研究》 《基于综合集成研讨厅的公共安全风险感知平台构建》 ……	复杂问题分解结果-文本示例： 联合战役情报保障工作包括情报的计划与指导、搜集、处理与利用、分析与整理、分发与整合、评估与反馈六个流程，情报计划与指导行动具体包括……搜集具体包括…… 复杂问题分解结果-流程节点实体及关系示例： <pre>[{"name": "计划与指导", "nodes": [{"type": "task", "executor": "指挥官", "name": "确立关键情报需求", "next": [{"name": "分配联合情报体系和力量"}]}, {"type": "task", "name": "分配联合情报体系和力量", "next": [{"name": "制订搜集和支援计划"}]}, {"type": "task", "name": "制订搜集和支援计划", "next": [{"name": "向高层提出申请"}]}, {"type": "task", "name": "向高层提出申请", "nodes": [{"name": "增加情报支援"}]}, {"name": "搜集", "nodes": [{"type": "task", "name": "建立搜集需求", "next": [{"name": "配置搜集力量"}]}, {"type": "task", "name": "配置搜集力量", "next": [{"name": "请求支援"}]}, {"type": "task", "name": "请求支援", "next": [{"name": "搜集信息"}]}, {"type": "task", "name": "搜集信息", "next": [{"name": "初步处理"}]}]}</pre>
	复杂问题分解结果-流程图显示 

针对上述问题,提出了基于大语言模型的复杂问题分解流程自动生成方法,该技术在知识库各类数据的支撑下,利用大语言模型的文本生成能力、思维链机制、人类语言对齐能力、实体关系抽取能力,结合图形化控件,支持用户面向体系设计工作中,以问答交互模式构建人机交互场景,实现机器智能与人类智慧的有效融合,并将复杂问题分解结果的文本转为对应的系统架构、业务流程、信息活动、能力分解、系统组成,具体包括步骤包括:①基于三级文本摘要的资源数据存储。②基于问题规则要素的问答交互。③基于大语言模型集合的实体关系抽取和结果评估。

通过上述步骤,可以实现体系设计领域的复杂问题分解,复杂问题分解技术能够为回答复杂问题提供证据支持,降低体系设计作业的专业门槛,为体系设计提供直观的知识信息支撑,增强人机交互的流畅性和友好性。

1.2 相关内容研究现状

复杂问题分解技术主要包括基于传统机器学习的问题分解和基于深度学习的问题分解。前者主要包括基于规则模板的方法和基于分割的方法,后者主要包括基于Transformer的方法、基于图神经网络的方法、基于注意力机制的方法、基于查询图的方法、基于强化学习的方法。

基于传统机器学习的问题分解的研究,借助特征工程的方法,提取问句的代表性特征,包括句子的词法特征、语义特征。根据这些特征借助规则或模板等生成相应的简单子问题,通过单跳问答系统得到子问题的答案,再经过组合与评分得到原问题的答案。Hartrumpf^[2]提出了分解规则:针对问句中时间分解、针对主题实体中地名分解、针对问题条件中地名分解、

针对并列情景分解等,提出基于问题语义表示的分解。采用所定义的分解规则为问题生成具有足够语义表示的解析器。王振宇等^[3]提出了一种基于句法模板的复杂问题分解方法,通过对复杂问题进行问题实体抽取、模板匹配和问题依赖图生成等处理,实现对复杂问题的分解。

基于深度学习的问题分解的研究,基于神经网络的深度学习采用端到端方法,模型训练过程不进行模块划分,统一优化任务目标,并且自动化地提取特征,不需要人为干预。基于深度学习的方法主要解决两个问题:子问题生成、子问题组合排序。Zhang等^[4]提出一个基于Transformer框架的问题分解方法,能够将输入的复杂问题直接生成与人类语言对齐的子问题,且无词序和内容限制。问题分解方法由Transformer编码器和迭代的解码器组成,直接生成子问题文本表达。提出了一种层次语义识别模型,基于分解-集成的思想,进行解析架构设计。Khot等^[5]提出一个Text modular networks架构,基于该架构设计了ModularQA系统,系统由单跳事实型问答和问题逻辑计算等模块组成,能够通过子模型将复杂问题分解为子问题。

2 复杂问题分解流程自动生成方法

2.1 主要步骤

以技术方案、标准文件、领域知识等资源数据为依托,利用text2vec将资源数据转化为向量数据,之后对资源数据匹配检索技术实现用户所提复杂问题与资源数据的相关性匹配,提取相关知识数据,结合大语言模型的交互问答界面实现复杂问题的文本分解结果,接着利用大语言模型

集合进行实体关系抽取，将文本分解结果转为图的结构化表达，详见图 1。

(1) 基于三级文本摘要的资源数据存储。目前开源大模型对通用领域的问答效果较好，但对于体系设计专业领域，目前的开源大语言模型生成效果较不理想，通过对领域文本、知识、素材的处理，利用大模型对文档进行文档级、章节级、段落级的摘要提取，并利用向量模型进行文本向量化处理，使得专家知识能够赋能智能模型，辅助后续的问答交互功能。

(2) 基于大语言模型的问答交互。以问题分类、问题要素模板作为规则知识，融合上一步骤命中的文本信息，利用大语言模型的对话生成能力，采用思维链机制，通过多轮问答逐步辅助用户进行问题分解结果的推荐和回答、复杂问题分解、通用大语言模型对体系设计领域的业务适

配性。

(3) 基于大语言模型集合的实体关系抽取和结果评估。利用通用大语言模型的少样本学习能力，实现文本转为图；采用 ChatGLM3-6B、Qwen1.5-14B-chat，以及 Qwen1.5-72B-chat 三种大语言模型对生成进行打分评价，择优录取，提高实体关系抽取的成功率和正确率。

2.2 基于三级文本摘要的资源数据存储

用户在体系设计过程中，需要参考相关信息资源，体系结构设计主要关注等视图。当将大模型应用于实际业务场景时会发现，由于模型的训练数据未涵盖相关业务领域、大模型幻觉问题以及数据安全性考虑等问题，通用的基础大模型基本无法满足实际业务需求。

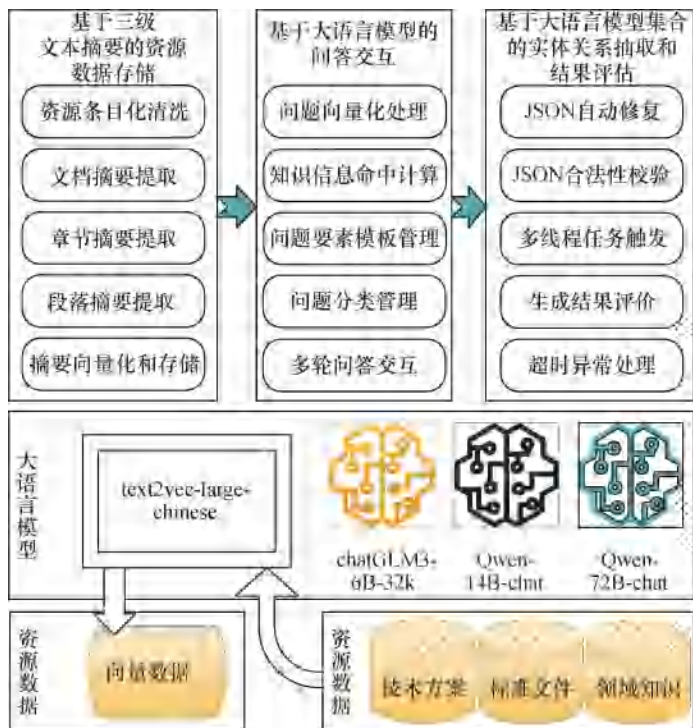


图 1 复杂问题分解流程自动生成步骤

检索增强生成 (Retrieval Augmented Generation, RAG), 该技术的利用能够在一定程度上有效解决以上问题。RAG 的一般应用流程: 把文本分割成块, 然后把这些分块嵌入向量与 transformer 编码器模型, 把所有这些向量建立索引, 最后创建一个 LLM (大语言模型) 提示语, 告诉模型回答用户的查询, 给出在搜索步骤中找到的上下文。在运行时, 用相同的编码器模型完成用户查询的向量化, 然后执行这个查询向量的索引搜索, 找到 top-k 的结果, 从数据库中检索到相应的文本块, 并提供给 LLM 提示语 Prompt 作为上下文。以上是进行基于知识的交互问答的一般流程, 但由于其匹配策略、文本分割策略较简单, 往往无法有效、全面地识别与问题相关的知识, 故本文采用基于文本摘要的三级资源数据匹配检索策略进行相关知识搜索。

在进行资源检索之前, 将知识信息存储在向量数据库中, 主要包括三类数据: 文档摘要信息、章节摘要信息以及条目 (摘要) 信息。文档摘要和章节摘要能够确保粗粒度信息不漏检, 条目 (摘要) 信息确保细粒度信息不漏检。信息资源通常具备章节大纲, 而体系结构要素可能蕴含在多级章节层次结构段落中, 需要转换为体系结构视图的文本语义层次关系天然包含在大纲层次结构中, 因此, 在将文本传递给大模型之前, 先将大纲层级进行解析并将层次关系体现到文本语义描述中。

具体流程用伪代码表示如下:

```
\begin{algorithm}[H]
\caption{文档条目化解析与摘要提取}
\begin{algorithmic}[1]
\Procedure{EntryParsing}{ $ document $ }
  \State $ entries \gets \emptysetset $
  \ForEach{ $ paragraph \in document $ }
```

```
  \If{ $ paragraph \text{ matches regex for
chapter number } $ }
    \State $ entry \gets \text{create entry
with paragraph and chap- ter number} $
    \State $ entries.add(entry) $
  \EndIf
\EndFor
\State \Return $ entries $
\EndProcedure

\Procedure {SummaryExtraction} { $ document, entries $ }
  \State $ summaryDocument \gets \text{extract
summary from the entire docu- ment using large language
model} $
  \State $ summaryVectorDocument \gets \text{
convert summary to vector using pre- trained model} $
  \ForEach{ $ entry \in entries $ }
    \State $ summaryChapter \gets \text{extract
summary from the chapter in entry using large language
model} $
    \State $ summaryVectorChapter \gets \text{
convert summary to vector using pre- trained model} $
    \State $ en- try.updateSummary (summaryChapter,
summaryVectorChapter) $
  \EndFor
  \State \Return $ entries $
\EndProcedure

\end{algorithmic}
\end{algorithm}
```

2.3 基于问题规则的大语言模型问答交互

提高复杂问题分解的效率和质量, 解决通用大语言模型对体系设计领域的业务适配性, 如图 2、图 3 所示。

首先用户输入复杂问题, 系统利用大模型和问题分类字典对复杂问题的分类进行识别, 之后根据问题分类结果进行问题要素规则匹配查询, 根据要素规则和提示

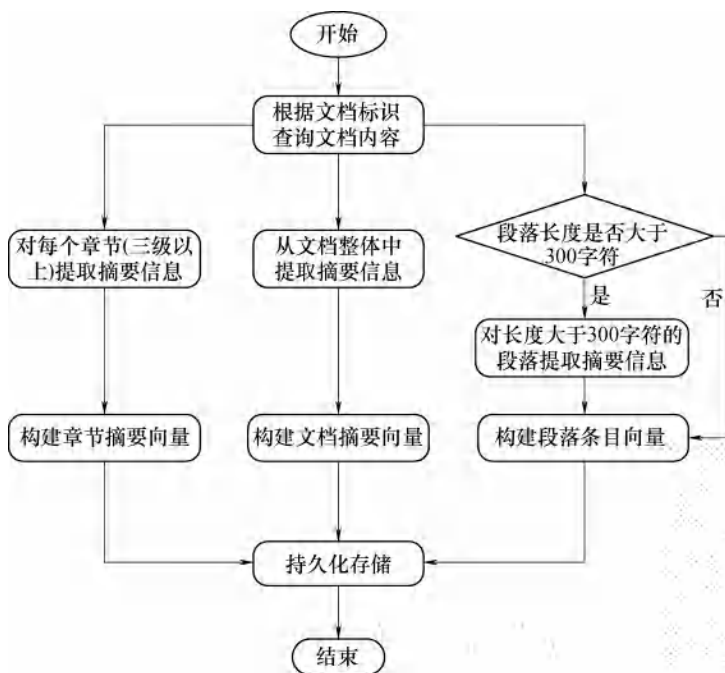


图2 基于三级文本摘要的资源数据存储

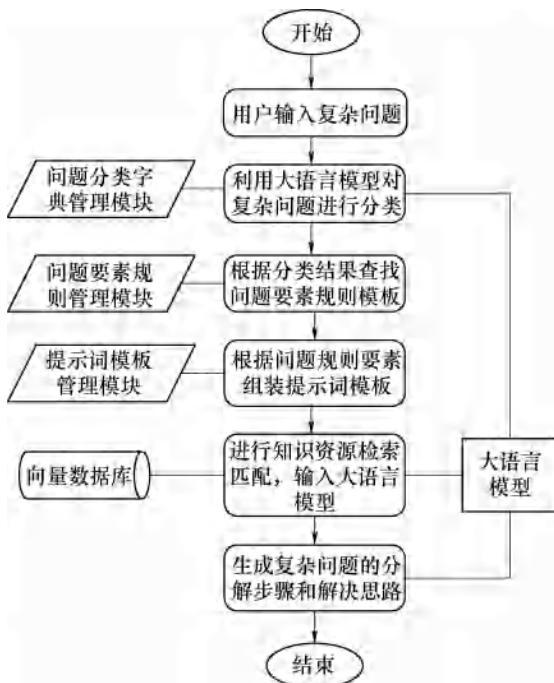


图3 基于问题规则的大语言模型问答交互

词模板组装提示词，结合上一步所命中的知识资源数据，进行相关知识检索，输入大语言模型后，大模型能够基于正确的知识，围绕问题要素进行复杂问题的解决思路的解答。

具体实现伪代码如下：

```
\begin{algorithm}[H]
\caption{复杂问题处理算法}
\begin{algorithmic}[1]
\Procedure{ComplexQuestionProcessing}{$question$}
\State 初始化问题分类字典 $question-ClassificationDict$
\State 初始化大模型 $largeModel$
\State 初始化资源数据存储 $resourceData$
```

```
\State 使用大模型和问题分类字典对问题进行分类识别：
```

```
\Statex \hspace{2em} $classificationResult \gets
largeModel.classify(question, questionClassificationDict) $
\State 根据问题分类结果进行要素规则匹配查询：
```

```
\For {每个分类结果 $class$ in $classificationResult$}
\Statex \hspace{2em} $ruleMatch \gets
ruleMatching(class, resourceData) $
\EndFor
```

\State 组装提示词模板：

```
\For {每个匹配到的规则 $rule$ in $rule-Match$}
\Statex \hspace{2em} $promptWordTemplate \gets
createPromptWordTemplate(rule) $
\EndFor
```

\State 结合资源数据进行相关知识检索：

```
\For {每个提示词模板 $template$ in $promptWordTemplate$}
\Statex \hspace{2em} $knowledgeRetrievalResult \gets
knowledgeRetrieval(template, resourceData) $
\EndFor
```

\State 输入大语言模型：

```
\For {每个知识检索结果 $result$ in $knowledgeRetrievalResult$}
\Statex \hspace{2em} $finalAnswer \gets largeModel.
generateAnswer(result) $
\EndFor
```

\State 返回最终答案：

```
\Statex \hspace{2em} return $finalAnswer$
\EndProcedure
\end{algorithmic}
\end{algorithm}
```

其中，知识命中方法采用的是余弦相似度，阈值取 0.6，经过实验发现，阈值的区间在 0.6~0.7，知识匹配的效果最好。

2.4 基于大语言模型集成和评估的实体关系抽取

该模块主要利用通用大语言模型信息抽取能力，将文本信息转换为结构化数据，如 JSON 对象，之后利用图形插件将 JSON 对象解析后显示在前端，从而实现复杂问题分解结果的结构化信息可视化。通用大语言模型在此特定的输入和输出业务需求场景中，由于在训练过程中该领域语料库匮乏，导致识别准确性并不高，为解决此问题，主要利用通用大语言模型的少样本学习能力，并利用多个大模型集成与评估技术提升该模块的可靠性和准确性。

(1) 结构化信息抽取。构建体系设计领域的文本信息抽取的小样本，并作为示例参数输入大模型调用的接口中，引导大模型按照样例的格式进行文本解析和信息抽取生成；此外，在提示词中，同时定义大模型的业务角色、任务输入和任务输出格式，如图 4 所示。

(2) 大语言模型集成和结果评估。如图 5 所示，利用 langchain 大模型，结合多线程机制，采用多模型并行作业方式，本

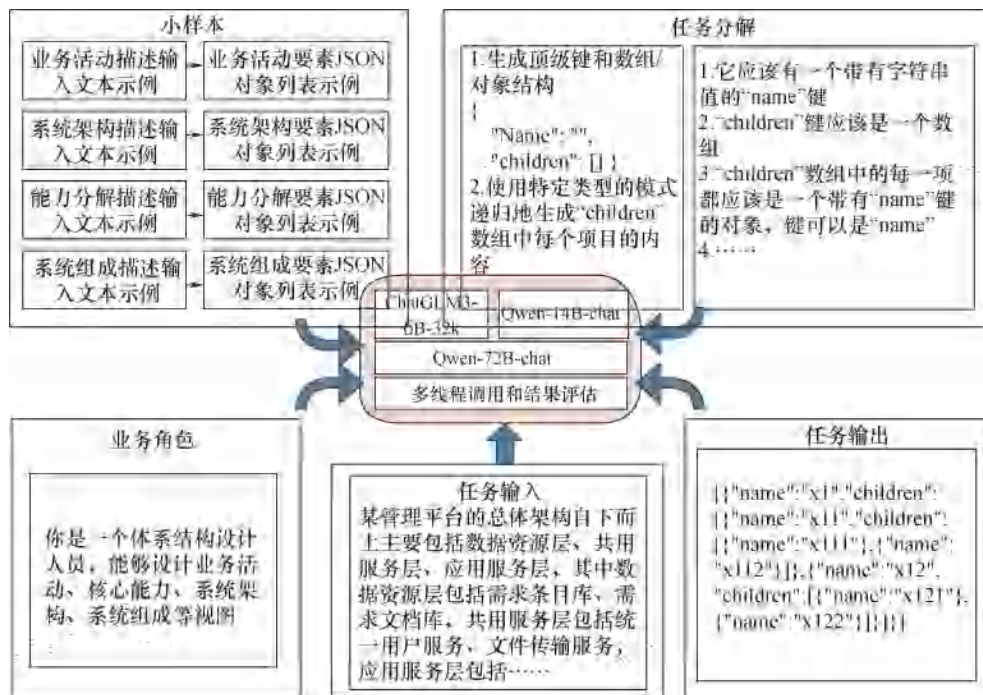


图 4 JSON 结构化信息抽取

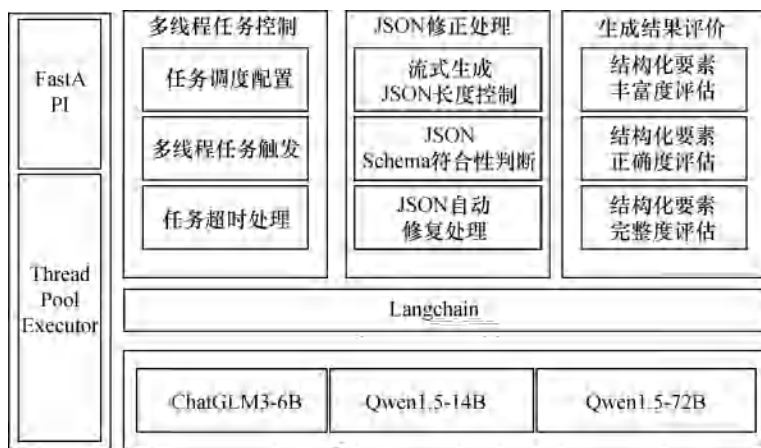


图 5 模型集成和结果评估

次试验主要采用了 ChatGLM3-6B、Qwen 1.5-14B-chat，以及 Qwen1.5-72B-chat 三种大语言模型辅助 JSON 结构化信息抽取的实现；之后利用 JSON 修正处理机制，对各个大模型抽取生成的结果进行打分评价，择优录取，提高实体关系抽取的成功率和正确率。

3 实验分析

3.1 实验设置

结合体系设计领域复杂问题，以联勤保障领域、网信体系等论文为素材，构

建复杂问题自动分解流程生成试验环境。实验环境主要包括模型及工具准备、知识资源文件、问题分类字典、问题规则要素。

(1) 本次实验采用 ChatGLM3-6B、Qwen1.5-14B-chat, 以及 Qwen1.5-72B-chat 进行复杂问题分解流程自动生成的试验研究, 服务器操作系统是 ubuntu21.42, 显卡配置是 A6000 的 8 卡。所需要的模型、工具如表 2 清单所示。

表 2 模型及工具清单

序号	模型/工具	用途
1	text2vec-large-chinese	将文本数据进行向量化处理
2	ChatGLM3-6B	大语言模型
3	Qwen1.5-14B-chat	大语言模型
4	Qwen1.5-72B-chat	大语言模型
5	Milvus	向量数据库
6	体系需求采集与管理工具	将文档资源进行条目化解析和存储管理

(2) 首先准备好要导入的相关知识文件, 将利用 text2vec-large-chinese 模型对文档的三级摘要进行向量化处理, 如表 3 所示。

表 3 知识资源

序号	知识资源文件
1	军事信息系统体系结构设计方法及其应用分析
2	网络信息体系的顶层框架设计研究
.....
3	军事信息系统需求模型一致性检验方法
4	美军联合战役情报保障问题研究

(3) 问题分类字典如表 4 所示。

(4) 问题分类要素规则主要针对各个分类的要素进行了分析和编辑。其中对于

业务流程分类的规则要素如表 5 所示。

表 4 问题分类字典

序号	分类名称	分类标识
1	系统架构	AV-6
2	业务流程	OV-5a
3	信息活动	ProA-1a
4	能力分解	CV-1a
5	系统组成	SV-1a

表 5 业务流程问题要素规则

序号	分类名称
1	活动名称
2	执行者
3	信息输入
4	信息输出

(5) 根据导入的 30 篇论文资料, 人工方法从中抽取共 50 个问答对, 并标注出其答案中对应的体系模型要素, 如表 6 所示。

表 6 问答对

序号	模型要素分类	问答对数量
1	系统架构	10
2	业务流程	10
3	信息活动	10
4	能力分解	10
5	系统组成	10

3.2 实验案例分析

(1) 将知识资源文件导入体系需求采集与管理工具, 工具将解析文件, 并以条目化方式存储在关系型数据库中, 并利用大模型 Qwen1.5-14B 对文档进行三级文本摘要提取, 之后调用 text2vec-large-

chinese 对摘要进行向量化处理。

(2) 以用户输入复杂问题为案例：联合战役情报保障工作流程有哪些主要步骤和内容。

(3) 系统首先利用大模型对问题分类进行判断，得出问题分类为“业务流程”，其问题规则要素包含如表 4 所示。

(4) 按照用户的问题及规则要素在知识资源构建的向量数据库中进行资源匹配。

(5) 按照用户问题及规则要素进行提示词组装如下，并输入大语言模型：

<相关内容>

美军的联合战役情报保障工作包括情报的计划与指导、搜集、处理与利用、分析与整理、分发与整合、评估与反馈六个流程……

</相关内容>

你是一个体系架构设计人员,针对需求“联合战役情报保障工作流程有哪些主要步骤和内容”这个复杂问题,根据相关内容进行解答,要包含要素活动名称、执行者、信息输入、信息输出。

(6) Qwen1.5-B-chat 生成的答案如图 6 所示。



图 6 大模型生成复杂问题分解结果文本

(7) 将生成的答案转为流程图，如图 7 所示。

3.3 实验效果评价

(1) 基于问题规则的大语言模型问答交互效果。利用 50 个问答对，结合体系设计领域知识资源，对用户问题的输出结果采用专家评价的方式进行效果统计，如表 7 所示。

表 7 问答效果实验结果分析

序号	体系设计问题类型	知识点命中率	事实一致性	答案与用户问题相关性
1	系统架构	90.93	91.62	92.73
2	业务流程	91.94	90.64	91.88
3	信息活动	91.56	91.66	91.65
4	能力分解	91.94	90.56	90.44
5	系统组成	90.96	90.55	90.76
6	平均值	91.466	91.006	91.492

对知识命中的误差主要基于两个原因，一是大模型所支持的最大上下文长度是 32768Byte，为避免模型处理异常，需要对获取的知识文本进行截取，从而导致信息丢失；二是基于摘要的向量匹配会丢失一些关键字精确匹配的效果。

(2) 基于大语言模型集合的实体关系抽取效果评价。针对 50 个用户问题所输出的体系设计分解结果文本，从文本中提取出系统架构、业务流程、信息活动、能力分解、系统组成等体系设计实体要素及实体关系，效果如表 8 所示。

表 8 体系设计要素实体抽取实验结果分析

序号	体系结构模型类型	精确率 (%)	召回率 (%)	F1 值
1	系统架构	84.93	82.52	83.725
2	业务流程	77.26	78.03	74.645
3	信息活动	78.38	79.09	78.735
4	能力分解	86.54	88.06	77.3
5	系统组成	86.14	87.36	86.75
6	平均值			80.231

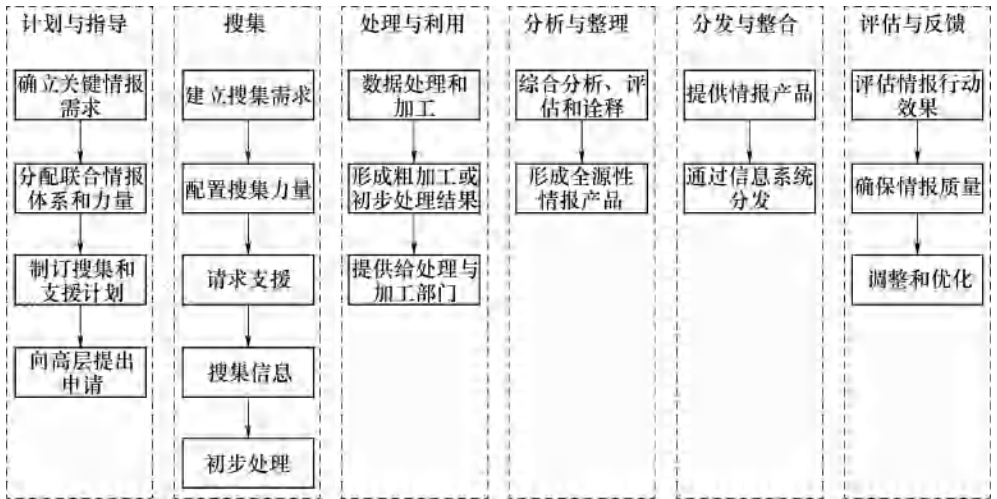


图7 将复杂问题分解结果转为业务流程模型

经过实验发现，实体抽取的效果取决于文本表达的准确性，文本中需要正确表达出实体间的从属、关联等关系，才能实现实体及关系的正确抽取，此外，序号、标号也会对大模型识别体系要素层次关系具有正向引导作用，在后续的项目工程中，可以进一步规范文本输出格式实现效果的进一步提升。

4 结束语

本文提出了一种基于大语言模型的复杂问题分解流程自动生成方法，基于三级文本摘要的资源数据存储、大语言模型问答交互、基于大模型集合的实体关系抽取与结果评估等思路进行方法实现。最后，结合具体实验环境和案例进行了实验，结果显示利用该方法能够有效解决体系设计领域复杂问题分解问题，验证了本文方法的有效性。

参考文献

- 舒振, 刘俊先, 罗爱民, 等. 军事信息系统体系结构设计方法及其应用分析 [J]. 科技导报, 2018, 36 (20): 48-56.
- HARTRUMPF S. Semantic decomposition for question answering [C] //European Conference on Artificial Intelligence. 2008: 313-317.
- 王振宇, 陆辰, 葛唯益, 等. 基于句法模板的复杂问题分解方法 [J]. 指挥信息系统与技术, 2019, 10 (5): 24-27.
- ZHANG H Y, CAI J J, XU J J, et al. Complex question decomposition for semantic parsing [C] //Proceedings of the 57th Conference of the Association for Computational Linguistics. 2019: 4477-4486.
- KHOT T, KHASHABI D, RICHARDSON K, et al. Text modular networks: learning to decompose tasks in the language of existing models [C] //Conference of the North American Chapter of the Association for Computational Linguistics. 2021: 1264-1279.

基于大语言模型的军事方案自动生成框架设计

王晓明¹ 包 括¹ 滕 飞¹

摘 要 为了提升军事指挥人员在复杂战场环境中的应变能力和决策效率,提出了基于大语言模型的军事方案自动生成框架。该框架以军事领域预训练大模型为基础,综合业务场景数据治理、领域大模型微调、检索增强生成、智能体 workflow 编排等技术,利用大模型的自然语言交互与工具调用执行的能力,自动分析与理解战场态势,高效准确生成行动决策内容,为指挥员提供智能化的决策支持和执行指导。

关键词 大语言模型, 决策自动生成, 模型微调, 检索增强生成, 智能体, workflow 编排

Design of a Framework for Automatic Generation of Military Plans Based on Large-Language-Model

WANG Xiao-Ming¹ BAO Kuo¹ TENG Fei¹

Abstract To enhance the ability to adapt to complex environments and improve decision-making efficiency, a framework for automatically generating military plans based on Large-Language-Model (LLM) has been proposed. The framework is built upon military domain-pretrained models, and integrates technologies such as scenarios data governance, domain-specific model fine-tuning, Retrieval-Augmented-Generation, and intelligent agent workflow orchestration. By leveraging the natural language interaction and tool invocation capabilities of LLM, it can automatically analyze and understand battlefield situations, efficiently and accurately generate decision content, and provide intelligent decision support and execution guidance for military individuals.

Key words large language model, decision-auto-making, fine-tuning, retrieval-augmented-generation, intelligent agent, workflow orchestration

0 引言

军事决策是为了达到一定的军事目的,在掌握大量军事信息的基础上,经过判断、推理而选择军事方案,下定决心并付诸实施的过程。传统军事决策主要依赖于指挥员对战场信息快速筛选、整合与分

析,快速完成行动方案的制订与选择。随着军事科技的高速发展和战争形态的迅猛变化,战争动态性与复杂性日益突出,“战争迷雾”严重影响指挥人员的判断和认知,因此,有必要引入信息化、自动化、智能化的辅助决策工具,帮助军事指挥员在复杂动态的战场环境中具有更好的信息处理能力、应变能力和决策能力。

1. 北京跟踪与通信技术研究所

1. Beijing Institute of Tracking and Telecommunications Technology

近年来,人工智能尤其是大模型技术在智能交互、内容生成等领域发展迅速。大模型因其在数据搜集分析、自然语言处理、推理泛化等方面具有优势,因此,在决策领域应用具有一定的可行性^[1]。本文以仿真推演中军事方案高效准确生成为需求,提出了一种基于大语言模型的军事方案自动生成框架。该框架以军事领域预训练大模型为基础,综合业务场景数据治理、领域大模型微调、检索增强生成、智能体 workflow 编排等技术,利用大模型的自然语言交互与工具调用的能力,自动分析与理解战场态势,高效准确生成行动决策内容。

1 现状分析

1.1 军事方案制订

军事方案的制订是一个“感性+理性”的过程,感性要求指挥员有着对战场环境与作战进程的“直觉”,表现出高超的临场指挥艺术,而理性则要求指挥员通过大量的演习训练将“直觉”和“艺术”培养出来。数字空间模拟对抗的仿真推演成为演习演训的主要手段之一^[2-3],本文所涉及的军事方案的制订,正是基于仿真推演而开展的。

一般来说,军事方案制订涉及行动构想、任务生成、军事行动(COA)规划、计划生成、行动指令等阶段,而后基于仿真系统开展仿真执行、测试验证、迭代优化、行动总结的流程实验^[4]。在整个过程中,大部分工作需要依赖技术人员与业务人员来合作完成,如军事领域知识梳理整合、行动构想的形式化表征、多场景多任务模板设计、任务序列主观判定优化、可执行计划求解方法设计、海量仿真结果分析整理等。可以看出,现有军事方案制订

具有人力密集、业务密集、技术密集的特点,但自动化水平不高,智能化特点不足,人机交互能力一般。

1.2 大模型的决策优势

大模型属于人工智能生成(AIGC)技术的一种,能够通过学习人类语言与相关领域知识,获得智能化的创作和涌现能力,从而自动生成不同于训练数据的新内容^[5]。自2022年,以ChatGPT、SORA、文心一言^[6]为代表的大模型展现了通用大模型在人机智能交互、多模态内容生成等方面的强大能力,广泛用于教育、娱乐、新闻、科技、艺术等民用领域。大模型正在从“能听、会说、能看、会控”,逐步走向“能理解、会思考、会创作”,进一步去实现“自主决策、自主处理问题”。

大模型在情报分析、军事决策等军事领域具有较大的发展与应用潜力^[7-8]。美国Scale AI公司的大语言模型可帮助作战人员、分析人员和决策者加速对战场态势的理解、计划和行动。美国Palantir(明略数据)公司的人工智能平台AIP(软件智能体平台),集成大语言模型实现了对作战数据协同、行动方案建议等,为作战指挥提供快速方案并优化后勤保障管理,如图1所示。

大模型应用于军事方案制订,主要得益于以下几个特点:

(1) 自然语言处理能力和推理能力,可以智能地分析、理解和生成战场态势,为指挥员提供智能化的决策支持和行动指导。

(2) 大语言模型的自动化处理能力,调用小模型可以实现整个过程的自动化处理和优化,最大程度上减少人为的思考和操作。

(3) 大语言模型可以整合多种工具和系统,包括仿真系统、数据分析系统、报告生成系统等,实现多元信息交互和协同处理。

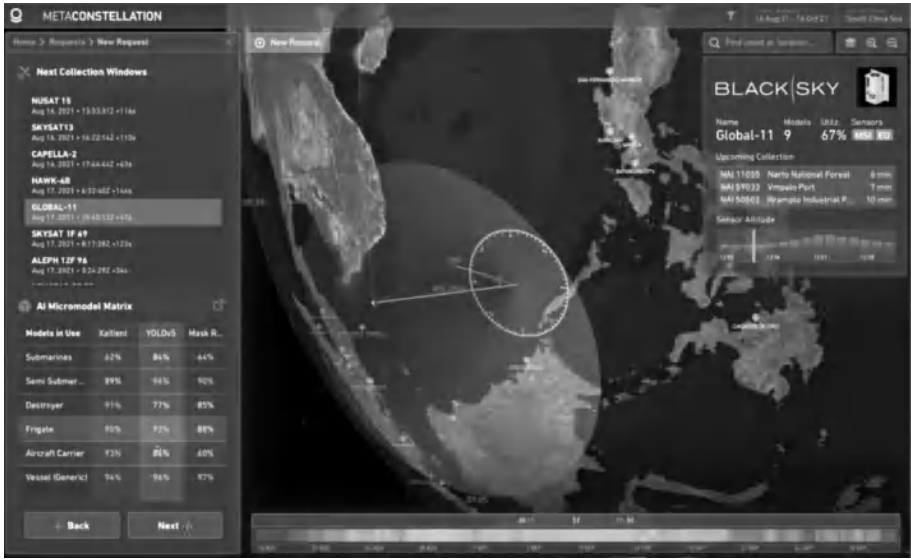


图1 Palantir 开发的大模型决策平台 AIP

2 关键问题

基于大语言模型的军事方案自动生成^[9], 是在实际流程中替代或辅助指挥员完成思考并操作, 如进行行动阶段划分、行动方案描述、填参数、文字转代码、绘制甘特图、分析数据并生成报告等。图2给出了军事方案生成的五个阶段。

其中:

(1) 行动构想划分阶段, 利用领域大模型的数据抽取与清洗能力完成多源异构的非结构化军事数据的标准化, 通过提示工程控制领域大模型输出形式, 实现行动构想和行动任务的形式化表示, 辅助行动构想划分。

(2) 行动任务生成阶段, 利用大语言模型的生成能力自动解析军事任务并完成任务模板中部分参数的填充。

(3) COA 规划阶段, 利用大模型的上下文学习、思维树训练及对外部模型调用能力, 完成行动序列生成与优化。

(4) 行动计划生成阶段, 结合求解结果和想定生成行动计划生成规范性描述, 并生成行动甘特图。

(5) 行动指令生成阶段, 将规范性描述转化为调用仿真代码进行推演, 基于大模型仿真结果数据进行数据比较分析、报告生成。

在上述过程中, 大模型在数据处理、代码生成等方面都得到良好的应用, 但仍需要解决以下两个关键问题:

(1) 垂直领域知识生成的实时性与可信性。由于应用场景的特殊性, 面向军事领域垂直大语言模型必须具有准确的语言理解能力, 以及可靠可信的专业内容生成能力。增量预训练与模型微调训练使得领域大模型具备了大量的军事作战相关知识, 并在一定程度上具备良好的人机交互能力。但这两种方式仍是基于受数据依赖的深度学习方法, 对文本等知识库的构建与应用具有较高的标准要求。同时, 领域大模型在适应快速更新的军事理论、作战概念、装备技术、实践应用等动态数据存

在较大挑战，难以生成质量高、实时性强、可信性强的生成。

(2) 行动决策序列生成的专业性与准确性。军事方案生成是涉及多军种、多场景、多任务的复杂决策过程，通常涉及多名专业人员会商研讨，逐步迭代形成多个可行的方案并优化。尽管目前大语言模型具备一定的推理能力，但经测试单一任务

下，大模型经过若干次推理后准确度明显下降。另外，基于增量预训练和模型微调的大语言模型在面对不同场景时表现的泛化能力有限，且由于其生成机制和推理模式制约，在缺乏相关数据和背景知识的前提下，大语言模型会产生非严格基于事实的反应或者非专业的回答，即所谓的“幻觉”。

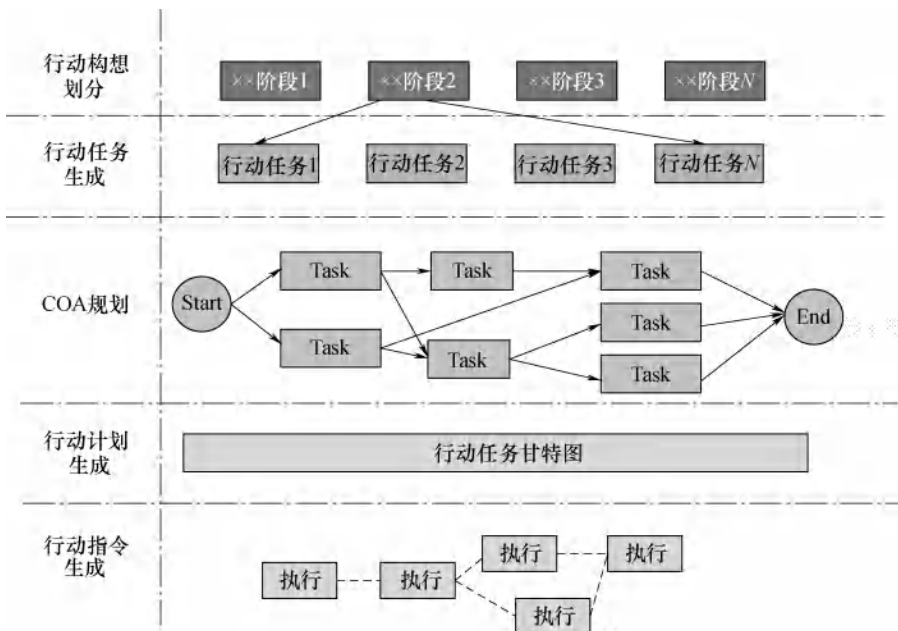


图2 军事方案生成五个阶段

3 框架设计

如图3所示，基于大语言模型的军事方案自动生成框架主要包括以下三个部分。

3.1 领域大模型

利用增量预训练与模型微调的方法，形成基础的军事领域大模型，为军事方案自动生成框架提供语言理解和生成能力。

从技术路线上看，军事决策类领域大模型，首先结合军事数据对通用大模型进

行增量训练，形成军事领域大模型，而后对其进行微调训练，使得领域大模型更加适应于下游特定任务，比如军事方案制订。形象地说，第一步是将大模型打造成“军事爱好者”，第二步则是将大模型培训成为“军事领域专家”。相比之下，微调更加重要。

大模型微调主要包括两类方法：全量参数微调与参数高效微调。全量参数微调方法^[10]是在大模型基础上调整所有层和参数，以适应特定任务，这一过程可以使用较小的学习率和特定的任务数据进行，充

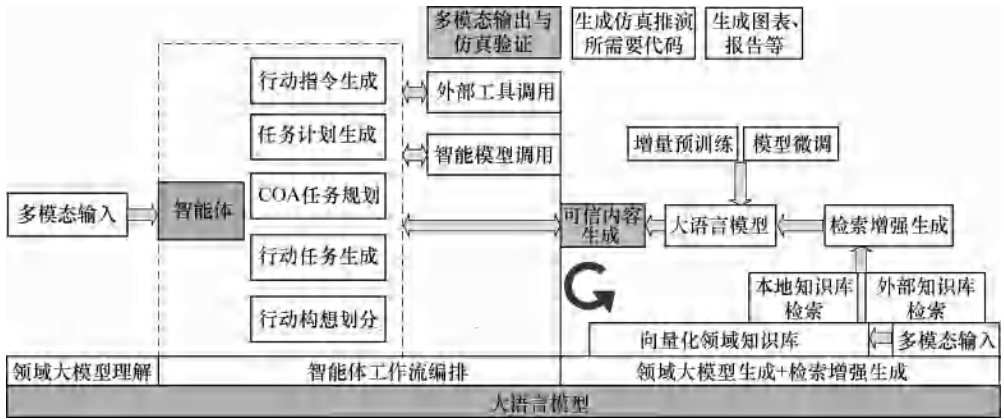


图3 基于大语言模型的军事方案自动生成框架

分利用预训练大模型的通用特征，但需要更多的计算资源。参数高效微调（PEFT）是指微调少量或额外的模型参数，并固定大部分预训练模型参数的方法^[11]，即减少可训练参数数量的情况下同时保持全量参数微调相当的性能，目前主要包括 LoRA、prefix-tuning、P-tuning、Prompt-tuning、AdaLoRA^[12-14]等参数高效微调方法。领域大模型的微调需要适应的下游任务包括以下三方面。

1. 符合业务框架的规划内容的生成

符合业务框架的规划内容生成涉及将军事作战中的战略、战术、情报、后勤等内容，根据特定的业务框架和需求进行生成。因此，对领域大模型微调使其能够理解业务框架，包括其中的关键概念、组织结构、决策流程等。

2. 适应仿真并进行调用的代码生成

军事方案生成需要通过军用仿真系统进行应用与验证，要求领域大模型具备调用仿真并执行的自动化能力，因此，需要针对代码输出方面进行大模型的微调，明确大模型所需要深入理解的仿真环境，包括编程语言、仿真平台、输入输出格式等。

3. 结合提示工程进行军事业务推理

结合提示工程进行军事业务推理是指

利用设计好的提示语或前缀来引导语言模型进行推理，从而生成符合军事业务逻辑和需求的推理结果。通过给模型提供特定的上下文信息，引导其理解和推理与军事业务相关的问题。

通过增量预训练与模型微调形成的领域大模型，针对军事场景具有良好的理解能力与较为准确的生成能力。

3.2 可信内容生成

可信生成，是指通过对本地知识库与外部知识库多级检索增强，提升大模型对最新的军事领域知识和概念的适应性，产生符合要求、准确且多样的回答军事方案的文本内容，实现领域大模型灵活交互与可信生成。主要包括两个部分：

(1) 领域数据治理及行动方案知识库构建。军事方案的制订涉及大量的相关数据、知识，包括开源数据、条令条例、经典战例以及私有化的军事文档，大部分知识数据属于非结构化、半结构化。面向军事方案制订的领域大模型，需要对数据进行清洗和标准化处理，形成适应于领域大模型的结构化文本语料，而结构化的文本语料可用于支持领域大模型的增量预训练

与微调训练，也可以构建军事方案知识向量库。利用知识向量化将自然语言文本转换为领域大模型可以理解和处理的数值形式，并形成向量数据库，便于大模型向量化检索，快速召回最相关的内容进入上下文，辅助生成更专业内容。

(2) 基于行动方案知识库的检索增强生成。可信生成实现的核心是大模型检索增强生成技术 (Retrieval-Augmented-Generation, RAG)，这是一种结合传统信息检索技术和最新的生成式深度学习模型，旨在提升大型语言模型在特定任务

上的表现。大模型检索增强生成通过在生成过程中引入外部知识源，使得模型能够访问和利用更广泛的信息，其优势在于：

(1) 生成包含更多细节和背景信息的内容，进一步提高生成的准确性、相关性和实时性。

(2) 可以适应各种不同的任务和领域，只需更换检索的外部数据库即可。

(3) 外部知识库作为生成知识的信息源，提高了生成内容的可追溯性和可解释性，如图4所示。

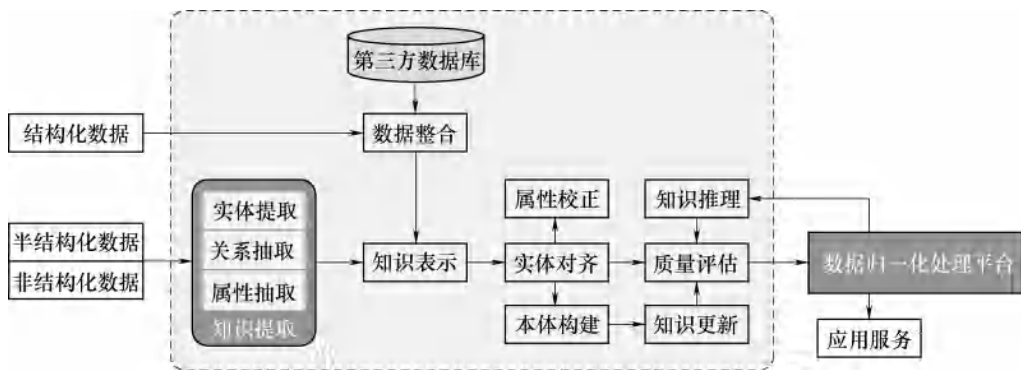


图4 数据清洗与标准化处理

3.3 智能体 workflow 编排

与传统大语言模型的单次提示工程不同，大模型智能体及 workflow 编排通过创建提示性的框架和引导，引入业务上更精细的规则和标准处理流程，多次提示大模型，生成更高质量、更为准确、更为可靠的内容，适合严谨军事方案生成场景。

1. 大模型智能体能力架构

大模型智能体 (LLM agent)^[15] 是一种以大模型为核心控制器的智能系统，通过包含规划 (plan)、记忆 (memory) 与工具 (tools) 等关键模块的架构，来执行复杂任务的大模型应用程序。

计划模块的功能包括：①子目标和分解，基于思维链将大型任务分解为较小的、可管理的子目标，有效地处理复杂的任务；②反思与细化，通过反思与自省框架，对过去行为分析、总结和提炼，以提高自身的智能和适应性。

记忆模块的功能包括：①通过短期记忆进行上下文学习，生成用户期待的答案；②通过长期记忆，利用外部的向量存储（即构建的向量数据库）和快速检索来存储和召回无限信息。

工具使用模块的功能包括：①通过调用函数或者外部 API，以获取大模型能力以外的能力和信息；②通过调用插件访问最新信息或者特定的数据源。

2. 智能体 workflow

智能体 workflow (AI agent workflow) 成为大模型最新应用方式。和传统的大语言模型使用方式不同, 智能体 workflow 不是让大模型直接生成最终输出, 而是多次提示大模型, 使其逐步构建更高质量的输出。斯坦福大学吴恩达教授在红杉 AI 峰会上认为当前智能体 workflow 主要有以下四种设计模式:

(1) 反思 (Reflect), 驱动大模型审视和修正生成的输出, 并提出修改方向。

(2) 工具使用 (Tool Use), 通过生成代码、调用 API 等操作, 具有使用外部工具和资源能力。

(3) 规划 (Plan), 面对复杂任务时, 对任务进行分解, 并按照计划执行任务。

(4) 多智能体协作 (Multi-agent Collaboration), 多智能体协同工作, 共同完成复杂任务。

3. 方案生成 workflow 编排

面对多场景多目标的军事方案生成需求, 通过采用 workflow 编排的方式平衡模型能力与方案生成业务需求, 将行动方案规划的开放域、复杂多步问题, 分解为多个子问题分开解决, 提供大量提示性的框架和引导, “能用模型用模型、不能用模型的用流程”, 甚至采用人在回路方式, 将整个 workflow 白盒化, 把大模型能力限制在封闭的问题内, 让大模型更可控, 提升整个应用的可解释性和鲁棒性。

智能体 workflow 编排可以实现:

(1) 复杂决策过程的可视化编排, 即利用可视化工具和技术, 帮助军事人员、业务人员更直观地了解和管理模型的工作流程。

(2) 多场景的任务规划链路的分流推理, 通过任务规划链路的编排和对不同链路的分流推理实现, 提升了方案生成多元性, 如图 5 所示。

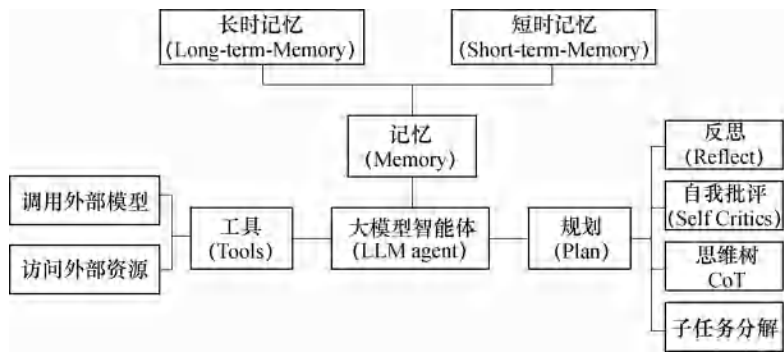


图 5 大模型智能体架构

4 应用方式

如图 6 所示, 基于大语言模型的军事方案自动生成框架, 可实现辅助或替代人力实现方案生成的自动化。包括: ①非结构化数据的标准化, 同时通过提示工程控制大模型

输出形式, 实现作战构想和军事任务的形式化表示; ②自动解析军事任务并进行部分参数的填充; ③通过上下文学习及调用外部模型进行行动序列的优化, 编排生成行动方案; ④按照行动方案, 解析行动序列生成仿真代码语言, 调用仿真进行推演; ⑤对仿真验证结果自动总结, 生成报告。

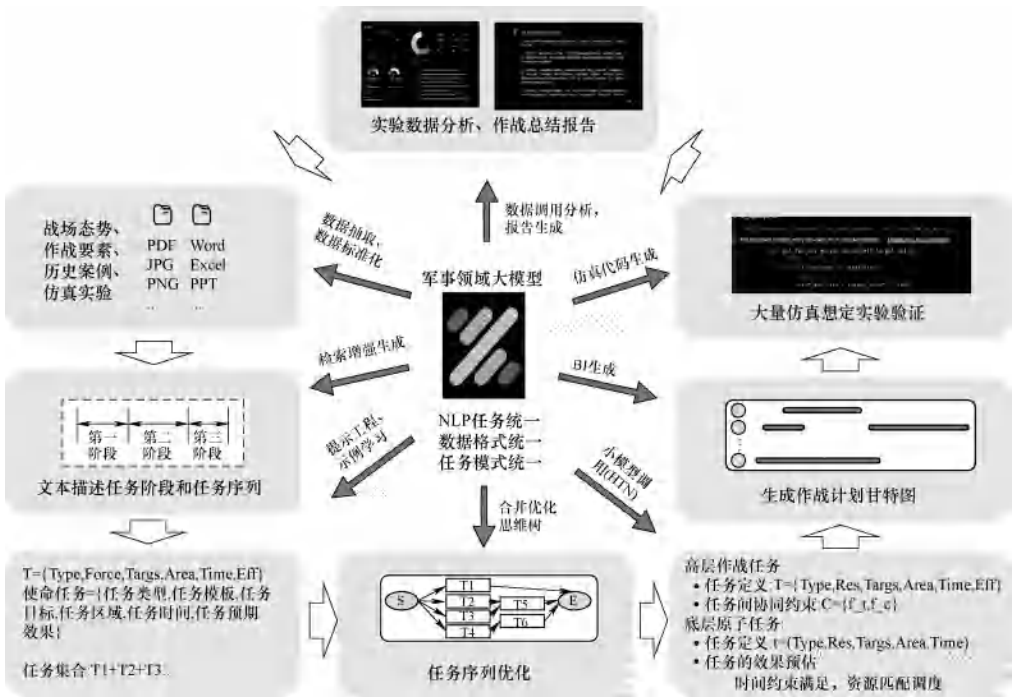


图6 军事方案生成流程中的应用方式

围绕行动方案生成应用，设计任务规划智能体与任务执行智能体两类，其中，任务规划智能体实现当前战场态势的行动方案规划，任务执行智能体执行当前方案并评估，二者结合实时迭代实现军事方案

的动态重构。

如图7所示，以行动方案生成任务规划阶段为例，大模型能力覆盖方案生成业务知识、任务规划、任务序列生成、任务执行的全流程中。其应用流程为：

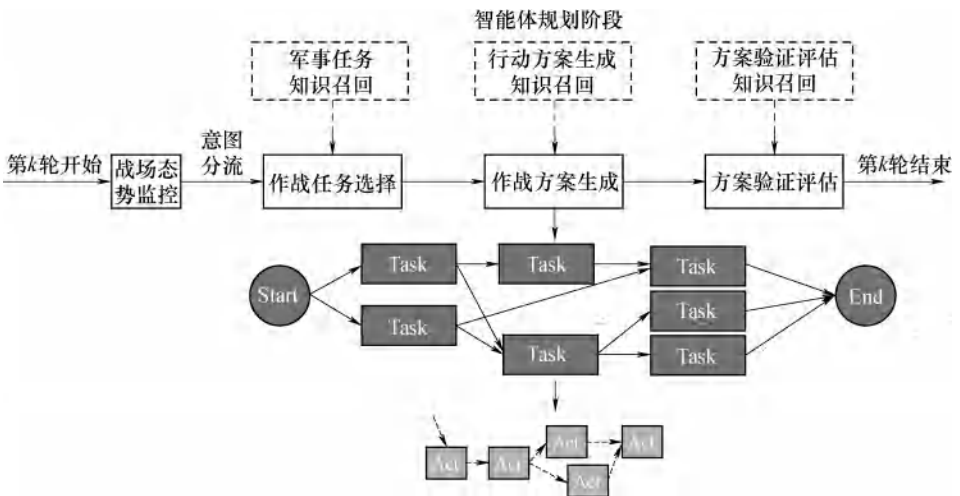


图7 智能体规划阶段示意图

(1) 基于训练后的领域大模型在当前战场态势下进行意图理解完成分类任务,明确军事任务选择;同时在军事任务选择、行动方案生成、方案验证评估环节,均通过大模型的检索增强辅助提高大模型对不同环节业务的理解。

(2) 在任务规划过程中,通过示例学习,在提示中加入目标示例,实现对大模型输出的控制,同时通过提示工程提高大模型对当前任务的拆解能力,拆解为可实现的子任务,实现任务序列的生成。

(3) 在子任务执行过程中,大模型检索调度合适的工具(内部外部各类算法、模型、程序等),通过反思(reflect)方式解决子任务;完成任务执行后进行结果反馈及反思,有助于后续的重新规划与二次迭代。

5 结束语

本文以军事方案高效准确生成为需求牵引,以军事领域的大语言模型为核心,综合了智能体 workflow、检索增强生成等技术,形成了一种基于大语言模型的军事方案自动生成框架,该框架可初步支持行动方案的智能生成,对构建新型军事指挥控制辅助决策的技术体系具有参考作用。后续,将结合敌我友环各类要素、资源和时间等约束条件,逐步提升复杂对抗条件下的军事方案生成的科学性与可信性。

参考文献

- 1 杨芸,李雪青.基于人工智能的智能化战争形态发展研究[J].国防科技,2023,44(1):47-53.
- 2 陈俊,邓青.当前军事仿真领域内新技术的应

用与发展[J].信息与电脑(理论版),2019(5):24-25.

- 3 BRUZZONE A G, MASSEI M. Simulation-based military training [M]. Guide to Simulation-Based Disciplines: Advancing Our Computational Future, 2017,315-361.
- 4 张俊峰,薛青,吴堃,等.军事行动推演系统通用建模机制研究[J].计算机仿真,2018,35(6):13-17.
- 5 CHANG Y. A survey on evaluation of large language models [J]. ACM Transactions on Intelligent Systems and Technology, 2024, 15(3): 1-45.
- 6 KALYAN K S. A survey of gpt-3 family large language models including chatgpt and gpt-4 [J]. Natural Language Processing Journal, 2023: 100048.
- 7 曹宏业,刘潇,董绍康,等.面向强化学习的可解释性研究综述[J/OL].计算机学报,1-31[2024-06-27].<http://kns.cnki.net/kcms/detail/11.1826.TP.20240423.1319.004.html>.
- 8 蔡磊,孟宪波,韩冬梅,等.大模型在军事垂直领域的应用[J].舰船科学技术,2024,46(5):171-175.
- 9 汲克山,刘思培,李清玉,等.大模型在军事领域的应用与展望[C]//中国指挥与控制学会第十二届中国指挥控制大会论文集(下册).北京:兵器工业出版社,2024.
- 10 LV K. Full parameter fine-tuning for large language models with limited resources [J]. arXiv preprint arXiv: 2306.09782, 2023.
- 11 DING N. Parameter-efficient fine-tuning of large-scale pre-trained language models [J]. Nature Machine Intelligence, 2023, 5(3): 220-235.
- 12 HU E J. Lora: Low-rank adaptation of large language models [J]. arXiv preprint arXiv: 2106.09685, 2021.
- 13 LI X L, LIANG P. Prefix-Tuning: Optimizing Continuous Prompts for Generation [C]//Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language

- Processing. 2021: 4582-4597.
- 14 ZHANG Q. AdaLoRA: Adaptive budget allocation for parameter-efficient fine-tuning [J]. arXiv preprint arXiv: 2303. 10512, 2023.
- 15 LEWIS P. Retrieval-augmented generation for knowledge-intensive NLP tasks [J]. Advances in Neural Information Processing Systems, 2020, 33: 9459-9474.

基于大语言模型的军事智能翻译算法研究**

张聚憬¹ 杨娟^{1*} 谢林川¹

摘要 针对普通智能算法对外军相关军事文献翻译精度不高的问题,提出基于大语言模型的军事智能翻译算法(ITAfM算法)。该算法通过构建军事向量知识库,采用RAG方法将待翻译文本的特征向量与向量知识库进行相似度比对,检索待翻译文本所涉及的军事专业词汇的k-top关键词,同时改进了最优译文匹配检索方法,最终结合提示词工程实现精准翻译。实验证明,ITAfM算法对军事专业术语数据集翻译的BLUE得分较以往算法高,具备较为理想的翻译效果和实用价值。

关键词 智能翻译, 军事, 大语言模型, RAG, 语义相似度

Research on Military Intelligent Translation Algorithm Based on Large Language Model**

ZHANG Ju-Jing¹ YANG Juan^{1*} XIE Lin-Chuan¹

Abstract Addressing the issue of low translation accuracy in foreign military literature with conventional intelligent algorithms, a military intelligent translation algorithm (ITAfM) based on a large language model is proposed. This algorithm establishes a military vector knowledge base and employs the RAG method to compare the similarity between the feature vectors of the text to be translated and the vector knowledge base. It retrieves the k-top keywords related to the military professional vocabulary from the text, and enhances the optimal translation matching retrieval method. Finally, it integrates with prompt word engineering to achieve precise translation. Experimental results demonstrate that the ITAfM algorithm achieves a higher BLUE score in translating military terminology datasets than previous algorithms, offering effective translation and practical utility.

Key words intelligent translation, military, large language model, RAG, semantic similarity

0 引言

对外军军事文献的翻译工作作为情报

界对敌研究的关键环节,其准确性和效率直接影响到我军掌握敌动态的顺畅程度。特别是在涉及军事斗争的专业领域,如指挥、军兵种、武器装备等,由于术语的复

** 军事理论重点项目(J20231001)资助

** Supported by Key Projects in Military Theory (J20231001)

* 通讯作者

1. 中国人民武装警察部队警官学院

1. Chinese People's Armed Police Force Police Academy

杂性和专业性,对翻译质量的要求更为严格^[1]。传统的翻译方法,如人工翻译和基于规则的机器翻译,虽在一定程度上满足了翻译需求,但在处理大规模文本、保持术语一致性和适应语言变化等方面存在明显不足。而智能翻译算法如利用 OCR (光学字符识别) 技术从纸质或电子文档中识别英文文本,随后将识别出的文本传递给智能翻译算法^[2],为叙述方便,下文简称为 OCR 法。OCR 法基于深度学习和神经网络,通过训练大量双语语料库来构建翻译模型。然而,由于 OCR 识别过程中可能存在的误差,如字符识别错误或格式识别不准确,这些误差会被传递给翻译模型,从而导致翻译结果的准确性降低。另外,还有利用属性概率权重对文本中的词汇、句法和语义特征进行加权处理,从而实现对本体的有效分类算法^[3],本文简称为属性法。尽管属性法在多数场景下能够显著提高翻译质量,但在处理特定领域的专业术语和长难句时,由于算法对专业知识的缺乏,往往难以达到理想的翻译效果。Ban 等提出了一种基于机器智能翻译和安全物联网的英语自动翻译系统。该系统结合先进的机器翻译技术和物联网的安全特性,能够为用户提供高效、安全的翻译服务。但是,该系统的翻译准确性受到多种因素的制约,如训练数据的规模和质量、翻译模型的复杂性和泛化能力等^[4]。文献[5]通过构建多个英汉双语语料库,并利用关键词搜索技术从语料库中检索出与待翻译文本相似的句子或段落,从而实现英汉自动翻译。但由于语料库的规模和覆盖范围有限,该方法在处理某些特定领域的文本时可能无法找到足够相似的句子或段落,从而导致翻译结果的不准确。此外,关键词搜索技术的准确性和效率也受到待翻译文本的语言特性和复杂程度的影响。

当前,国内外大语言模型,如 chatGPT、InternLM 等,以其强大的语言理解和生成能力,为翻译算法的研究提供了崭新的思路。与传统的生成式模型相比,它在处理复杂问题时更加得心应手,生成的内容也更加准确。这些模型通过大规模语料库的预训练,能够学习到丰富的语言知识和上下文信息,从而在翻译过程中更好地理解 and 表达原文的含义。此外,检索增强生成 (RAG) 与大模型相结合能够迅速检索到相关信息,并据此生成高质量的自然语言文本^[6],与传统的生成式模型相比,它在处理复杂问题时更加得心应手,生成的内容也更加准确。因此,基于大语言模型的军事领域智能翻译算法,成为当前军事领域的研究热点^[7]。有鉴于此,本文提出 ITAfM (Intelligent Translation Algorithm for Military Field Based on Large Language Models) 算法,用以解决军事领域精准翻译问题。本文创新点如下:

(1) 提出了 k -top 关键词 V_k 提取方法,高效精准提取待翻译文本关键词。

(2) 提出了融合术语匹配率以及语义相似度两个指标的特定领域内准确度 DSA 评价方法,创新性对候选文本的翻译质量进行评估,从而有效提高了专业领域的翻译效果。

1 基于大语言模型的军事领域智能翻译算法

1.1 军事专业名词向量知识库构建

为结合 RAG 检索军事专业术语词汇对照表实现专业领域智能翻译,本文首先对军事专业术语中英文对照(包含 65319 条英汉军事术语对照,由原南京炮兵学院季西亚教授整理)中的名词进行对齐提取,

从而构建出平行语料库。

步骤 1: 进行文本分割。

由于对齐语料库采用 csv 格式存储, 记录之间使用换行符隔开, 为了确保后续检索的准确性, 在对文本进行分割时依据换行符进行分割, 将文本切分为若干片段 (Text Chunks)。

步骤 2: 进行文本嵌入。

为了便于后续的向量检索库的构建, 需对文本进行向量化, 首先需要对文本中的特殊字符、停用词等进行去除, 从而确保处理文本质量。其次将文本切分为单词或子词 (subword) 单元, 并映射到采用 Transformer 为基本架构的 Embdding 模型词汇表中, 生成对应的标记 (token) 序列。每个 token 通过嵌入矩阵 W_e 转换得到嵌入向量 $e^{[8]}$:

$$e = W_e \cdot \text{token} \quad (1)$$

将嵌入向量 e 作为 Embdding 模型的输入, 通过编码器进行编码, 得到每个标记的上下文表示。

步骤 3: 构建向量检索库。

为了便于后续大规模向量数据的检索, 需要将嵌入后的向量存储到向量库中, 本文采用开源向量检索库 Faiss 构建向量库。

至此, 军事专业名词向量知识库构建完毕。

1.2 关键词向量化提取

为了便于后续的关键词提取, 首先结合 Embdding 模型对输入给大模型的待翻译文本进行编码, 其计算结果得到 V_{Text} 。

假设军事术语词汇编码结果为 V_w , 那么可以计算出术语词汇编码向量与文本编码向量之间的相似度 $Sim(w, Text)$, 具体计算公式如式 (2)^[9]所示。

$$Sim(w, Text) = \frac{V_w \cdot V_{Text}}{\|V_w\| \cdot \|V_{Text}\|} \quad (2)$$

由于待翻译文本中的关键词与向量库中词汇存在一定偏差, 为了尽可能多地提取出关键词供后续的大模型翻译参考, 接下来, 将术语词汇与待翻译文本的相似度进行排序, 为此, 做如下定义:

定义 1: k-top 关键词 V_k 。

术语词汇与待翻译文本相似度高的前 k 个词叫作 k-top 关键词, 由式 (3) 确定:

$$V_k = \sum_{z \in \text{top-}k(Sim(w, Text))} p_\eta(z | V_{Text}) \quad (3)$$

式中, p_η 为检索器; z 为向量检索库; V_{Text} 为向量化后的待翻译文本。

通过以上流程即可完成对待翻译文本中涉及军事专业术语的关键词的有效提取。

1.3 改进的最优译文匹配检索

在提取出待译文本的关键词后, 本算法选择在军事专业术语向量知识库中检索包含这些关键词的术语文本, 并结合关键词权重来对检索结果进行优化, 从而生成最优译文匹配结果。

为了对关键词的译文文本进行有效检索, 首先结合逻辑操作符对检索条件进行定义。假设上文中提取出的中文关键词集合为 $K = k_1, k_2, \dots, k_n$, 其中 k_i 代表第 i 个关键词^[10]。那么设定 AND(\wedge) 表示所有关键词都必须出现在目标文本中, OR(\vee) 表示至少有一个关键词出现在目标文本中, NOT(\neg) 表示某个关键词不能出现在目标文本中。基于关键词集合和布尔操作符, 可以构建不同的布尔查询, 具体布尔查询对应情况如表 1 所示。

基于上述构建出的布尔查询对应规则, 在向量知识库中, 遍历与每个关键词相关联的文本列表。对于每个查询, 根据

所选的布尔操作符 (AND、OR、NOT), 可组合出关键词对应的文本列表。

表 1 布尔操作符查询对应情况

查询描述	布尔操作符
查询包含所有关键词的文本	$k_1 \wedge k_2 \wedge \dots \wedge k_n$
查询包含至少一个关键词的文本	$k_1 \mid k_2 \mid \dots \mid k_n$
查询包含关键词 k_1 但不包含关键词 k_2 的文本	$k_1 \wedge \neg k_2$

对于检索到的多个候选译文文本, 为了提高后期的翻译准确性, 需要改进传统的最优译文匹配检索方法。本文提出对候选文本的质量进行先期评估, 从而找到最优的匹配译文。为此, 做如下定义:

定义 2: 特定领域准确度 DSA, 如式 (4) 所示。

$$DSA = \frac{\ln(R_{TMR}) \cdot \omega_{TMR}}{R_{SS} \cdot \omega_{SS}} \quad (4)$$

式中, R_{TMR} 为候选文档与待匹配译文之间的语义相似度; R_{SS} 为军事领域语境下的术语匹配率; ω_{TMR} 和 ω_{SS} 分别为两个指标对应的权重分配系数。

DSA 融合了术语匹配率以及语义相似度两个指标, 可以用于衡量译文在特定领域内的准确性。DSA 的计算结果, 可以对候选文本的质量进行评估, 从而选取质量最高的候选文本 T_k 作为军事术语的最优译文传入给大模型。

1.4 结合提示词工程生成专业翻译

将待翻译文本中涉及军事专业词汇的短语或文段及其译文经过提示词模板的包装, 作为上下文传入给大语言模型, 本算法采用开源工具 Langchain 构造提示词模板 $p(\text{Text})$, 其基本框架为:

“你是一名出色的军事翻译官, 现由你来将以下英文军事文本内容翻译成中文: $\{\text{Text}\}$

文本中包含以下关键词: $\{V_k\}$

其中文释义为: $\{T_k\}$

在翻译时务必结合语境将关键词准确翻译出, 不得改变关键词的中文释义。

如英文: “naval rear shore command post was set in a pine forest nearby bight.” 的译文为: “海军岸上前进指挥所设在海岸凹入部附件的松林里。”

在模板中, Text 为待翻译文本, V_k 为文本中的军事专业术语, T_k 则为通过上述方法检索出的中文释义, 最终大语言模型得出的输出可用式 (5) 描述:

$$\hat{a} = \text{argmax}(\theta(a \mid p(\text{Text}))) \quad (5)$$

式中, θ 为大模型; a 为模型的输出; \hat{a} 为期望的输出结果。

ITAfM 算法框架如下:

输入: 包含军事术语的待翻译文本

1. 依据军事术语特点, 进行文本分割、文本嵌入, 构建军事专业术语向量知识库;
2. 基于式 (3) 进行 t-top 关键词向量化提取;
3. DSA (式 (4)) 量化的最优译文匹配检索;
4. 采用开源工具 Langchain 构建提示词模板 $p(\text{Text})$;
5. 大模型输出高质量最终译文。

ITAfM 算法流程如图 1 所示。至此, 基于大语言模型的专业领域智能翻译算法设计完成。

2 实验验证

为了验证本算法的性能, 通过实验验证环节, 对本算法的实际翻译效果进行检验。

2.1 实验说明

本次实验首先验证算法在 DSA 评分下

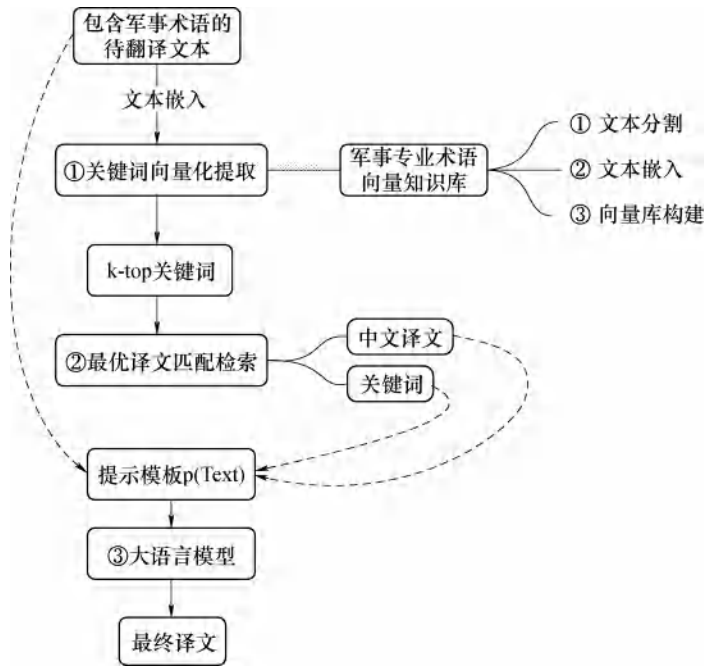


图 1 ITAFM 算法流程

的准确率。进一步选取两组常规的专业领域智能翻译算法作为对比对象，分别为 OCR 法和属性法。通过构建实验平台，采用三种翻译算法对同一组中文文本进行翻译处理，对比不同方法的实际翻译效果。

2.2 实验对象

构建包含军事专业术语中英文词汇对照表中词汇的实验数据集，首先需从对照表中筛选目标词汇，随后收集相关原始文本，进行分词、去除停用词等预处理。接着，在文本中精确标注目标词汇及其中英文对照，并按需划分成训练、验证和测试集。之后，对数据集进行清洗和验证，确保标注准确性和数据质量。从对照表中提取术语，确保术语的准确性和专业性，并从多个来源收集，具体包括外文军事文献、学术论文、军事新闻报道等。对收集

到的专业术语进行清洗，去除无关信息、特殊字符、冗余内容等。并使用数据库查询等技术手段进行去重，确保数据集中没有重复项。根据收集到的中英文对照表，将专业术语分为中文和英文两个部分。对于缺少英文对照的中文术语，本文选择通过机器翻译工具进行翻译，然后经过专家审核确认。为每个专业术语生成一定数量的句子或段落，这些句子或段落需要包含该术语，并符合专业领域的语言特点。

为了兼顾硬件条件限制和语言模型的上下文理解能力，实验所采用的大语言模型为上海人工智能实验室发布的开源模型 InterLM2-chat-20B，具体软硬件参数配置如表 2 所示。

本算法对实验数据集进行翻译测试时，需要对算法的具体参数进行设定，其具体参数配置情况如表 3 所示。

表 2 实验软硬件参数配置表

名称	参 数
操作系统	Ubuntu 22. 04 LTS
软件工具	Anaconda、Pycharm
硬件平台	Intel (R) Core (TM) i7-10750H CPU、NVIDIA GeForce RTX 4090
使用模型	InterLM2-chat-20B
量化程度	FP32
Embdding 模型	Python = 3. 10
编程语言	Python = 3. 10
学习框架	pytorch

表 3 智能翻译算法的参数配置

参 数	配置
专有名词的频次最大值 $\max P_i$	100
专有名词序列公共子串总数 n_{common}	25
文本编码 V_w 数量	150
词汇编码 V_{Text} 数量	100
布尔操作符数量	5

表 4 ITAfM 算法的翻译结果

序号	待翻译文本	候选译文	DSA (%)
1	The Chinese People’s Armed Police Force is on duty according to the regulations of guard duty of the Chinese Peoples Armed Police Force	中国人民武装警察部队按照中国人民武装警察部队执勤规定执勤	98.4
2	Militaries around the world are actively developing vehicle mounted laser air defence weapons to deal with drone swarms	各国军队正在积极研究车载激光防空武器以应对无人机蜂群打击	99.5
3	C ⁴ I integration support activity plays an important role in military action, and make full use of beta-gamma coincidence counting method to have the initiative in ones hands	C ⁴ I 综合集成支持小组在军事行动中扮演重要角色, 应当充分利用 β - γ 符合计数法来掌握战争主动权	98.6
4	On modern warships, an overhead feeding system is adopted, allowing the turrets to fire quickly and continuously, improving operational efficiency	在现代化的战舰上, 采用了上方供弹系统, 使得炮塔能够快速、连续地进行射击, 提高了作战效率	99.1

通过采用上述参数对本文提出的智能翻译算法进行配置, 并分别结合三种方法对实验数据集中的文本进行翻译处理。待实验完成后, 对不同翻译方法下的实际翻译结果进行记录, 并计算出不同翻译结果的 BLEU 分数, 从而实现实验对比分析。

2.3 翻译精度对比结果

本翻译算法所得到的翻译结果如表 4 所示。

其实际应用场景的翻译效果如图 2 所示。

上述实验结果显示, 采用 ITAfM 算法对军事领域文本进行智能翻译时, DSA 较高, 能够生成较为理想的译文。

进一步, 为验证本算法的有效性, 采用相同待翻译文本, 将本算法与 OCR 法、属性法的翻译结果用经典的 BLEU 分数对比, 具体得分对比结果如图 3 所示。



图2 智能翻译算法应用效果图

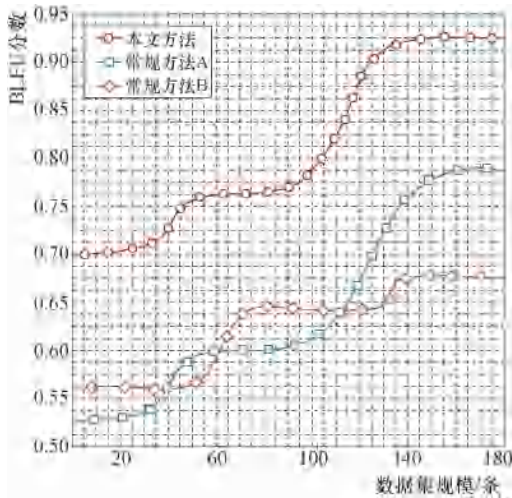


图3 相同翻译文本三种算法的 BLEU 分数

由图3可见,在针对相同的军事专业文本数据集进行翻译时,不同方法的实际翻译效果也有所不同。而本文提出的

ITAFm 算法在实际翻译精度方面明显优于两种常规的智能翻译算法,翻译输出与参考译文之间的相似度更高。

3 结束语

本文提出基于大语言模型的 ITAFm 算法,充分考虑外文军事文本的特点和翻译需求,通过构建评估指标,使模型能够更精确高效地翻译包含军事专业术语的文本。算法的精准性和高效性,在涉外军事研究和国际军事交流的翻译工作中有较大的实用价值,同时也可情报部门对敌情报分析提供有力支持。

参考文献

- 1 韩子满. 论军事文献中专有名词的翻译 [J]. 解放军外国语学院学报, 2009, 32 (2): 67-72.
- 2 叶佩, 王征风. 基于 OCR 识别的英语翻译系统设计 [J]. 自动化与仪器仪表, 2023 (2): 258-262.
- 3 冯国平, 曾祥滢. 基于属性概率权重的人工智能翻译文本特征分类算法 [J]. 自动化与仪器仪表, 2023 (11): 29-33.
- 4 BAN H, NING J. Design of English automatic translation system based on machine intelligent translation and secure internet of things [J]. Mobile information systems, 2021: 1-8.
- 5 贺婧. 基于多语料库关键词搜索的英汉自动翻译方法 [J]. 自动化与仪器仪表, 2023 (2): 170-175, 180.
- 6 NIKHIL K, DENG H, ADAM R, et al. Large Language Models Struggle to Learn Long-Tail Knowledge [C] //40th International Conference on Machine Learning. 2023: 4-7.
- 7 周忠良. 基于生成式人工智能的涉海翻译: 优势、挑战与前景 [J]. 中国海洋大学学报 (社会科学版), 2024 (2): 12-20. DOI: 10.16497/j.cnki.1672-335X.202402002.

- 8 VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need [J]. Advances in Neural Information Processing Systems, 2017, 30.
- 9 ZHESTIANKIN, BORIS, MARIA P. Zhestyatsky at SemEval-2021 Task 2: ReLU over Cosine Similarity for BERT Fine-tuning [C] //International Joint Conference on Natural Language Processing abs. 2021: 163-168.
- 10 陈家乐, 张艳玲. 计算机算法类资料的中英文智能翻译 [J]. 计算机技术与发展, 2021, 31 (7): 6. DOI: 10. 3969/j. issn. 1673 - 629X. 2021. 06. 029.

基于大语言模型的智能决策技术概览

王琪^{1,2*} 李雪飞^{1,2} 李婷婷¹ 王嘉康^{1,2} 徐勇军^{1,2}

摘要 大语言模型作为一种全新的智能决策方式,相比于传统的基于博弈论、启发式优化和知识的决策,其在通用性和人机交互智能性方面有着显著优势。尽管现有的基于强化学习的智能决策方式,在处理多智能体之间竞争合作决策问题时表现良好,但其在应对具有大规模离散动作和连续状态空间的复杂决策任务时,存在学习效率低下、模型可解释性差、泛化能力不足等问题。然而,大语言模型凭借其强大的语言理解和生成能力、跨任务知识迁移能力以及高效的数据利用等能力,能够准确理解决策任务问题背景、用户意图等相关信息,并在不同决策场景中共享底层特征表示,提高了学习效率和数据利用率,在复杂决策任务中表现出较强的适应性和泛化性,为实现人机协同的群体智能涌现提供了可能性。针对大语言模型时代下的决策范式转变,文章首先给出了现有决策技术研究现状,并探讨了国内外大语言模型的发展与现状,包括基于Transformer的Bert、T5和GPT系列大语言模型。然后,文章详细阐述了基于大语言模型的智能决策的技术路线、相关技术及主要挑战。最后,文章对基于大语言模型的智能决策进行了总结与展望。

关键词 大语言模型, 深度强化学习, 智能决策, 思维链技术, 微调技术, 通用人工智能

A Survey on Large Language Model based Intelligent Decision-Making

WANG Qi^{1,2*} LI Xue-Fei^{1,2} LI Ting-Ting¹ WANG Jia-Kang^{1,2} XU Yong-Jun^{1,2}

Abstract Large language models, as a novel intelligent decision-making approach, offer significant advantages in terms of versatility and human-computer interaction intelligence when compared to traditional decision-making methods relying on game theory, heuristic optimization, and knowledge. While current intelligent decision-making techniques based on reinforcement learning excel in addressing competitive and cooperative decision-making scenarios involving multiple agents, they encounter challenges when applied to complex decision-making tasks characterized by extensive discrete actions and continuous state spaces. These challenges include issues like subpar learning efficiency, limited model interpretability, and a lack of generalization capabilities. However, leveraging its robust language comprehension and generation capabilities, cross-task knowledge transfer, and efficient data utilization, large language models can precisely grasp the context of decision-making tasks, user intentions, and relevant information. By sharing foundational feature representations across diverse decision scenarios, large language models enhance learning efficiency, optimize data utilization, and demonstrate remarkable adaptability and generalization in intricate decision-making contexts. This capability opens up possibilities for the emergence of

* 通讯作者

1. 中国科学院计算技术研究所 2. 中国科学院大学

1. Institute of Computing Technology, Chinese Academy of Sciences 2. University of Chinese Academy of Sciences

swarm intelligence in human-machine collaboration. In light of the transformative impact of large language models on decision-making paradigms, this paper initially presents the current research landscape of existing decision-making technologies. It then delves into the evolution and status of large language models both domestically and internationally, focusing on prominent models like Bert, T5, and the GPT series based on Transformer architecture. Subsequently, the paper provides a detailed exploration of the technical roadmap, associated technologies, and primary challenges associated with intelligent decision-making utilizing large language models. Finally, the paper concludes with a summary and outlook on intelligent decision-making empowered by large language models.

Key words large language model, deep reinforcement learning, intelligent decision-making, chain of thought technology, fine-tuning technology, artificial general intelligence

1 研究背景与意义

智能决策^[1]是指个人或组织利用多种智能技术和工具,基于预定目标,对相关数据进行建模、分析并做出决策的过程。智能决策已经应用在很多领域中,包括文本-语音-视频生成^[2]、蛋白质结构预测^[3]等,以及机器人、工业医疗自动化和通用人工智能的研究。决策应用包括数学推理、常识推理、逻辑推理、多模态推理等思维链决策过程^[4]。智能决策不仅推动了各领域的智能化和自动化应用,还对通用人工智能^[5]、脑机接口和群体决策^[6]的研究具有重要意义,常用于复杂任务管理与调度、集群协调与规划、动态规划和设计。

传统决策技术主要包括基于博弈论^[7]、基于启发式优化^[8]以及基于知识^[9]的决策。这些传统技术在处理简单、线性的决策问题时比较有效,但在面对多维非线性的复杂决策空间存在一定局限性。随着人工智能技术的快速发展,以深度强化学习^[10]、大语言模型^[11]技术为代表的智能决策技术^[12]应运而生。尽管基于深度强化学习的智能决策技术在解决多智能体之间竞争合作决策问题时表现良好,但在处理大规模离散动作和连续状态空间的复杂

决策任务时,仍存在学习效率低下、模型可解释性差、泛化能力不足等问题。

近年来,深度神经网络和强化学习技术的不断演进,促进了大语言模型(Large Language Model, LLM)的迅速发展,推动了ChatGPT^[13]等大语言模型的产生。超级计算^[14]、大数据^[15]、预训练技术^[16]也为大语言模型的发展提供了良好的发展空间。大语言模型经历了统计语言模型、神经语言模型、预训练语言模型^[17]和LLM四代演化过程^[11]。通过持续的技术创新和优化,LLM在多任务学习、知识迁移以及复杂推理等方面取得了突破性进展,并凭借其强大的语言理解和生成能力、跨任务知识迁移能力以及高效的数据利用等能力,能够准确理解决策任务问题背景、用户意图等相关信息,并在不同决策场景中共享底层特征表示,提高了学习效率和数据利用率,在复杂决策任务中表现出较强的适应性和泛化性,为实现人机协同群体智能涌现和提升提供了更为强大和灵活的技术支持。

当前,基于大语言模型(LLM)的智能决策在民用和军用领域呈现出巨大的潜力。在民用领域,LLM的应用涵盖了工业控制中的机械臂精准抓取^[18]、自然语言处理中的文本生成、摘要提取和语言翻译等任务。此外,在医疗决策领域,LLM能够

辅助进行医疗问答和自动处方的生成，而在智能家居控制^[19]方面，LLM 则能够提供更加智能化和个性化的居住环境管理。在军用领域，LLM 在指挥控制方面同样发挥着重要作用，如可以提升军事用户的认知能力，使其能够更明智、更快地做出决策。另外，LLM 还能够拟制敌人难以预测的行动方案，为未来智能化战争无人集群决策对抗^[20]提供了新的策略工具。

本文针对大语言模型时代下的决策范式转变，全面概述了决策技术的研究现状，梳理了基于 LLM 的智能决策技术路线和相关技术，探讨了基于大语言模型

的智能决策面临的挑战及发展趋势，为智能决策技术进一步发展与应用提供了基础。

2 现有决策技术研究现状

现有决策技术根据技术发展路线可以分为传统决策技术和智能决策技术，如图 1 所示。传统决策技术主要包括基于博弈论^[7]的决策、基于启发式优化的决策以及基于知识的决策技术。智能决策技术主要包括基于深度强化学习的智能决策和基于大语言模型的智能决策技术。

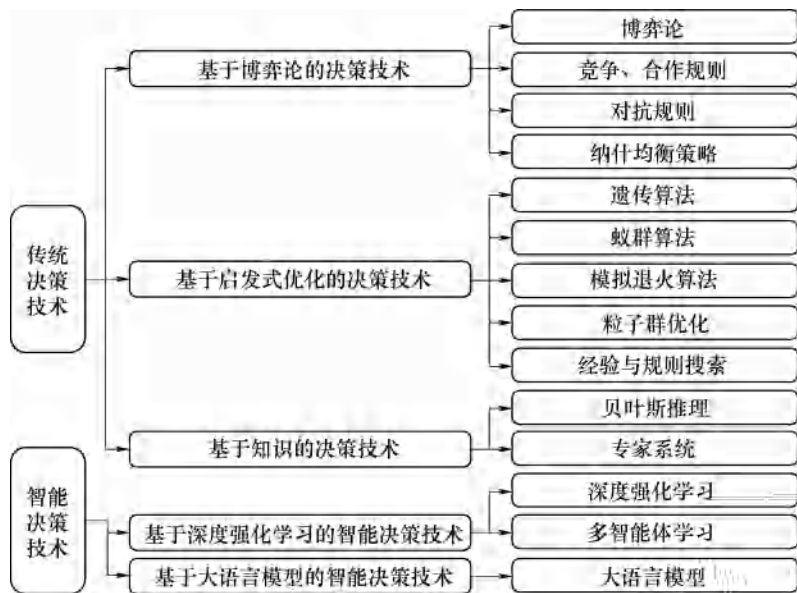


图 1 现有决策技术分类：传统决策技术和智能决策技术

基于博弈论的决策技术是指利用博弈论^[7]和具有竞争性质现象的数学理论方法，优化游戏中个体行为决策，并确定最佳对抗策略，通过博弈实体合作、竞争和激励等方式实现系统目标最优化决策。实体博弈过程在预定义对抗关系的基础上实现目标最优化，并达到纳什均衡和实现最优决策。但是基于博弈的决策技术一般仅

适用于离散且低维博弈环境中，并且需要人工辅助和利益均衡，在面对高维连续的博弈空间时，存储和计算成本庞大且难以维持。

基于启发式优化^[8]的决策技术是指基于启发式算法，如遗传算法、蚁群算法、模拟退火算法、粒子群优化等启发式优化算法，利用数据训练实现目标决策、策略

优化的决策技术。启发式算法是一类利用经验和规则的搜索算法，用于解决复杂的优化问题，具有较好的鲁棒性和全局搜索能力。基于启发式的决策算法能够在复杂环境下或时间受限情况下寻找最佳可行决策方案。然而，启发式优化算法容易陷入局部最优，且随着决策任务增多可能会面临维度灾难和计算复杂度高的问题。

基于知识的决策技术是指利用领域专家知识和经验、大数据提取和匹配、数据挖掘、数据分类和回归算法实现决策，如贝叶斯推理、专家系统。利用大数据提取实体关系和知识图谱实现问答和经验决定性决策，如基于专家系统的决策^[9]利用专家的经验实现推理决策。总体上基于知识的决策算法可以通过关联规则获得针对相应情况的最佳策略。然而，知识库的构建和维护增加成本和复杂性，知识库需要及时更新难以适应环境的变化。基于知识的决策技术一般用于离散状态空间决策，面对高动态、高维且连续的决策问题，决策算法的准确性和效果难以保障。

智能决策技术以深度强化学习和大语言模型技术为基础，具有一定的泛化性并能解决较复杂的决策优化问题。基于深度强化学习的决策技术，基于马尔可夫决策过程进行建模，能够用于高维状态空间 S 和高维连续动作空间 A 的映射选择上。目前，深度强化学习算法主要分为基于值函数的算法和基于策略梯度的算法。考虑在大部分决策场景中，智能体数量不唯一，因此衍生出了多智能体深度强化学习算法。

基于值函数的强化学习算法主要包括 Q -learning^[21] 和 SARSA^[22]，由于上述两种表格型的强化学习算法无法处理动作状态空间数量较大的情况，且无法泛化至未探索的状态上，因此，DQN^[23] 使用神经网络拟合值函数以解决这两种问题。Double

DQN^[24] 使用双神经网络解决 DQN 中过度估计值函数的问题，Dueling DQN^[25] 使用优势函数估计值函数，Rainbow^[26] 算法总结了六种 DQN 的变体，其组合显著提升了算法性能。与此同时，C51^[27] 算法、QR DQN^[28]、IQN^[29]、FQF^[30] 等值函数分布强化学习算法，将值函数估计为概率分布，以进一步获取准确的值估计。

然而，基于值函数的强化学习算法无法处理连续动作，因此，诞生出了直接学习策略的强化学习算法。REINFORCE^[31] 算法使用蒙特卡罗方法估计期望奖励，然而，其运行速度过于缓慢。Actor-Critic^[32] 算法通过时序差分方法以缩短训练时间，A3C^[33] 算法使用并行框架加速训练。DPG^[34] 算法学习确定性策略以降低方差并进一步提升样本效率，随后 DDPG^[35] 算法使用神经网络拟合值函数，TD3^[36] 限制了 DDPG 对值函数的过高估计以降低误差。SAC^[37] 算法结合最大熵原理以平衡探索和利用。PPO^[38] 算法引用置信域优化的思想，以限制策略的更新步长。

尽管基于深度强化学习的智能决策在性能上有了很大的提升，可是神经网络的可解释性需要进一步研究，深度强化学习算法的泛化性需要进一步提升，而 LLM 在复杂决策任务中表现出较强的适应性和泛化性，为实现人机协同群体智能涌现和提升提供了更为强大和灵活的技术支持。

3 大语言模型的发展与现状

本节深入探讨了 LLM 的发展与现状，首先回顾了 LLM 的起源，从早期的 Transformer 架构开始，逐步介绍了 Bert、T5 以及 GPT 系列等重要模型的发展，接着详细介绍了现有的主流国内外 LLM，并探讨了

基于 LLM 的任务决策研究现状。

3.1 大语言模型起源和发展历程

大语言模型的起源可追溯至 Transformer^[39]模型的提出，其架构如图 2 所示，将输入信息序列逐一编码，形成编码信息后再逐一输入解码器序列中，生成目标输出信息，编码器和解码器的结构如图 3 所示。Transformer 以其独特的多头注意力机制^[40]，有效处理序列数据，优化了编码器-解码器框架，从而在自然语言处理 (NLP) 领域引发一场变革，为后续 LLM 的发展奠定了基础。

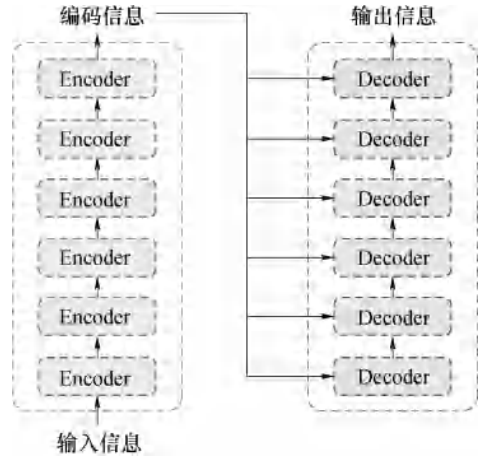


图 2 Transformer 的架构

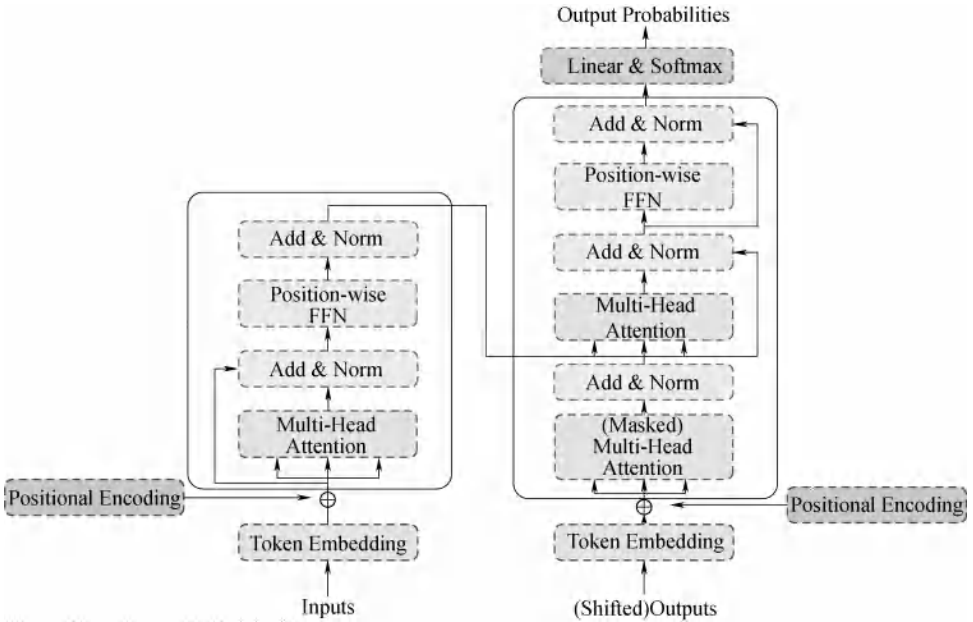


图 3 编码器 (Encoder, 左) 和解码器 (Decoder, 右) 的结构

继 Transformer 之后，Bert 模型的问世进一步推动了 LLM 的发展，模型结构如图 4 所示。Bert 通过其双向训练机制，显著提升了模型在语言理解方面的能力。其结构由多层 Transformer 堆叠而成，特别设计了“[CLS]”和“[SEP]”Token 来优化句子级别的表示，使其在遮蔽语言模型和下一

句预测任务上取得了突破性的性能^[17]。

GPT 系列模型则在 Bert 的基础上，进一步扩展了 LLM 的应用范围和深度。GPT-1 简化了 Transformer 的解码器结构，移除了一个多头注意力模块，如图 5 所示，以提高效率和性能，为后续更大规模的 GPT 模型铺平了道路。

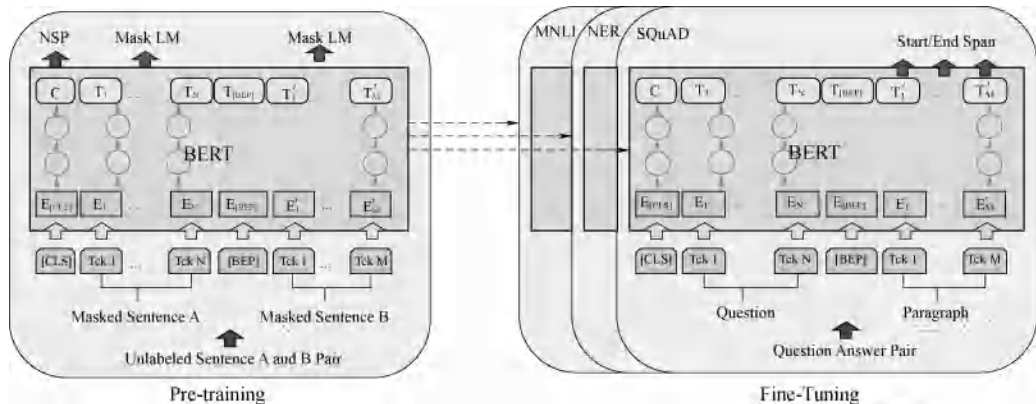


图 4 Bert 模型的预训练和微调过程

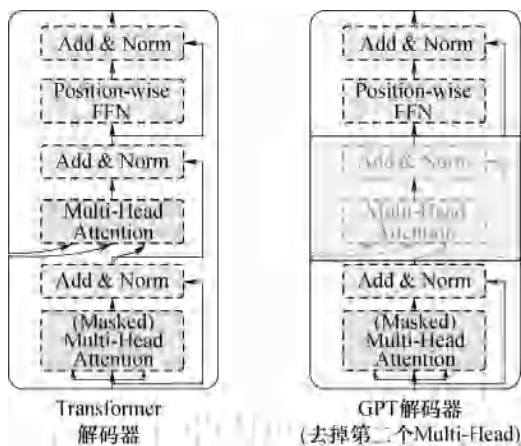


图 5 GPT 解码器的结构

T5 模型的提出，标志着 LLM 在任务泛化上迈出了重要一步。T5 将多种自然语言处理任务统一为文本-文本模式^[41]，通过在预训练和微调阶段使用一致的目标函数和解码策略，实现了对多样任务的灵活处理。T5 的创新之处在于其位置嵌入和 Normalize 操作，这些改进使得模型在特定任务上更加精准和高效。

总体来看，从 Transformer 到 Bert、GPT 系列，再到 T5，LLM 在理解、推理和生成方面的能力不断进化，此演进过程展示了 LLM 在模拟复杂语言现象和执行高级认知功能方面的潜力，为未来在智能决策、语言理解的深度和广度，以及自然语言生成的准

确性和可靠性方面提供了理论支撑。

3.2 大语言模型研究现状

3.2.1 国内外 LLM 研究现状

如表 1 所示，自 2018 年 OpenAI 发布具有 1.17 亿参数的 GPT-1 模型以来，人们见证了 LLM 的迅猛发展。如表 1 所示，国外的研究现状表明，OpenAI 的 GPT 系列^[13]模型不断刷新着参数规模的纪录，从 GPT-2 的 15 亿到 GPT-4 的 1.8 万亿参数，这些模型在多个任务上展现出了卓越的性能。与此同时，微软的 BingChat 和 Google 的 PaLM 也在聊天和通用领域取得了显著进展。特别值得一提的是，Meta 的 LLaMA 模型，以其 70 亿~700 亿不等的参数量，为 2024 年的研究树立了新的标杆。

转观国内，如表 2 所示，大语言模型的研究同样如火如荼。阿里云的通义千问^[42]、百度的文心一言^[43]等模型，不仅在参数规模上与国际接轨，更在开源社区中发挥着重要作用。智谱华章的智谱清言、百川智能的百川等模型，也体现了国内在闭源模型方面的研究力度。在特定领域，如法律、医疗、教育等，国内研究者也推出了 ChatLaw、灵心、桃李等专业模型，这些模型在各自领域内展现出强大的应用潜力。

表 1 国外大语言模型

LLM	机构	参数量	类别	时间	开/闭源
GPT-1	OpenAI	1.17 亿	通用	2018	开源
GPT-2	OpenAI	15 亿	通用	2019	开源
GPT-3	OpenAI	1750 亿	通用	2020	—
ChatGPT	OpenAI		通用	2022.11	—
GPT-4	OpenAI	1.8 万亿	通用	2023.3	—
BingChat	微软	1100 亿	聊天		—
PaLM2	Google	3400 亿	通用	2023.05.11	—
Claude	Anthropic		通用	2023.03	—
LLaMA-3	Meta	70 亿, 130 亿和 700 亿	通用	2024.04.19	开源

表 2 国内大语言模型

LLM	机构	参数量	类别	时间	开/闭源
通义千问	阿里云	720 亿	通用	2023.09.13	开源
文心一言	百度	2600 亿	通用	2023.03.16	开源
智谱清言	智谱华章	130 亿	通用	2023.08.31	—
百川	百川智能	超千亿	通用	2023.04.10	开源
书生	上海人工智能实验室	30 亿	通用	2023.11.17	开源
曹植	达观数据		工业	2023.07.08	—
Deepseek Coder	深度求索	670 亿	代码	2023.11.02	开源
星火	科大讯飞		通用	2023.05.06	开源
豆包	字节跳动	1300 亿	通用	2023.08.18	—
紫东·太初	中国科学院自动化研究所	千亿参数	通用	2023.06.16	开源
盘古	华为	2000 亿	工业	2023.07.06	开源
MOSS	复旦大学	160 亿	科研	2023.02.20	开源
悟道·天鹰	智源人工智能研究院	70 亿	通用	2023.06.09	开源
KnowLM	浙江大学 & OpenKG		通用		开源
混元	腾讯	万亿参数	通用	2023.09.07	开源
ChatLaw	北京大学信息工程学院	130 亿	法律	2023.07	开源
百聆 (BayLing)	中国科学院计算技术研究所		科研	2023.07.10	开源
灵心	华南理工大学未来技术学院		医学	2023.10.17	开源
致远	北京交通大学		交通	2023.07.19	开源
本草	哈尔滨工业大学		医疗	2024.04.12	开源
桃李	北京语言大学		教育	2023.08.21	—
Chat-UniVi	北京大学信息工程学院	130 亿	科研	2023.12.22	开源
问道	携程		文旅	2023.07.17	—

3.2.2 基于 LLM 的任务决策研究现状

LLM 通过上游预训练和下游任务对齐的训练模式，实现了能力激发和任务决策，并通过人类反馈的方式实现人类对齐，如图 6 所示。在上游预训练中，具有庞大参数规模的 LLM 利用大规模数据，完

成模型预训练，获得在通用任务上的决策能力；在下游任务中，通过相关任务数据集进行模型参数的微调，提高特定任务的决策能力。此外，LLM 也可以通过设计合适的提示词^[11]提升在下游任务中的决策性能。

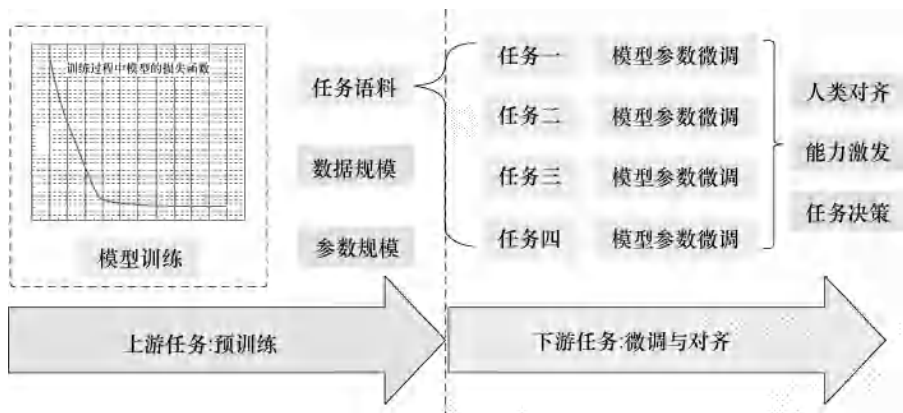


图 6 大语言模型的上游和下游任务

目前，现有的 LLM 在序列决策问题上显示出了巨大的潜力，并成功扩展到了任务决策领域。通过结合人类反馈对齐和强化学习技术，LLM 能够在复杂的决策场景中表现出色。在单任务序列决策中，LLM 的智能决策能力已经证明优于传统的强化学习算法和基于规则的人工智能系统，它们在智能性、可解释性和泛化能力方面都具有显著优势。

在智能决策的范式中，通常将问题视为从状态空间 S 到动作空间 A 的最优选择映射，即马尔可夫决策过程 (MDP)，它由状态空间、动作空间、奖励空间以及状态转移概率和奖励折扣因子定义。LLM 的智能决策过程可以根据部署模式分为集中式、分布式和复合范式。智能体基于任务触发的奖励、标签、目标和人工监督等进行决策驱动，完成给定状态下的动作选择。RL 利用累积奖励 (Q 值) 实现 a_t 的选择，计算方案如式 (1) 所示。

$$Q(a_{t+1} | s_{t+1}) = r_t + \gamma_{(s_t, a_t)} [Q_{\pi}(s_t, a_t)] \quad (1)$$

累积奖励 $Q(a_{t+1} | s_{t+1})$ 越大，则说明对应的动作 a_{t+1} 是当前状态 s_{t+1} 下的最优决策，相比于 RL 使用累积奖励进行最优决策，LLM 一般利用强大算力^[14]、庞大参数和数据规模实现最优决策。

此外，LLM 在多任务智能决策方面也展现出了其独特的优势。LLM 和强化学习可以同时扩展到多任务场景，其中每个任务的执行都会反馈一个奖励，从而实现多个智能体联合驱动的奖励决策。在这些多任务场景中，奖励反馈之间可能存在博弈竞争关系，包括完全竞争、完全合作、互相独立和互相联合等模式。强化学习可以实现多任务的联合决策，而 LLM 则可以通过并行处理实现多任务的独立决策。

综上所述，LLM 在任务决策领域的研

究现状表明, LLM 不仅在理论上具有强大的潜力, 而且在实际应用中也展现出了广泛的应用前景。随着技术的不断进步, LLM 有望在未来的决策智能化过程中发挥更加关键的作用。

4 大语言模型智能决策技术路线

LLM 在决策任务上拥有着巨大的潜力, 为了最大限度地激发 LLM 的决策能力, 设计一个合理的架构和使用相关的能力增强技术非常重要。本节依次描述 LLM

智能决策的结构和相关的决策能力增强技术。

4.1 LLM 智能决策的结构

LLM 智能决策的结构可分为记忆、规划、工具和动作四大模块, 如图 7 所示。记忆和规划模块可以让 LLM 拥有动态决策的能力, 利用长短期记忆和推理反馈等规划技术可以实现 LLM 智能决策。然而, 工具和动作模块可让 LLM 与环境进行交互, 更新环境状态并获得奖励反馈, 从而影响 LLM 的下一步决策。

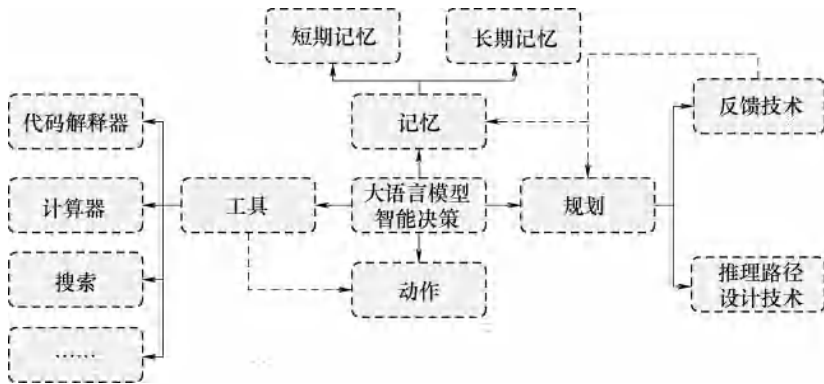


图 7 LLM 智能决策的结构

4.1.1 记忆模块

记忆模块中存储了 LLM 和环境交互的信息以及一些基础知识。通过记忆模块, LLM 能够不断成长, 自我提升, 从而进行更有效的决策。

记忆模块的结构设计参考了人类记忆过程, 人类记忆过程会通过短期记忆维持信息并通过长期记忆巩固信息, 所以 LLM 智能决策的记忆模块采用类似的结构, 使用上下文窗口内的输入信息模拟短期记忆, 通过外部向量存储技术模拟长期记忆, 短期记忆涉及的技术为上下文学习技术, 而长期记忆则涉及检索增强生成技术 (RAG)。通过这两种记忆结构的混合, LLM 可以在复杂的环境中进行高效的决策。

4.1.2 规划模块

LLM 智能决策的规划模块部分包括反馈技术和推理路径设计技术。

反馈技术中, *reflexion*^[44] 通过将任务反馈信号转化为反思数据, 并将其保存在长期记忆中以诱导后续决策, 持续提升 LLM 的决策能力; *self-refine*^[45] 则通过对任务结果的评估, 并将数据作为短期记忆再次输入 LLM, 不断改进决策。

推理路径设计技术指的是将复杂问题按照链式结构^[46]、树式结构^[47]或者图式结构进行分解。链式推理模仿人逐步思考的过程, 将任务分解为多个中间步骤, 每个步骤只导向一个后续步骤; 而树式结构和图式结构则参考人类发散思考的过程,

每个步骤可能会有多个后续步骤。

4.1.3 工具模块

工具模块的使用增强了 LLM 的动作能力，进而能够影响 LLM 的决策能力。相关的工具使用案例如下：WebGPT^[48] 会借助搜索引擎提取相关网页的内容并与 LLM 本身知识进行整合回答问题；TPTU^[49] 可以借助 python 解释器完成编程任务；vision agent^① 可以利用各种图像以及视频算法工具完成复杂任务决策。现有的大部分 LLM 已经开始在内部集成了工具调用的功能，使得工具的调用更加便捷。

4.1.4 动作模块

动作模块负责将 LLM 的决策指令转换为具体的动作。LLM 的动作来源于内部记忆存储的相关动作信息或者是 LLM 的显式动作规范，如工具模块可作为记忆相关的动作信息，而提示词中的具体动作要求可作为显示动作规范。在执行完动作后，环境状态会发生改变，通过将动作结果反馈给 LLM，LLM 可更新内部的记忆，从而优化后续决策，如 Re-Act^[50] 通过交替使用推理和行动完成复杂任务，PS^[51] 通过完整任务决策分解然后在执行动作的过程中不断修正的方式完成复杂任务决策。

4.2 相关的决策能力增强技术

4.2.1 微调技术

通过使用任务相关的数据集进行微调，LLM 对特定任务的决策能力能够得到极大提升。微调技术主要包括 Prefix Tuning、Prompt Tuning、P-Tuning、LoRA (Low-Rank Adaptation)、QLoRA、AdaLoRA、BitFit 等。Prefix Tuning 的技术原理是在输入 Token

之前构造一段任务相关的虚拟 Token 作为 Prefix，然后训练时只更新 Prefix 参数，而 LLM 中其他参数固定；P-Tuning 将 LSTM 作为提示编码器并随机初始化参数，在微调阶段只更新 LSTM 的参数；Prompt Tuning (P-Tuning v2) 初始化每个任务对应的参数矩阵，训练过程中 LLM 的参数被冻结，只有任务矩阵参数会被更新；LoRA 的核心思想是在 LLM 参数矩阵外增加旁路矩阵，只训练这一部分的参数。

4.2.2 思维链技术

思维链技术是指模仿人类思考的过程，通过提示让 LLM 学习这种思考模式，最终得到问题的答案，而思维树和思维图则是在思维链的基础上形成的机构变体，通过这些技术能够极大提高 LLM 在各种推理决策任务上的成功率，如图 8 所示。如 Few-Shot CoT 回答对应的问题前提供几个具体的问题，逐步解答过程让 LLM 去学习，从而提高 LLM 的推理能力；Zero-Shot CoT^[52] 使用提示词“Let’s think step by step”引导模型逐步思考；LTM prompting^[53] 让 LLM 将原来的问题分解为多个子问题，然后让 LLM 按顺序依次解决这些子问题，最后得到答案；Tot 将复杂问题解决过程建模树搜索结构，通过探索不同的路径来得到问题的最优解；而 Got 则是进一步将 LLM 生成的信息建模为图，提高 LLM 的决策能力。

5 基于 LLM 的智能决策主要挑战

5.1 高质量训练数据不足

大语言模型在上游训练中需要海量的语料来训练模型，下游指令微调时需要不

① <https://github.com/andrewyng/translation-agent>

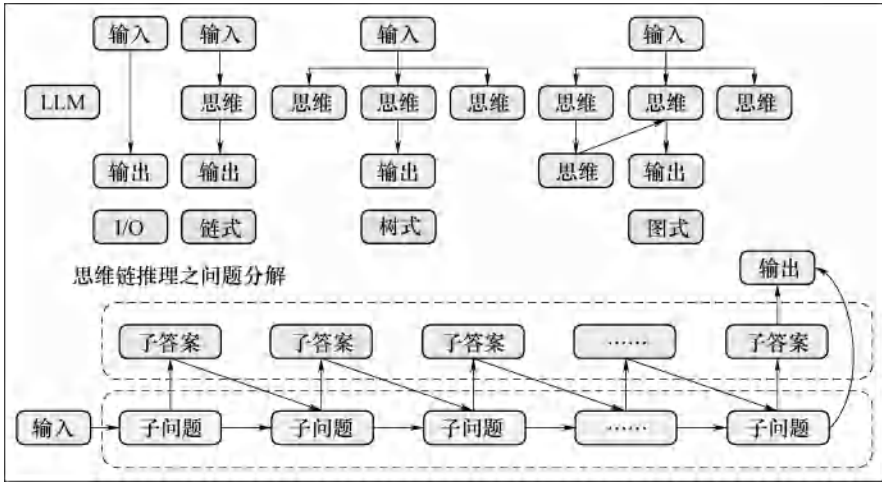


图 8 思维链复杂问题分解结构与过程

同的任务语料来进行参数微调。如 ChatGPT 的模型参数数量由亿级增长至千亿级，训练数据由 GB 增长至百 TB 级，并且由于信息壁垒和数据提取难的问题，多数模型训练数据呈现零散且杂乱的性质。LLM 需要的大数据多数情况下依靠人工逐条采集汇总，工作量巨大且准确性低。

目前，用于 LLM 任务推理训练的效果最好的中文 AI 训练数据集是“弱智吧”，用于推理决策的数据集目前难以构建。GPT 的训练数据主要来源于网页内容，包括维基百科、古腾堡书籍等，网络数据目前仍然是大语言模型海量任务语料的数据来源。因此，高质量的决策数据集不足是目前大语言模型训练的缺陷。

5.2 智能决策可解释性和机器幻觉问题

LLM 模型在决策过程和推理过程的可解释性和可信性尚待进一步优化。由于 LLM 缺乏足够的可解释性和可靠性，模型可能会出现机器幻觉问题，即向用户提供看似真实但完全错误甚至虚构的反馈内容，如 ChatGPT 有时提供的相关参考文献

是完全虚构的。这一生成式人工智能的缺点需要建立完善的评价体系，对于民用和军用领域是一个很大的挑战，要求在 LLM 输出基础上对模型不断进行调整和修正。

5.3 模型规模和计算资源庞大

LLM 的参数规模不断扩大，参数量基本达到百亿到千亿级别，如表 1 和表 2 所示。根据大语言模型的扩展发展，LLM 的扩展法则表明模型的参数和数据规模越大模型决策性能越好。然而，随着模型参数规模和数据规模的增长，引发了计算资源和算力资源的挑战。因此，如何实现高效准确的智能决策，同时均衡模型参数规模和数据规模，是需要解决的重要问题。

5.4 数据泄密和不良信息生成风险

LLM 的训练需要海量数据，可能包括敏感和隐私信息，而模型的输出取决于输入和训练数据，因此，可能生成隐私、敏感、暴力等不良信息。在数据隐私和生成信息方面，LLM 存在着数据泄露、不良生成信息等问题，特别是军用 LLM 模型训练数据，对模型训练数据安全和隐私有着更

高的要求。因此，基于 LLM 的智能决策需要建立严格的提示工程和敏感关键词检测机制，保护 LLM 的生成无隐私和敏感信息。

综上，针对上述大语言模型存在的一系列挑战，已有研究工作利用人类对齐、思维链和各种微调技术抑制 LLM 的机器幻觉问题和隐私泄露风险。另外，思维链技术^[46]和神经网络可解释性的研究有助于提高 LLM 的可解释性，促使与人类对齐并揭示了大语言模型的推理过程。此外，为了节省 LLM 对计算资源和算力资源的消耗，大语言模型可以通过修剪、蒸馏和量化、参数共享技术实现模型压缩，节省算力和存储资源。

6 结束语

本文概述了基于 LLM 的智能决策技术，并详细阐述了 LLM 的现状、智能决策现状、技术路线和研究挑战，包括 LLM 决策的记忆、规划、工具和动作，以及 LLM 在智能决策方面面临的多种挑战。基于 LLM 的智能决策技术发展和应用前景广阔，未来研究方向包括思维推理和任务分解的优化，结合文本、图像和音视频等多模态智能决策和个性化决策，模型可解释性与可信度增强，生成对抗攻击和防御策略，以提升模型在智能决策任务中的鲁棒性和安全性。

参考文献

- 1 张洪广, 杨林, 杨雄军, 等. 大模型驱动的智能辅助决策原理与典型应用 [J]. 指挥与控制学报, 2024, 19: 1-8.
- 2 YIN S, FU C, ZHAO S, et al. A Survey on Multimodal Large Language Models [J]. arXiv, 2024.
- 3 JUMPER J, EVANS R, PRITZEL A, et al. Highly Accurate Protein Structure Prediction with AlphaFold [J]. Nature 596, 2021, 7873: 583-589.
- 4 CHU Z, CHEN J, CHEN Q, et al. A Survey of Chain of Thought Reasoning: Advances, Frontiers and Future [J]. arXiv, 2023.
- 5 BUBECK S, CHANDRASEKARAN V, ELDAN R, et al. Sparks of Artificial General Intelligence: Early Experiments with GPT-4 [J]. arXiv, 2023.
- 6 WANG M, FU W, HE X, et al. A Survey on Large - Scale Machine Learning [J]. IEEE Transactions on Knowledge and Data Engineering, 2020, 1-1.
- 7 MA Z, WANG S, DENG X, et al. An Improved Approach for Adversarial Decision Making under Uncertainty Based on Simultaneous Game [C] // In 2018 Chinese Control And Decision Conference (CCDC). 2018: 2499-2503.
- 8 GIGERENZER G, GAISSMAIER W. Heuristic Decision Making [J]. Annual Review of Psychology, 2011, 1: 82-451.
- 9 KIREEVA N, POZDNYAK I, FILIPPOV N. Development of a Decision - Making Algorithm for Expert System in Information Security [C] // In 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 212-16. Kharkiv, Ukraine: IEEE, 2020.
- 10 WANG X, WANG S, LIANG X, et al. Deep Reinforcement Learning: A Survey [J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 1-15.
- 11 ZHAO W, ZHOU K, LI J, et al. A Survey of Large Language Models [J]. arXiv, 2023.
- 12 张振乾, 汪澍, 宋琦, 等. 人工智能大模型在智慧农业领域的应用 [J]. 智慧农业导刊, 2023, 3 (10): 9-12, 17.
- 13 刘学博, 户保田, 陈科海, 等. 大模型关键技术与未来发展方向: 从 ChatGPT 谈起 [J]. 中国科学基金, 2023, 37 (5): 758-766. DOI: 10.16262/j.cnki.1000-8217.20231026.004.
- 14 JIANG B, TANG Z, XIAO X, et al. Efficient and Automated Deployment Architecture for OpenStack in TianHe SuperComputing Environment [C] // IEEE Transactions on Parallel and Distributed Sys-

- tems. 2022; 1811–24.
- 15 CUZZOCREA A. Big Data Lakes: Models, Frameworks, and Techniques [C] //In 2021 IEEE International Conference on Big Data and Smart Computing (BigComp), 1–4. Jeju Island, Korea (South): IEEE, 2021.
 - 16 WANG L, EDDIE L K. Double PT: Enhancing Meta-Learning Performance with Pre-Train and Meta-Pre-Train Processes [C] //In 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI), 688–92. Atlanta, GA, USA: IEEE, 2023.
 - 17 DEVLIN J, CHANG M – W, LEE K, et al. BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding [J]. arXiv, 2019.
 - 18 LIAO J, ZHANG H, QIAN H, et al. Decision-Making in Robotic Grasping with Large Language Models [C] //In Intelligent Robotics and Applications. 2023.
 - 19 董正浩. AI大模型在智慧城市领域的应用与前景 [J]. 通信世界, 2023, 17: 39–40.
 - 20 WANG Q, LI T, XU Y, et al. How to prevent malicious use of intelligent unmanned swarms [J]. The Innovation, 2023, 4 (2).
 - 21 WATKINS C. Learning from delayed rewards [D]. PhD thesis, University of Cambridge England, 1989.
 - 22 ZOU S, XU T, LIANG Y. Finite-Sample Analysis for SARSA with Linear Function Approximation [J]. arXiv, 2019.
 - 23 MNIH V, KAVUKCUOGLU K, SILVER D, et al. Human-Level Control through Deep Reinforcement Learning [J]. Nature, 2015, 7540: 33–529.
 - 24 HASSELT H, GUEZ A, SILVER D. Deep Reinforcement Learning with Double Q – Learning [C] //Proceedings of the AAAI Conference on Artificial Intelligence. 2016.
 - 25 WANG Z, SCHAUL T, HESSEL M, et al. Dueling Network Architectures for Deep Reinforcement Learning [J]. arXiv, 2016.
 - 26 HESSEL M, MODAYIL J, HASSELT H, et al. Rainbow: Combining Improvements in Deep Reinforcement Learning [J]. arXiv, 2017.
 - 27 BELLEMARE M, DABNEY W, MUNOS R. A Distributional Perspective on Reinforcement Learning [J]. arXiv, 2017.
 - 28 DABNEY W, ROWLAND M, BELLEMARE M, et al. Distributional Reinforcement Learning with Quantile Regression [J]. arXiv, 2017.
 - 29 DABNEY W, OSTROVSKI G, SILVER D, et al. Implicit Quantile Networks for Distributional Reinforcement Learning [J]. arXiv, 2018.
 - 30 YANG D, ZHAO L, LIN Z, et al. Fully Parameterized Quantile Function for Distributional Reinforcement Learning [J]. arXiv, 2020.
 - 31 WILLIAMS R J. Simple Statistical Gradient-Following Algorithms for Connectionist Reinforcement Learning [J]. Mach Learn, 1992, 8: 229–256.
 - 32 SUTTON R S, MCALLESTER D, SINGH S, et al. Policy Gradient Methods for Reinforcement Learning with Function Approximation [J]. Advances in Neural Information Processing Systems, 2000, 12: 1057–1063.
 - 33 MNIH V, BADIA A, MIRZA M, et al. Asynchronous Methods for Deep Reinforcement Learning [J]. arXiv, 2016.
 - 34 SILVER D, LEVER G, HEES N. Deterministic Policy Gradient Algorithms [J]. arXiv, 2014.
 - 35 LILICRAP T, HUNT J, PRITZEL A, et al. Continuous Control with Deep Reinforcement Learning [J]. arXiv, 2019.
 - 36 FUJIMOTO S, HOOF H, MEGER D. Addressing Function Approximation Error in Actor – Critic Methods [J]. arXiv, 2018.
 - 37 HAARNOJA T, ZHOU A, ABBEEL P, et al. Soft Actor-Critic: Off-Policy Maximum Entropy Deep Reinforcement Learning with a Stochastic Actor [J]. arXiv, 2018.
 - 38 SCHULMAN J, WOLSKI F, DHARIWAL P, et al. Proximal Policy Optimization Algorithms [J]. arXiv, 2017.
 - 39 LIN T, WANG Y, LIU X, et al. A Survey of Transformers [J]. arXiv, 2021.
 - 40 VASWANI A, SHAZEER N, PARMAR N, et al. Attention Is All You Need [J]. arXiv, 2023.
 - 41 RAFFEL C, SHAZEER N, ROBERTS A, et al. Exploring the Limits of Transfer Learning with a

- Unified Text-to-Text Transformer [J]. arXiv, 2023.
- 42 BAI J, BAI S, YANG S, et al. Qwen-VL: A Versatile Vision-Language Model for Understanding, Localization, Text Reading, and Beyond [J]. arXiv, 2023.
- 43 SUN Y, WANG S, FENG S, et al. ERNIE 3.0: Large-Scale Knowledge Enhanced Pre-Training for Language Understanding and Generation [J]. arXiv, 2021.
- 44 SHINN N, CASSANO F, BERMAN E. Reflexion: Language Agents with Verbal Reinforcement Learning [J]. arXiv, 2023.
- 45 MADAAN A, TANDON N, GUPTA P, et al. Self-Refine: Iterative Refinement with Self-Feedback [J]. arXiv, 2023.
- 46 WEI J, WANG X, SCHUURMANS D, et al. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models [J]. arXiv, 2023.
- 47 YAO S, YU D, ZHAO J, et al. Tree of Thoughts: Deliberate Problem Solving with Large Language Models [J]. arXiv, 2023.
- 48 NAKANO R, HILTON J, BALAJI S, et al. WebGPT: Browser-Assisted Question-Answering with Human Feedback [J]. arXiv, 2022.
- 49 RUAN J, CHEN Y, ZHANG B, et al. TPTU: Large Language Model-Based AI Agents for Task Planning and Tool Usage [J]. arXiv, 2023.
- 50 YAO S, ZHAO J, YU D, et al. ReAct: Synergizing Reasoning and Acting in Language Models [J]. arXiv, 2023.
- 51 WANG L, XU W, LAN Y, et al. Plan-and-Solve Prompting: Improving Zero-Shot Chain-of-Thought Reasoning by Large Language Models [J]. arXiv, 2023.
- 52 KOJIMA T, GU S, REID M, et al. Large Language Models Are Zero-Shot Reasoners [J]. arXiv, 2023.
- 53 ZHOU D, SCHÄRLI N, HOU L, et al. Least-to-Most Prompting Enables Complex Reasoning in Large Language Models [J]. arXiv, 2023.

基于大语言模型的作战辅助决策 智能体框架设计

李凯^{1,2} 王瑞^{1,2} 许霄¹ 郭圣明¹ 陶九阳¹

摘要 随着大语言模型 (Large Language Models, LLMs) 在自然语言处理任务方面的巨大突破, 越来越多的研究者尝试在复杂任务处理方面开展技术探索, 特别是兵棋推演过程中, 如何基于大语言模型辅助指挥员有效提升指挥控制能力成为亟须探索和解决的问题。针对这一挑战, 文章构建了基于大语言模型驱动的作战辅助决策智能体框架, 设计了面向兵棋推演的智能体基础组件, 并结合典型应用场景, 探索了智能体在作战辅助决策中的总体架构、记忆存储、任务规划及工具调用的实现思路和方法, 为基于大模型的自适应作战辅助决策提供了技术指导 and 可行方案。

关键词 大语言模型, 智能体, 兵棋推演, 作战辅助决策

Assistant Decision-Making Agent Framework Based on Large Language Models

LI Kai^{1,2} WANG Rui^{1,2} XU Xiao¹ GUO Sheng-Ming¹ TAO Jiu-Yang¹

Abstract With the significant breakthrough of Large Language Models (LLMs) in natural language processing, more and more researchers are attempting to explore technology in complex task processing, especially during the war game. How to effectively improve command and control capabilities based on LLMs has become an urgent issue that needs to be explored and solved. In response to this challenge, this article constructs a framework for combat decision-making intelligent agents driven by large language models, designs basic components of intelligent agents for war game, and explores the overall architecture, memory storage, task planning, and tool invocation of intelligent agents in assisting combat decision-making in typical application scenarios. This provides technical guidance and feasible solutions for adaptive combat auxiliary decision-making based on large models.

Key words large language models, agent, war game simulations, combat auxiliary decision-making

0 引言

随着 2022 年底 OpenAI 开发的基于大

模型的 ChatGPT 聊天机器人程序震撼上线, 大语言模型技术迅速“席卷”了整个社会, 人工智能技术因此迎来了一次重要进展, 其在智能问答、机器翻译、代码生

1. 智能博弈重点实验室 2. 中国科学院软件研究所

1. State Key Laboratory of Intelligent Game 2. National Key Laboratory of Space Integrated Information System, Institute of Software Chinese Academy of Sciences

成、文本分类等多种场景中的广泛应用使其备受欢迎。随后开展的各项工稳步推动了大模型的快速发展，并取得了显著成就。2023年3月，OpenAI推出了标志性的GPT-4模型，将模型能力提升至全新高度，并将其扩展至拥有多模态功能的GPT-4V模型。2024年5月，OpenAI发布了多语言、多模态GPT-4o，作为GPT系列最新的旗舰型号，它提供GPT-4级别的智能服务，但速度更快，并改进了其跨文本、语音和视觉的功能。

大模型的成功源于其在大规模未标注数据集上进行预训练，并通过微调、上下文学习等方式适配各种下游任务，从而实现最佳性能。由于大模型在自然语言处理任务方面表现出来的强大的能力，越来越多的研究学者对大模型在开放世界中进行环境感知、决策及执行动作等方面的能力产生了极大的兴趣，即以基础大模型作为智能应用技术的内核，以自主智能体作为载体与动态环境开展交互。特别是兵棋推演领域，如何通过大模型辅助指挥员提升作战指挥控制能力。

兵棋推演（Wargaming）作为一种模拟战争或军事冲突的工具和方法，通过在接近真实模拟环境中进行战役和战术操作，能够辅助开展任务规划、方案验证和计划执行等指挥控制活动。

针对兵棋推演的基本要素、运用特点及主要研究难点，国防大学胡晓峰教授等^[1]全面综述了以AlphaGo^[2]为代表的智能技术在兵棋推演领域潜在探索方向，并给出了态势理解与自主决策可行的技术路径。和当前兵棋推演关注的重点不同，本文关注的是兵棋推演中的智能体技术研究，旨在探索基于大语言模型，构建兵棋推演仿真环境下的作战辅助决策智能体框架，设计智能体自适应作战决策控制的关

键组件及运行机制，从而实现动态变化战场环境中的作战实体或作战编组的任务生成与决策控制执行，并结合典型应用场景，开展潜在用途和应用能力分析。

1 从大模型迈向智能体

1.1 大模型概述

构建基于大模型的智能体，首先需要剖析大模型的基本概念、技术架构及能力特点。大模型是指包含数千亿（或更多）参数的Transformer^[3]语言模型，这些大模型在大规模文本数据上进行训练^[4]，如GPT-3^[5]、PaLM^[6]和LLaMA^[7]。目前大模型主要建立在Transformer架构上，与小型语言模型有相同的预训练目标（如语言建模），然而大模型大幅扩展了模型规模、数据规模和总计算量。大量研究表明，当规模达到一定水平时，性能显著提高，这也是大模型区别传统语言模型的最显著特征，文献[8]将这种特征定义为大模型的“涌现能力”，即小型模型中不存在但在大型模型中产生的能力。GPT-3可以通过“上下文学习”的方式来利用少样本数据解决下游任务，而GPT-2则不具备这一能力。最新的语言模型（如GPT-4）则侧重于复杂任务的求解，通过预测下一个词元的预训练任务进行学习，虽然并没有针对特定的下游任务进行优化，却能够建立远强于传统模型的通用任务求解能力。除了涌现能力与复杂任务求解能力外，大模型在跨领域知识储备、复杂任务推理、人类指令对齐及工具使用等方面均表现出前所未有的能力。

由于大模型在逻辑推理及复杂任务分析方面取得了巨大进步，越来越多的研究工作开始探索将大模型作为智能体的核心

组件，以提高智能体在开放领域和动态环境中的性能。

1.2 智能体概述

随着基于深度强化学习技术的AlphaGo、AlphaStar^[9]等智能体（Agent）分别在围棋、星际争霸等游戏环境中战胜人类顶尖职业选手，智能体的概念获得了重大关注，但智能体并不是一个新兴的概念。Agent^[10]的概念由马文·闵斯基（Minsky）在其1986年出版的《思维的社会》一书中提出，作者认为社会中的某些个体经过协商之后可求得问题的解，这些个体就是Agent，Agent应具有社会交互性和智能性。斯图尔特·罗素（Russell）^[11]在其经典教材 *Artificial Intelligence: A Modern Approach* 中指出，智能体是一个具备环境感知、决策制定及动作执行能力的

自主算法系统。迈克尔·沃德里奇（Wolrdridge）^[12]认为智能体是指具有自主性、社会性、反应性和能动性等基本特性的计算机硬件或软件。

智能体技术与人工智能技术的发展类似，经历了基于符号规则^[13]的智能体时期，基于深度强化学习的智能体时期，发展到了以大模型为内核的智能体时期。基于符号规则的智能体通过专家预定义好的规则逻辑，在特定场景中模拟人类完成相应任务，如基于行为树框架构建知识规则智能体，能够分别设置逻辑节点的运行机制和动作节点的处置规则，实现有限状态空间中的决策知识嵌入，能够较好完成相应任务。但受限于规则的数量和质量，基于符号规则的智能体往往无法应对未经历的场景，其适应性和灵活性较差，如图1所示。

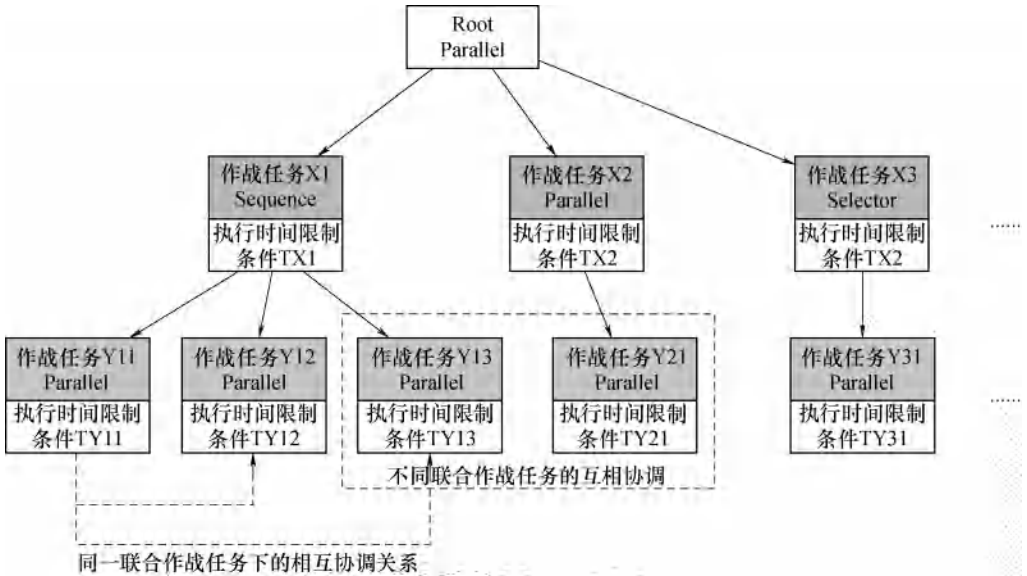


图1 基于符号规则的智能体

随着机器学习技术的发展，以深度强化学习为代表的智能体扮演了重要角色。深度强化学习智能体旨在与环境进行交互，收集状态、动作与奖赏等序列数据进

行训练学习最佳策略，通过探索和利用机制，不断试错并根据环境反馈信息优化调整自身策略，从而最大化奖励，实现预期目标^[14]。虽然深度强化学习智能体能有效

应对复杂多变的博弈对抗环境，并做出高效决策，但基于深度强化学习的智能体可解释性较弱，并且难以在场景变化的情况下实现模型的迁移，如图 2 所示。

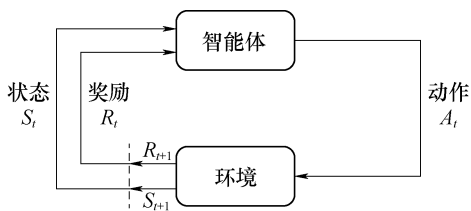


图 2 基于强化学习的智能体

1.3 大模型智能体

不同于传统的智能体技术，基于大语言模型的智能体具备通过独立思考、调用工具去逐步完成给定目标的能力。大模型驱动的智能体能够利用自身所具备的深度理解和生成能力，来执行复杂任务，可以

在无须大量特定领域数据的情况下，经过多轮迭代实现规划和执行动作，快速适应并胜任新的任务，以达到预期作战目标。

智能体根据用户设定的目标，确定好需要履行特定角色，自主观测感知环境，根据获得的环境状态信息，检索历史记忆以及相关知识，通过推理规划分解任务并确定行动策略，并反馈作用于环境，以达成目标。在这个过程中，智能体能够持续学习，像人类一样不断进化。基于大语言模型来构建一个智能体，充分地利用大语言模型的内生能力来驱动不同的组成单元。如图 3 所示，在作战仿真推演环境中，基于大模型的智能体能够辅助指挥员开展作战指挥控制活动，通过自然语言与场景中的作战实体单元或作战编组进行指令传达，实现任务规划和作战控制等智能决策应用。

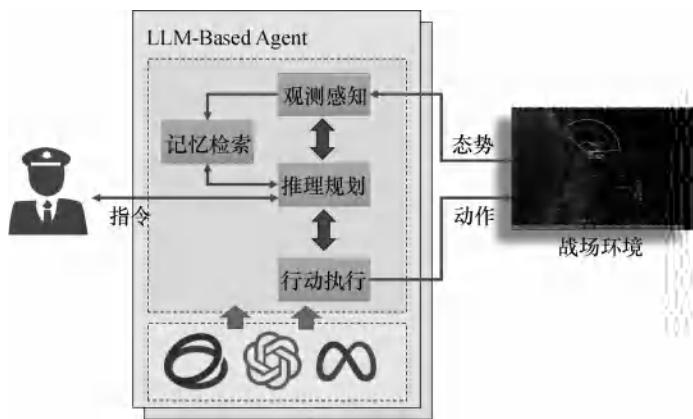


图 3 基于 LLM 的智能体作战决策应用

具体而言，智能体的一个典型的工作流程包括接收用户指令、环境感知、动态环境交互及行动执行等主要流程，并且在智能体运行的不同阶段，基于大型语言模型的智能体通过上下文学习和思维链提示方法与大型语言模型交互，获取必要的资源数据和决策结果。详细过程如下：

接收用户指令：智能体获取用户指令，分析需要扮演的角色，并对任务进行初步分解，形成子任务。

环境感知：智能体观测并感知环境状态，根据需要从历史记忆和知识储备中检索相关信息。

动态环境交互：智能体置身于动态环

境中，回顾过去的行为，通过推理分析任务，规划未来的动作并确定执行策略。

行动执行：行动执行模块将智能体的决策转化为对环境的具体输出，控制并影响环境的未来状态，以完成用户设定的目标。

2 自适应作战决策智能体框架设计

开展基于大语言模型的作战决策技术研究，应该抓准兵棋推演的主要作战流程、任务需求及运行机制，明确人与机器的关系、智能体与仿真平台的关系及决策信息流转路径等内容。基于以上考虑，本章给出了基于大语言模型的作战辅助决策框架。

基于大语言模型的作战辅助决策框架如图4所示，主要以联合作战仿真推演系统为例说明智能体执行作战计划的完整作战决策过程。

作战计划执行。基于大语言模型的智能体加载作战计划，并基于联合作战仿真推演系统开展作战控制，联合作战计划推演控制引擎基于时间及分支条件有序开展作战任务的执行，并基于专业的战术任务智能体集，形成兵棋指令组，驱动联合作战仿真推演系统开展实体装备行动控制。其中，基于大模型驱动的智能体针对接收的作战任务需求，需要开展模型选择，调用指定类型的战术任务智能体。需要指出的是，战术任务智能体的实现不依赖于大语言模型，其面向典型作战场景，控制己方作战兵力及装备设施，采用传统的知识规则方法或者深度强化学习实现即可。战术任务智能体的执行依赖作战推演系统推送的实时态势数据及基础想定数据，部分战术任务智能体考虑记忆模块存储的历史数据。

智能态势认知。智能体在执行作战计

划过程中，需要自主实时开展智能态势认知，监控作战任务清单，发现任务执行过程中的潜在风险因素。一方面，基于智能体的反思机制，可以定时获取战术任务智能体相关的兵力资源、弹药消耗、事件报告及任务状态等基础信息；另一方面，需要开展面向任务清单的智能态势风险监控评估，能够基于任务清单数据，大语言智能体自主开展模型选择，选择合适的风险监控评估模型，分析任务执行过程中潜在的硬毁伤及软毁伤风险。

辅助动态调控。辅助动态调控基于当前任务执行反馈及智能态势认知反馈基础上，智能体统筹形成标准化的辅助动态调控任务需求，自主开展任务分解，面向应急处置及临机调控两类模型工具，开展模型选择、模型执行及结果反馈。

智能体基于以上三个主要步骤进行循环迭代，实现在兵棋推演系统中的自适应作战决策。除此之外，为了支持人机混合编组下的作战辅助决策，引入了作战决策AI助手，采用提示模板的多模态数据规范，主动下达作战任务需求。并且基于作战决策任务及反馈结果，对齐 Prompt 中数据格式，支持指挥员查看、编辑和调整作战任务和执行结果，从而提升大语言模型智能体下一轮任务规划过程中的作战决策性能。

3 基于兵棋推演的智能体基础组件

完成基于大语言模型的作战辅助决策框架设计基础上，本节面向兵棋推演的作战决策场景，开展智能体基础组件的构建。如图5所示，主要包含记忆组件、规划组件及执行组件（工具）。

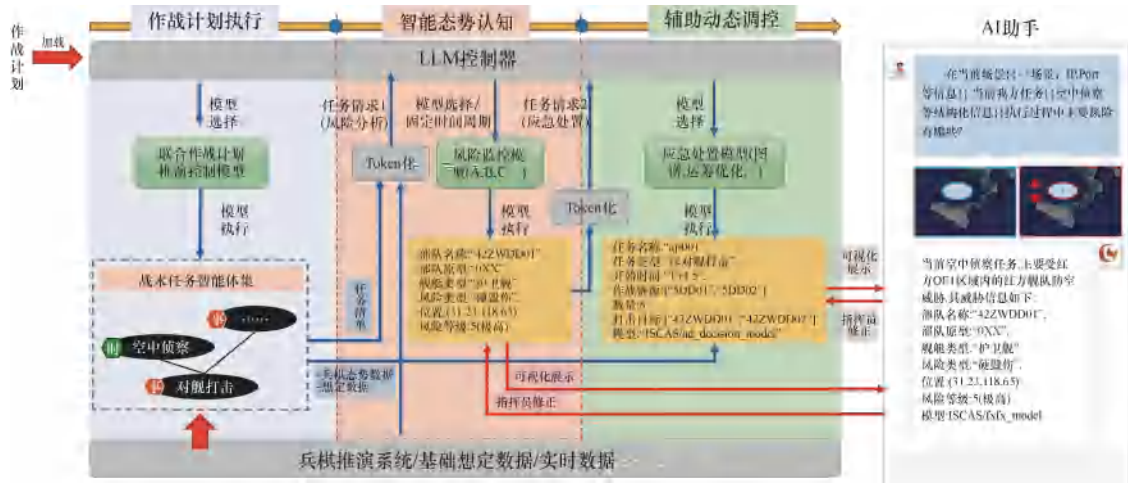


图4 基于LLM的作战决策框架示意图

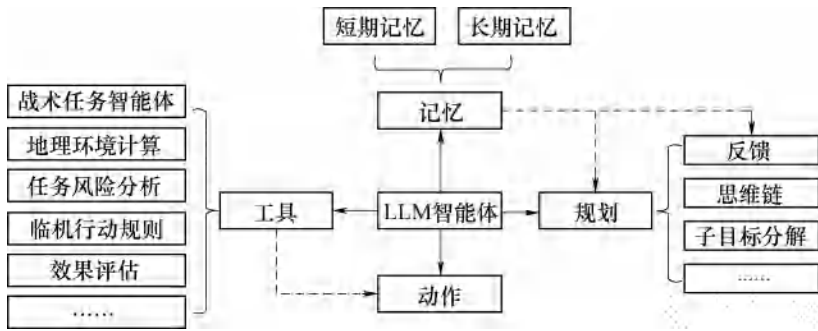


图5 基于LLM的智能体核心组件

3.1 记忆组件

记忆组件作为智能体架构的重要组成部分，直接影响作战决策的效率和准确性。记忆组件包含短期记忆和长期记忆，采用特定对象列表组成，对象由仿真推演过程数据转换而来，包括实时态势信息、历史态势信息、战场环境数据、事件数据及报告数据。其中实时态势信息及历史态势信息包含作战实体信息、武器装备信息及作战统计信息，战场环境数据记录地理位置、天气气象等公共环境数据，战场情况数据及报告数据主要记录与任务指令相关的作战数据，包括任务执行日志、战损

战果报告数据。

在记忆组件中，为了从智能体历史经验数据中提取有效观测值，可以构建检索模块，实现关键节点检索，包括历史枢纽态势和关联态势。枢纽态势对后续决策产生重大影响，关联态势能够记录序列数据，提升智能体序贯决策能力。

为了构建规范可读性较强的提示数据，分析态势数据结构特点，提取关键要素信息，设计带插槽机制的标准自然语言模板，实现数据的快速转换，生成符合作战决策需求的观测数据，如图6所示。

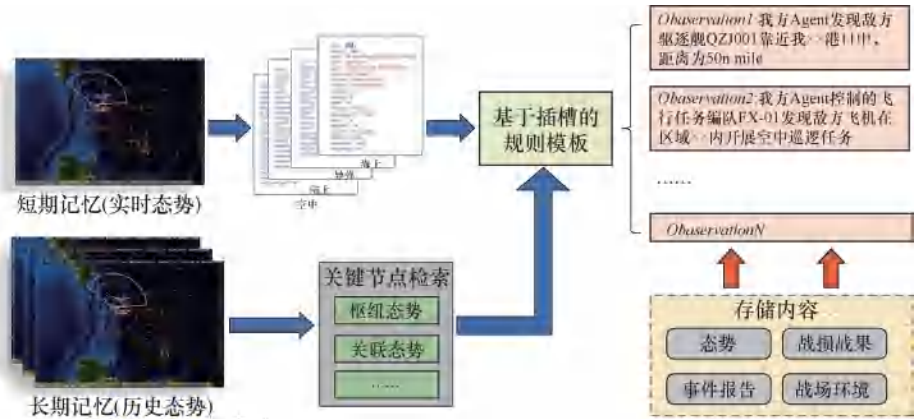


图 6 兵棋推演环境记忆组件设计

3.2 规划组件

规划组件为智能体引入了类似于人类解决任务的思考方式，将复杂任务分解为一系列简单易于管理的子任务，并为每一个子任务完成制订适当的计划。这种方法降低了一次性解决任务的难度，有助于提高问题解决的效率和效果，增强智能体对

复杂环境的适应能力和操作的可靠性。

兵棋推演过程中，人作为作战决策的主体，担当下达任务需求及执行智能体策略的重要角色，本文设计了先计划再执行的任务分解逻辑，采用内外循环结构，外循环负责任务规划，内循环作为执行工具，专注于处理分解的子任务，如图 7 所示。

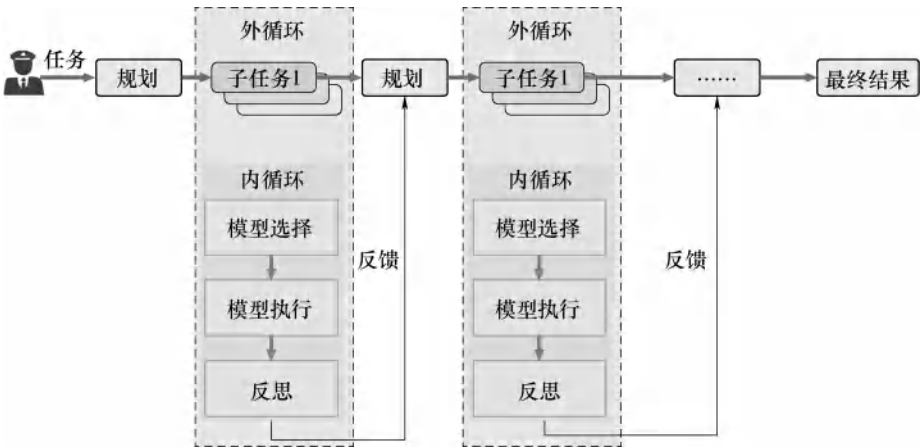


图 7 基于内外循环的任务规划机制

基于大语言模型开展任务分解，可以采用 Prompt 提示工程将任务描述和示范以自然语言文本形式输入给大模型，引导大语言模型生成针对具体任务的规划结果。

通过上下文学习机制，基于任务示范，大模型能够在没有显式梯度更新的情况下识别和执行新任务。

针对复杂的作战任务需求，分解生成

的子任务需要考虑工具调用的标准数据规范。一方面，智能体能够根据子任务的属性信息完成工具的选择，并能够将相应的任务参数输入给工具中，实现工具的执行；另一方面，需要明确任务间的依赖关系，子任务的执行往往依赖前置任务执行的结果。本文设计的子任务基本属性包含任务 ID、任务类型、任务依赖、任务参数及任务执行结果，如表 1 所示。

表 1 子任务属性

任务属性	符号表示	属性描述
任务 ID	Task_id	任务唯一标识符
任务类型	Task_type	任务类型，对应态势认知、决策规划及控制执行等不同模型工具类
任务依赖	Task_dep	依赖的前置任务，只有前置任务执行，才能执行当前任务
任务参数	Task_arg	任务执行需要的参数，输入给工具
任务执行结果	Task_res	工具执行反馈的结果

以联合制空推演场景为例，指挥官输入某区域制空权争夺的任务需求，大语言模型驱动的智能体基于提示工程开展任务规划，分解的子任务分别为区域飞行任务评估及制空作战任务，两个子任务详细参数如图 8 所示，以制空权争夺子任务为例，可以发现任务依赖“dep”参数列表包含数值 0，即表示该任务的执行依赖前一个任务的完成，即智能体认为开展制空作战，首先需要评估区域内敌我双方飞行任务编队的制空能力，通过区域飞行任务评估结果的反馈，为制空作战任务提供情报数据支撑，从而显著提升制空作战任务执行效果。

在应对复杂任务时，智能体还可以根据环境的实时反馈进行迭代优化，从而更高效地解决涉及复杂推理的问题。比如，在任务开始时，智能体根据长短期记忆和环境制订初步规划，并在每一步行动前根据新接收到的信息对当前规划进行细致调整，确保其行为的合理性。



图 8 子任务分解示例

3.3 执行组件

执行组件是智能体区别于大语言模型的一个重要组成部分，它的主要职责是执

行由规划组件分解的任务解决方案，即规划组件中内循环部分具体与环境进行交互的动作行为，并获得实际的执行效果反馈。具体来说，智能体会在行动决策过程

中执行规划组件制订的明确行动规划，同时会参考记忆组件中的长短期记忆来帮助执行准确的行动。

基于兵棋推演的作战决策亟须专业性较强的执行组件支撑，包括情报信息获取、态势智能认知、自主规划控制及作战效果评估 OODA 环四个阶段的应用服务需求。本文在执行组件层面，采用外部工具的方式提升智能体任务执行能力，外部工具主要包含战术任务执行智能体、任务风险评估模型、临机动态调控模型、态势优

劣评估模型及作战效果评估模型五类专业性较强的模型服务。通过引入外部工具，可以有效弥补基于大语言模型的智能体在垂直领域有限的专业知识，增强其专业性和适应性。

为了有效提升任务执行的外部工具支撑能力，本文设计了可扩展的外部工具模型库，构建了统一标准化的接口规范，包括模型输入结构和输出结果反馈，如表 2 所示，展示了作战决策过程中外部工具模型的部分示例数据。

表 2 外部工具库示例

任务	参数	候选模型集	描述
目标威胁评估	<pre>{ "ip": "192.168.1.26", "ai_port": 30006, "sdb_info": { "db_port": 30009, "user": "zkr", "passwd": "123" }, "resource": ["12WD01", ...], ... }</pre>	[ISCAS/fx, SU/fx, ...]	<pre>["能够实现对敌方实体列表进行威胁评估分析，支持 python 语言，基于 AI 接口采用 CNN 实现", ...]</pre>
联合制空行动推荐	<pre>{ "area": "A 岛北部区域", "star_time": t1, "end_time": t2, "resource_stric": {"歼击机": 20%} }</pre>	[ISCAS/zk, SU/zk, ...]	<pre>["运用运筹优化方法，开展联合制空行动规划，求解近似解，快速生成子任务序列，采用 python 语言", ...]</pre>

在工具调用机制方面，主要采用任务类型过滤模型库的选择范围，并基于模型的历史标签、历史调用频率和模型描述信息进行排序。工具调用反馈的结果一般为结构化的数据，为了较好地融合规划的任务列表、任务选中的模型和模型的推理结果，需要将过程数据及结果数据以结构化的格式发送给智能体，智能体再以自然语言形式返回。

4 结束语

本文面向联合作战兵棋推演应用场景，分析了大模型的能力特征，总结概括了智能体的概念及技术发展历程，并着重介绍了大模型驱动的智能体在作战辅助决策方面的应用模式。在此基础上，本文构建了基于大语言模型的作战辅助决策框架

及基于兵棋推演的智能体基础组件，为基于大模型的自适应作战决策的发展提供了技术引导和总体框架设计。

参考文献

- 1 HU X, HE X, TAO J. AlphaGo's breakthrough and challenges of wargaming [J]. *Science & Technology Review*, 2017, 35 (21): 49-60.
- 2 SILVER D, HUANG A, MADDISON C, et al. Mastering the game of Go with deep neural networks and tree search [J]. *Nature*, 2016, 529: 484-489.
- 3 VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need [C] //in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4 - 9, 2017, Long Beach, CA, USA*. 2017.
- 4 SHANAHAN M. Talking about large language models [J]. *CoRR*, vol. abs/2212. 03551, 2022.
- 5 BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners [C] //in *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems*. 2020.
- 6 CHOWDHERY A, NARANG S, DEVLIN J, et al. Palm: Scaling language modeling with pathways [J]. *CoRR*, vol. abs/2204. 02311, 2022.
- 7 TOUVRON H, LAVRIL T, IZACARD G, et al. Llama: Open and efficient foundation language models [J]. *CoRR*, 2023.
- 8 WEI J, TAY Y, BOMMASANI R, et al. Emergent abilities of large language models [J]. *CoRR*, vol. abs/2206. 07682, 2022.
- 9 VINYALS O, BABUSCHKIN I, CZARNECKI W, et al. Grandmaster level in StarCraft II using multi-agent reinforcement learning [J]. *Nature*, 2019, 575 (7782): 350-354.
- 10 MINSKY M. *The Society of Mind* [J]. Simon & Schuster, 1986.
- 11 Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach (4th Edition)* [J]. Pearson, 2020.
- 12 WOOLDRIDGE M, JENNINGS N R. Intelligent agents: Theory and practice [J]. *The Knowledge Engineering Review*, 1995, 10 (2), 115-152.
- 13 DIETRICH J. Rule-based agents for the semantic web [C] //In: *Electronic Commerce Research and Applications*. 2003.
- 14 LUCIAN B, ROBERT B, BART D. A Comprehensive Survey of Multiagent Reinforcement Learning [C] //In: *IEEE Transactions on SMC*. 2008.

基于多模态大模型的态势认知方法与应用

武霞^{1*} 王元斌¹ 李鼎¹ 王振杰¹ 高子文¹

摘要 为应对战场态势的复杂性及单一模态信息的局限性，提出一种基于多模态大模型的态势认知方法，并应用于海上战场态势认知。该方法利用计算机视觉、自然语言处理、大模型等技术，有效融合文本、图像和时序多模态信息。通过模型预训练和指令微调，高效完成目标识别、威胁判断等简单态势认知任务，并构建态势库。基于态势库，模型能够进一步实现战场态势评估等综合态势认知任务，为军事指挥决策提供全面准确的态势信息支持和决策依据。

关键词 态势认知，多模态大模型，指令微调，模型预训练

Situation Awareness Method and Application Based on Multi-modal Large Model

WU Xia^{1*} WANG Yuan-Bin¹ LI Ding¹ WANG Zhen-Jie¹ GAO Zi-Wen¹

Abstract To address the complexity of battlefield situations and limitations of single modal information, a multi-modal large model-based situation awareness method for maritime environments is proposed. This method leverages computer vision, natural language processing, and large models to integrate text, image, and time series data. Through pre-training and instructional fine-tuning, it efficiently performs simple tasks like target identification and threat assessment, building a situation library. Utilizing this library, the model further accomplishes comprehensive tasks like battlefield situation assessment, offering comprehensive and accurate information support for military command and decision-making.

Key words situation awareness, multi-modal large model, instruction fine-tuning, model pre-training

0 引言

近年来，人工智能技术取得了突破性进展，特别是以大模型为核心的技术变革，引发了广泛关注。2022年底，OpenAI发布的语言大模型 ChatGPT，以及随后涌

现的各类语言模型和多模态模型，不断刷新人们对人工智能的认知^[1]。

大模型基于“大模型+大数据+大算力”的加持，能够通过语言、视觉交互完成多种任务，具备强大的学习能力、泛化能力和任务处理能力。多模态大模型能够有效融合图像和文本数据，为战场态势认

* 通讯作者

1. 武汉数字工程研究所

1. Wuhan Digital Engineering Institute

知带来了新的机遇。此外，多模态大模型还能够通过强大的学习能力进行语义理解和知识推理，从而实现更全面、准确的态势认知。

1 问题的提出

态势认知是军事指挥决策的核心，旨在全面、准确地感知、理解和预测战场环境、敌我态势和作战行动^[2]。海战场态势生成主要包括目标发现与识别^[3-4]、信息融合处理^[5]、目标意图识别^[6]、威胁研判、态势分发等步骤^[7]，最终按照用户的不同需求，形成不同层级的战场态势，并分发给用户。

在目标信息融合处理方面，主要是将来自不同传感器的探测信息等进行融合，以弥补单一传感器精度不高、数据有缺失的问题。目标信息融合的类型包括雷达、光电、电侦等数据的融合，目前的目标信息融合算法有最小二乘法、基于二分图的最优目标关联匹配法^[8]、序贯卡尔曼滤波算法^[9]、面向基于最优权值分配原则的加权平均法^[10]等。在目标综合识别方面，目前最热门的方式是基于图像的目标识别。其可以分为传统的目标识别方法和基于深

度学习的目标识别方法。基于深度学习的目标识别算法又可分为以 R-CNN^[11]为代表的二阶段算法以及以“你只需看一次”（You Only Look Once, YOLO）系列^[12-14]和“单点多框检测器”（Single Shot MultiBox Detector, SDD）算法^[15]为代表的一阶段算法。这类算法在图像数据充足时，经过训练能够得到性能较优的算法，研究较多，在此不再赘述。此外，目标威胁判断一般基于目标运动状态和历史战术动作等要素构建模型^[16]，战术意图模型一般采用序列贝叶斯网络模型^[17]等。

目前大多数态势认知算法都是基于单一传感器的数据，针对某一个具体的任务进行研究，忽略了态势认知不同任务之间的相关性，且无法解决由于单一模态的信息缺失引起的态势认知精度不高的问题。

基于以上问题，本文提出一种基于多模态大模型的态势认知方法，并将其应用于海上战场态势的认知，如图 1 所示。该方法利用计算机视觉、自然语言处理、大模型等人工智能技术，通过对图像、文本和时序类等多模态数据进行处理，构建了一个统一的多模态大模型，从而实现更全面、准确的战场态势评估和预测等海上态

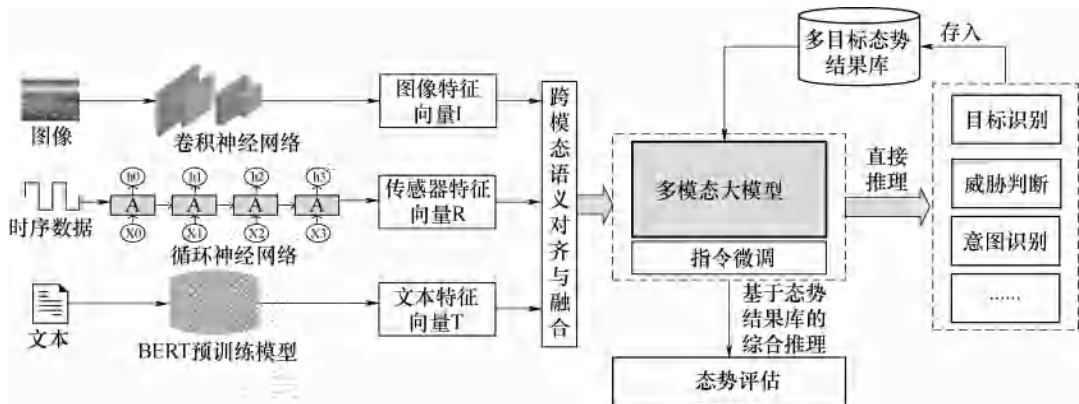


图 1 多模态态势认知大模型构建框架

势认知能力。模型采用预训练和指令微调相结合的方式,仅需少量数据进行微调即可高效、准确地完成目标识别、威胁判断等简单态势认知任务,并构建态势库。基于态势库,模型能够进一步实现战场态势评估等综合态势认知任务,为军事指挥决策提供全面、准确的态势信息支持和决策依据。此外,该模型能够有效弥补单一传感器的不足,实现多模态态势认知,并具有强大的学习能力和泛化能力。随着参数和数据规模的提高,模型的态势认知能力将会进一步提升,为未来军事作战提供更加强大的支持。

2 模型架构

人工智能正在从文本、语音、视觉等单模态智能向着多种模态融合的通用人工智能方向发展。对多模态数据进行统一建模,从而增强模型的跨模态语义对齐能力,实现图像、文本等多模态信息的统一表示,并向集推理、决策等于一体的认知智能演进。

为了提升态势感知能力,本文提出一个基于多模态大模型的态势认知框架,并在现有开源多模态大模型的基础上进行定制化改进和扩展。现有模型大多擅长处理图像和文本数据,但缺乏对时序数据的直接处理能力。时序数据具有更高的实时性和稳定性,能够提供动态环境下的即时信息,不受光照、遮挡等环境影响。因此,研究能够处理图像、文本和时序等多模态信息的大模型,能够更全面、准确地获取战场态势信息,提升态势认知能力。

具体来说,提出的多模态态势认知大模型框架如图1所示。首先,对多模态信息进行处理与编码,形成向量后对其进行

跨模态语义对齐与融合,然后输入多模态大模型。对于如目标识别、威胁判断、意图识别等仅与战场态势中单个或局部目标相关的简单态势任务,首先构建指令微调样本集,其次使用参数高效微调方法获得态势认知领域大模型,最后生成推理结果并将结果存入态势库。对于综合态势任务,如战场态势评估等,可根据具体的任务筛选相关的态势库,并通过构建指令模板进行推理,获得态势评估任务结果。

2.1 数据编码模块

数据编码模块由图像编码器、时序信息编码器和文本编码器组成,不同的编码器负责将不同模态的数据转换为统一的特征向量,以便进行跨模态对齐与融合。

图像编码器:采用基于卷积神经网络(CNN)的编码器,通过卷积层、池化层等提取图像的局部特征和全局特征。其输入形式为图像,包括卫星图像、无人机视频等,输出是图像特征向量,包含了图像的语义信息和不同目标的位置信息。

时序信息编码器:由于循环神经网络(RNN)能够处理时间序列数据,并捕捉数据随时间变化的动态特性,因此,时序信息编码器选用循环神经网络对时序数据进行处理。时序信息数据能够提供目标的动态行为,如目标的运动轨迹等,将其过去噪、归一化、滤波等预处理后,输入RNN网络中学习数据的长期依赖关系和模式,最后输出包含时序数据的语义信息和时间序列信息等的特征向量。

文本编码器:文本编码器采用BERT预训练模型来有效捕捉文本中的长距离依赖关系和上下文信息。通过BERT预训练模型,输出包含输入文本语义信息的文本特征向量。

2.2 跨模态语义对齐与融合模块

不同模态数据（如图像、文本、时序数据）在表征方式和语义信息上存在显著差异，其各自的表征空间往往不一致。为了帮助大模型更好地理解对象之间的指代关系，并有效地融合来自不同模态的信息，本文提出在大模型训练之前进行跨模态语义对齐与融合。具体步骤如下。

1. 目标对齐

图像：利用目标检测算法识别图像中的目标，并获取其位置坐标。

文本：利用自然语言处理技术，将目标名称等文本信息转换为文本向量。

时序数据：将时序数据中的目标位置信息与图像数据中的目标位置进行对齐，如通过匹配时间戳或位置坐标。

例如，假设文本描述中提到“敌舰”，则需要先在图像中定位到“敌舰”的位置，并将其与时序数据中对应的“敌舰”位置进行匹配。

2. 特征融合

使用数据编码模块将不同模态的特征统一编码为向量后，进行拼接形成包含多模态信息的特征向量。然后，使用特征融合层（如卷积层、全连接层、注意力机制等）对拼接后的特征进行融合，以增强不同模态信息之间的交互和语义关联。

通过跨模态语义对齐与融合，可以将不同模态的信息映射到相同的语义空间，消除模态差异，便于模型理解和处理；可以通过融合来自不同模态的信息，更全面地理解目标的态势和意图，增强信息互补性；可以增强模型的泛化能力，使其在面对新的数据和任务时能够更好地适应，进而提升模型性能。

2.3 多模态大模型预训练模块

本文选用 VisualGLM^[18]、LLaVA^[19]等开源多模态大模型作为预训练模型，并设计预训练任务以提升模型对不同模态数据的理解和处理能力，并弥补单一模态信息的不足。预训练任务包括图像-文本匹配、图像-时序匹配等，通过对比学习方法，拉近正样本之间的距离，增大负样本之间的距离，从而学习到更有效的特征表示。

2.4 态势认知子任务模块

在模型顶层，构建一个多任务学习框架，对于目标识别、威胁判断、意图识别等仅与战场态势中单个或局部目标相关的简单态势任务，如目标识别、威胁判断、意图的识别等，使用指令微调方法获得态势认知领域的多模态大模型，再构建提示完成简单态势任务推理，推理结果存入多目标态势结果库。每个子任务都对应一个特定的输出，如目标识别任务输出目标的类别，威胁判断任务输出目标的威胁等级等。对于与完整态势相关的综合任务，则利用该态势库以及微调后的领域大模型，基于提示模板的方式推理获得结果。

3 预训练任务

由于不同态势任务之间往往存在一定的内在联系，采用大模型进行预训练可以充分利用这些任务之间的相关性。通过预训练，大模型能够在学习过程中捕捉到跨任务的通用特征及模式，从而增强其对不同态势任务的泛化能力；同时，多模态预训练能够有效弥补单一传感器的局限性，提高态势认知的准确性。经过预训练的大模型，不仅能在特定态势任务上表现优异，还能在面临新的或相关的态势任务

时, 展现出更好的适应性和准确性。

CLIP 模型^[20]是图文对比学习的经典工作, 为了提高模型的学习能力和泛化能力, 本文基于 CLIP, 进行不同模态之间预训练任务损失函数的设计。在训练过程中, 使用对比学习的方式对图像、文本和时序信息进行学习, 将匹配的图像-文本对、图像-时序对视为正样本, 将当前训练 batch 中的其他随机图像-文本、图像-时序对视为负样本。

计算区域到单词的相似度的方式如下: 首先, 给定一个图文对 (I, T) , 其中图像 $I = \{r_1, r_2, \dots, r_i, \dots, r_n\}$, $i = 1, 2, \dots, n$, r_i 代表检测到的图像中的物体区域; 文本 $T = \{w_1, w_2, \dots, w_j, \dots, w_m\}$, $j = 1, 2, \dots, m$, w_j 表示句子中的单词。对于每个区域 r_i , 计算其与句子中第 j 个单词的相似度:

$$\alpha_{ij} = \frac{\exp(s(r_i, w_j))}{\sum_{j=1}^m \exp(s(r_i, w_j))} \quad (1)$$

其次, 对单词特征加权得到物体区域的语义表示:

$$\alpha'_i = \sum_{j=1}^m \alpha_{ij} w_j \quad (2)$$

最后, 通过对区域的相似度进行相加, 得到区域到单词的相似度:

$$s(I, T) = \sum_{i=1}^n s(r_i, \alpha'_i) \quad (3)$$

同理, 可以得到单词到区域的相似度。

本文通过视觉编码器和文本编码器分别得到图像 I 的特征向量 \mathbf{F}_I 和文本的特征向量 \mathbf{F}_T 后, 在同一个批次 B 中, 图像-文本损失函数如下式所示:

$$L_{I2T} = -\log \frac{\exp(s(\mathbf{F}_I, \mathbf{F}_T))}{\sum_{T' \in B} \exp(s(\mathbf{F}_I, \mathbf{F}_{T'}))} \quad (4)$$

$$L_{T2I} = -\log \frac{\exp(s(\mathbf{F}_I, \mathbf{F}_T))}{\sum_{I' \in B} \exp(s(\mathbf{F}_{I'}, \mathbf{F}_T))} \quad (5)$$

$$L_{ITC} = \frac{1}{2}(L_{I2T} + L_{T2I}) \quad (6)$$

同理, 图像-时序对可以表示为 (I, R) , 其中图像 $I = \{r_1, r_2, \dots, r_i, \dots, r_n\}$, $i = 1, 2, \dots, n$, r_i 代表检测到的图像中的物体区域; 时序 $R = \{r_1, r_2, \dots, r_p, \dots, r_q\}$, $p = 1, 2, \dots, q$, r_p 表示的是某一个物体在一定时间内的运动轨迹。然后, 与计算图像-文本损失函数方式类似, 首先使用图像编码器和时序编码器得到图像 I 的特征向量 \mathbf{F}_I 和时序的特征向量 \mathbf{F}_R 后, 图像-时序损失函数如下式所示:

$$L_{I2R} = -\log \frac{\exp(s(\mathbf{F}_I, \mathbf{F}_R))}{\sum_{R' \in B} \exp(s(\mathbf{F}_I, \mathbf{F}_{R'}))} \quad (7)$$

$$L_{R2I} = -\log \frac{\exp(s(\mathbf{F}_I, \mathbf{F}_R))}{\sum_{I' \in B} \exp(s(\mathbf{F}_{I'}, \mathbf{F}_R))} \quad (8)$$

$$L_{IRC} = \frac{1}{2}(L_{I2R} + L_{R2I}) \quad (9)$$

那么, 最终的图像-文本-时序损失函数可以表示为:

$$L = L_{ITC} + L_{IRC} \quad (10)$$

4 任务相关的大模型微调与推理

4.1 简单态势任务

对于简单态势任务, 可首先构建指令微调样本集, 其次使用参数高效微调方法获得态势认知领域大模型, 最后进行推理生成结果, 并将结果存入态势库。

1. 微调样本集构建

首先, 确定所有可能的态势任务, 针对不同的任务设计多个差异性问題; 其次, 基于历史态势分析数据经过人工提取一部分任务相关的问答样本; 最后, 使用通用大模型对已有样本集进行扩增, 形成丰富多样的态势任务问答集。

2. 大模型指令微调

大模型微调输入由三部分组成：一是大模型指令，用于描述当前态势任务；二是任务问答举例，采用 Few-shot 的方式进行微调；三是当前对象的多模态输入。大模型微调的输出就是任务回答。针对目标识别、威胁判断、意图识别三种任务来说，指令可构建如下形式：“你是一个态势分析大模型，可基于当前目标的图像、文本、时序等多模态信息，进行目标识别、威胁判断和意图识别。多模态信息已经过融合处理，模型输出应遵循以下格式：{(1) 目标识别结果：目标类型：×××；目标位置：×××；目标大小：×××；(2) 威胁判断结果：目标威胁等级：×××；目标威胁描述：×××；(3) 目标意图：目标潜在意图：×××}。这里有几个态势任务例子 {举例：请识别给定信息中的目标类型，评估该目标的威胁等级，并分析该目标的潜在意图}。下面给出多模态融合信息：{图像，文本，时序诗句}。”大模型微调方法采用 LoRA^[21] 微调，这是一种参数高效微调方法，能在低资源情况下完成领域知识学习。

3. 大模型推理与态势结果存储

大模型推理输入结构与训练阶段相同，仍然保留完整指令。经过推理可获得当前目标的具体类型、威胁度、意图信息，推理结果以文本表示。为建立当前战场态势库，可将该目标的推理结果使用 BERT 模型向量化处理，将处理后的向量与文本结果合并统一存储。

4.2 综合态势任务

综合态势任务属于简单态势任务的上层任务。可根据当前具体任务筛选相关的态势库，然后构建指令模板，联合已经过滤后的态势库，推理获得态势评估任务

结果。

1. 态势库筛选

为保证大模型能充分获取任务相关的态势信息，应对完整态势目标进行筛选。筛选可基于余弦相似度匹配完成，计算向量化后的任务文本和态势库中的所有目标向量的相似度，取最相关的 20% 目标作为大模型参考输入。例如，对于任务：评估当前态势中存在威胁的舰船目标的意图，则应该筛选态势目标库中具有威胁的舰船目标。

2. 提示构建与推理

这里不再进行微调训练，而是直接使用前述微调后的多模态大模型，采用基于提示的方法推理获得态势评估结果，提示构建与前述指令构建相似，包括任务描述、筛选后的态势库以及回答结构。

5 结束语

本文提出了一种基于多模态大模型的态势认知方法，旨在提升海上战场态势的认知能力。该方法融合了计算机视觉、自然语言处理和大模型等先进技术，能够有效处理和分析图像、文本、时序等多种模态数据。模型首先利用战场上采集的文本-图像对、图像-时序对等多模态数据进行预训练，学习多模态数据的语义关联和特征表示。随后，通过指令微调的方式，利用少量与任务相关的数据进行模型适配，从而完成态势认知大模型的构建。基于预训练和微调后的模型，通过构建提示，模型能够高效完成目标识别、威胁判断等简单态势认知任务，并将结果存入态势库。同时，基于态势库，模型能够通过构建提示的方式进一步完成战场态势评估等综合态势认知任务，为军事指挥决策提供全面、准确的态势信息支持。

通过多模态态势认知大模型, 战场人员能够实现对战场态势全方位、多层次的理解, 并能够应用于多种任务。模型的学习能力和泛化能力, 使得它在面对新的数据和任务时能够快速适应, 并提高态势认知的准确性。

为了更好地将多模态大模型应用于军事态势认知, 并为未来的军事决策提供可靠和有效的支持, 未来可以进一步研究以下方向: ①研究模型的轻量化, 使其能够在资源受限的设备上运行, 如小型舰艇上的嵌入式系统; ②研究小样本学习, 降低战场数据稀缺对模型能力的限制; ③研究模型的可解释性, 增强模型的透明度和可信度; ④探索对抗学习方法, 以提高模型的安全性, 并使其能够有效抵御对抗攻击。

参考文献

- 1 WU T Y, HE S Z, LIU J P, et al. A brief overview of ChatGPT: The history, status quo and potential future development [J]. *IEEE/CAA Journal of Automatica Sinica*, 2023 (5): 1122-1136.
- 2 刘熹, 赵文栋, 徐正芹. 战场态势感知与信息融合 [M]. 北京: 清华大学出版社, 2019.
- 3 BLASCH E. Multi-Intelligence critical rating assessment of fusion techniques (MiCRAFT) [C] // *Proceedings of Signal Processing, Sensor/Information Fusion, and Target Recognition XXIV: Volume 9474. Balti-more: SPIE*, 2015: 81-88.
- 4 蒋超, 崔玉伟, 王辉. 基于图像的无人机战场态势感知技术综述 [J]. *测控技术*, 2021, 40 (12): 14-19.
- 5 邵振峰, 党超亚, 张红萍, 等. 多源遥感数据在战场环境智能态势感知的现状及展望 [J]. *中国空间科学技术*, 2024, 44 (1): 11-22.
- 6 贺玲, 贺照辉. 大数据技术在战场态势感知中的应用 [J]. *科技与创新*, 2023 (7): 178-181.
- 7 程晓雪. 海战场综合态势构建与同步方法 [J].

- 指挥信息系统与技术, 2016, 7 (3): 53-57.
- 8 吴汉宝, 李伦, 张志云. 基于二分图最优完备匹配的目标关联算法 [J]. *华中科技大学学报*, 2017, 45 (2): 95-100.
- 9 杨向广, 周永丰, 黄登斌, 等. 异步多传感器数据融合 [J]. *舰船电子工程*, 2006, 26 (1): 50-53.
- 10 黄友澎, 吴汉宝, 张志云. 基于方位合成的异类传感器航迹数据融合算法 [J]. *西南交通大学学报*, 2011, 46 (2): 277-281.
- 11 GIRSHICK R, DONAHUE J, DARRELL T, et al. Rich feature hierarchies for accurate object detection and semantic segmentation [C] // *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2014: 580-587.
- 12 REDMON J, FARHADI A. YOLO9000: better, faster, stronger [C] // *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2017: 7263-7271.
- 13 REDMON J, FARHADI A. Yolov3: An incremental improvement [J]. *arXiv preprint arXiv: 1804.02767*, 2018.
- 14 BOCHKOVSKIY A, WANG C Y, LIAO H Y M. Yolov4: Optimal speed and accuracy of object detection [J]. *arXiv preprint arXiv: 2004.10934*, 2020.
- 15 LIU W, ANGUELOV D, ERHAN D, et al. Ssd: Single shot multibox detector [C] // *European conference on computer vision*. Springer, Cham, 2016: 21-37.
- 16 葛顺, 夏学知. 用于战术意图识别的动态序列贝叶斯网络 [J]. *系统工程与电子技术*, 2014, 36 (1): 76-83.
- 17 李进军, 丛蓉, 熊吉光. 舰艇编队对空中目标的威胁程度判断模型 [J]. *火力与指挥控制*, 2005, 30 (7): 29-33.
- 18 DING M, YANG Z Y, HONG W Y, et al. Cogview: Mastering text-to-image generation via transformers. [J] // *Advances in Neural Information Processing Systems*, 2021 (34): 19822-19835.
- 19 LIU H T, LI C Y, LI Y C, et al. Improved Baselines with Visual Instruction Tuning [J]. *arXiv preprint arXiv: 2310.03744*.
- 20 RADFORD A, KIM J W, HALLACY C, et al.

Learning transferable visual models from natural language supervision [C] //International Conference on Machine Learning. Vienna, 2021: 8748 – 8763.

21 HU E J, SHEN Y, WALLIS P, et al. LoRA: Low-Rank Adaptation of Large Language Models [C] //International Conference on Learning Representations. 2022.

基于混合检索增强的双塔模型技术研究

郜洪奎^{1*} 马瑞祥¹ 包骐豪¹ 夏少杰¹ 瞿崇晓¹

摘要 知识检索趋向于运用向量检索加速信息获取，以便在大语言模型中整合提炼。然而，单一向量表示限制和缺乏精准排序造成无关信息混入，降低了答案匹配度。为应对挑战，提出了混合检索双塔模型，模型融合多路径召回策略，确保检索结果全面。通过采用双塔结构实现了对检索结果的多层次排序，显著提升了检索结果的相关性。进一步地，将优化信息与原始查询输入大语言模型生成精确答案。实验表明，此方法显著提升了检索的准确性。

关键词 知识搜索，大语言模型，混合检索双塔模型，多路径召回策略

Based on the Hybrid Retrieval-Augmented Dual-Tower Model

GAO Hong-Kui^{1*} MA Rui-Xiang¹ BAO Qi-Hao¹ XIA Shao-Jie¹ QU Chong-Xiao¹

Abstract Knowledge retrieval increasingly relies on vector-based methods to accelerate information acquisition for integration within large language models. However, limitations in single-vector representations and the absence of refined ranking mechanisms often allow irrelevant information to infiltrate, reducing the alignment of answers. To tackle these issues, we introduce a Hybrid Retrieval-Enhanced Dual-Tower Model that integrates multi-path retrieval strategies to ensure comprehensive search outcomes. Employing a dual-tower architecture enables multilevel sorting of retrieved results, considerably boosting their relevance. Additionally, enhanced information, alongside the original queries, is fed into the large language model to produce accurate answers. Empirical evidence confirms a substantial increase in retrieval accuracy, highlighting the effectiveness of this approach.

Key words knowledge search, large language models, hybrid retrieval-enhanced dual-tower model, multi-path recall strategies

0 引言

大语言模型在自然语言处理^[1]及多模态领域^[2]取得了突破性进展。这一进展的同时带来了“模型幻觉”问题，即模型有

时会生成貌似合理但实际上却是不准确或虚构的信息。为应对这一挑战，检索增强生成（Retrieval-Augmented Generation, RAG）技术应运而生，作为一种关键策略，它与 Transformer 技术几乎同期出现，并随着大语言模型的演进迅速发展成熟。

* 通讯作者

1. 中国电子科技集团公司第五十二所

1. The 52nd Research Institute of China Electronics Technology Group Corporation

RAG 专注于整合预训练模型的额外知识来提升模型的能力，初期的工作主要集中在优化预训练，参考文献 [3-5] 对此有详细阐述。ChatGPT^[1] 的推出展现了大语言模型在上下文学习方面的惊人能力。该事件促使 RAG 的研究方向发生转变，聚焦于如何在推理过程中为模型提供信息，以应对更深层次和复杂的知识问题。随着研究的不断深入，RAG 的策略不仅限于推理阶段，还进一步扩展到了微调大语言模型。本研究的关注点是在大语言模型的推理过程中融入外部知识，旨在增强模型处理复杂、知识密集型问题的能力。

伊扎卡尔 (Izacard) 等^[6] 与卡尔普欣 (Karpukhin) 等^[7] 的研究指出，结合 RAG 与大模型能有效提升准确性，减少事实错误，但仍面临知识全面性和检索精确性的挑战。Shi 等^[8] 和 Gao 等^[9] 指出，当前 RAG 因未受过高效利用检索信息的训练，导致选择和生成内容时的不准确性，输出与检索信息不完全匹配。阿塞 (Asai) 等^[10] 提出了一种自我反思的 RAG 策略，通过动态检索和反馈提高生成内容质量，但这一过程增加了计算成本。

尽管 RAG 技术在多个领域已取得显著进展，但在军事决策这一重要领域，其应用尚处于初步探索阶段，主要面临着两大挑战：首先，军事决策往往依赖于快速精准的信息获取，向量检索模型在处理如指挥控制、情报分析和军事决策等场景中的简短查询时，若不能精准理解用户查询意图，可能会导致错误的情报检索，进而影响指战员的战局判断和作战计划的制订。其次，缺乏高效的结果排序机制意味着在紧急情况下，军事人员可能需要从大量不相关性排序的信息中手动筛选重要情报，不仅耗时耗力且可能错失最佳决策良机，对作战效

率和安全构成严重威胁。

为应对军事决策场景中的挑战，提出了混合检索增强的双塔模型 (Hybrid Retrieval - Enhanced Dual - Tower Model, HREDTM)。该模型的核心目标是提升军事决策场景下信息检索的精确度及大型模型生成答案的准确性。本文的贡献主要体现在技术创新与应用优化两个方面。

在技术层面，HREDTM 集成了向量与关键词的混合检索模型，能从多个维度、多个角度准确捕捉军事决策人员的需求，确保检索结果的高相关性和准确性。同时，结合双向循环神经网络 (Bidirectional Long Short-Term Memory, BiLSTM) 和文本卷积神经网络 (Text Convolutional Neural Network, TextCNN) 的双塔模型，不仅能挖掘长距离语义特征，还能捕捉短距离语义信息，全面理解文本的多层次含义，特别适用于处理军事决策领域的复杂文本结构。

在应用层面，HREDTM 对军事决策的特殊需求进行了优化，确保在紧急情况下实现快速、精准的信息获取，同时通过高效的结果排序机制，帮助军事人员从海量信息中快速筛选关键情报，显著提升了军事决策的质量和效率。此外，HREDTM 直接应对军事决策中的信息获取速度与精度要求，有效增强了决策者的战局判断能力和作战计划制订效率，对提升作战效率和保障军事安全具有重大意义。

本文的结构如下：引言分析了当前 RAG 在信息检索领域内的研究现状及存在的问题，引出其在军事决策中的创新应用，明确研究方法 with 目标。接着，第一章详细介绍 HREDTM 模型的整体架构，并逐一深入解析各个子模块的设计与功能。随后，第二章是实验环节，包括实验数据来源、实验中的评价标准、模型参数，以及

实验结果分析。最后，在第三章对本文进行总结并展望未来的研究方向。

1 模型架构

本章主要介绍 HREDTM 模型的架构原理，如图 1 所示，主要包含三大核心组件：混合检索模型、双塔排序模型及大型问答模型。首先，通过混合检索模型，综合运用关键词匹配与向量表示技术，针对军事决策人员的查询精准定位知识库中的相关信息，其输入是军事决策人员的检索问题，输出是候选上下文列表。其次，双层排序模型介入，模型接收的是混合检索模型输出的候选上下文列表，并优化排列为重要性排序的上下文序列。最后，大型问答模型凭借强大的归纳推理与语言理解特性，对排序后的上下文列表与原始问题深入剖析，生成最终答案。

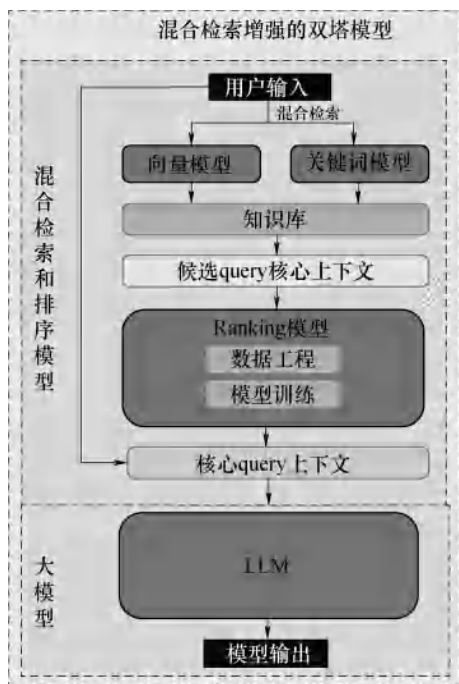


图 1 HREDTM 模型整体架构

整个流程，各个子模型间相互协作共同完成从接收军事决策人员的问题到输出精确答案。

1.1 混合检索模型

军事场景下的文献资料涵盖专业著作、学术论文以及日常训练日志等。其中，专业书籍与学术论文因具备固有的结构化特性，蕴含深厚的语义内容，特别适宜利用向量检索技术实现精确匹配。然而，在面对用户问题过于简洁或处理日常训练日志这类典型的非结构化数据时，向量模型往往难以捕捉到足够的语义信息，导致检索效果较差。相比之下，关键词检索模型直接依据文本中的词汇进行匹配，无须依赖复杂的语义理解，因此，在处理简短查询或非结构化文档时表现更佳。鉴于此领域数据的特殊性以及上述两种检索方法的独特优势，构建了混合检索模型，旨在结合向量检索的深入理解能力与关键词检索的快速定位优势，从而实现更全面且精确的信息获取，增强检索的效率和覆盖范围。

向量检索模型的基石是 BGE-M3^[11] 模型。为了更好地适应和优化军事应用场景，对 BGE-M3 模型进行了定制化训练，涵盖数据预处理和增量训练两个阶段。其中，数据预处理极为关键，其精细度直接影响向量模型的表现。该阶段涉及数据清洗，包括剔除文本中的非必要元素，如标点符号、数字和特殊字符，以及引入了一种效率至上的贪婪句子切分机制策略，旨在最大化利用文本信息，以确保生成的向量能够精准捕捉到文本语义。这一策略注重如何最有效地分割句子，以增强向量表示的准确性，算法细节如下：

(1) 通过标点符号分割文本，生成一系列候选句子，并设定一个最大句子长度阈值 L 。

(2) 从候选句子序列出发, 以首个句子为起点, 计算其字符数量。若字符数不超过 L , 则纳入最终句子集。随后, 检查第二个句子及其与当前最终句子集的字符数总和, 若总和仍不超过 L , 则将之加入, 此过程持续进行, 依次评估第三个、第四个、第五个句子等, 以此类推。

(3) 当构建的句子集 N 中所有句子的字符总和不超过 L 时, 一旦新增句子会导致总字符数超过 L , 则停止添加, 并回溯至最后一个满足条件的句子。具体而言, 计算该句子前一个句子的字符数, 并加上现有句子集的字符总和, 若此总和不超过 L , 则将前一个句子置于句子集开头。继续检查字符总数, 若保持在 L 之内, 就继续向前检验, 直至句子集的字符总数刚好或超过 L 为止。

特别地, 若单一句子长度本身就超过阈值 L , 需先将该句子分割, 确保每个部分的字符数不超过 L 。至于增量训练, 则遵循 BGE-M3 模型的官方指导实施。

为了构建一个高效且精准的军事决策领域关键词模型, 选取了 BM25^[12] 和 TextRank^[13] 两种算法作为其核心组成部分。相较于其他传统垂直领域的关键词模型, 所构建的军事决策领域关键词模型具有以下优势:

(1) 融合向量检索与关键词检索: 传统的关键词模型往往只依赖关键词匹配, 而文中模型结合了向量检索和关键词检索, 能够更全面、多角度地理解查询意图, 提高检索的准确性和召回率。

(2) 特定领域的深度优化: 鉴于军事决策领域特有的专业术语密集、语境复杂及信息安全要求高的特点, 模型在训练阶段使用了大量军事相关语料库, 确保了模型在军事领域的高度适用性, 能够准确识别并匹配专业术语, 同时兼顾信息安全,

为军事决策提供了坚实的数据基础。

(3) 实时性和动态适应性: 考虑到军事行动中实时决策的迫切需求, 采用了 BM25 算法, 它特别适用于需要快速定位关键信息的场景; 而 TextRank 算法, 通过图论评估词频重要性, 为决策者提供即时全面的信息概览。BM25 和 TextRank 的结合, 恰好满足了军事决策对于信息处理速度与精确度的高要求。

具体执行流程如下: 第一步, 借助 BM25 算法来衡量军事决策人员的查询与知识库中段落的相关程度; 第二步, TextRank 算法通过一系列迭代过程, 以军事决策人员的查询与各段落关联度为权重指标, 从中筛选出与查询最相关的文本作为潜在的上下文参考。以下是 BM25 和 TextRank 的具体计算公式:

$$IDF(q_i) = \log \frac{N - n(q_i) + 0.5}{n(q_i) + 0.5} \quad (1)$$

$$Score(Q, d) = \sum_i^n IDF(q_i) \cdot \frac{f_i \cdot (k_1 + 1)}{f_i + k_1 \cdot \left(1 - b + b \cdot \frac{dl}{avgdl}\right)} \quad (2)$$

$$WS(V_i) = (1 - d) +$$

$$d \cdot \sum_{V_j \in In(V_i)} \frac{w_{ji}}{\sum_{V_k \in Out(V_j)} w_{jk}} WS(V_j) \quad (3)$$

式中, k_1 , b 为调节因子; dl 为知识库中文本块 Q 的长度; $avgdl$ 为知识库中所有文本块的平均长度; q_i 为军事决策人员查询的第 i 个词; f_i 为军事决策人员查询的词 q_i 在文本中出现的频率; $IDF(q_i)$ 为军事决策人员查询的第 i 个词语的逆文档数;

w_{ji} 为任两点 V_i, V_j 之间边的权重; $WS(V_i)$ 为节点 (知识库中文本段落) V_i 的评分; $In(V_i)$ 为指向节点 (知识库中文本段落) V_i 的节点 (知识库中文本段落) 集合; $Out(V_i)$ 为节点 (知识库中文本段落) V_j 所指向的节点 (知识库中文本段落) 集合; d 为阻尼系数; $WS(V_j)$ 为上次迭代节点 (知识库中文本

段落) V_i 计算出的评分。注意, w_{ji} 和 $Score(Q, d)$ 表示含义相同, 即表示任意两点之间的相关性。

通过结合精准的向量检索技术和高效的关键词检索策略, 极大地提升了军事场景下的检索广度和深度。图 2 详细展示了所构建的混合检索模型的架构设计, 清晰展现了其内在机制与运作流程。

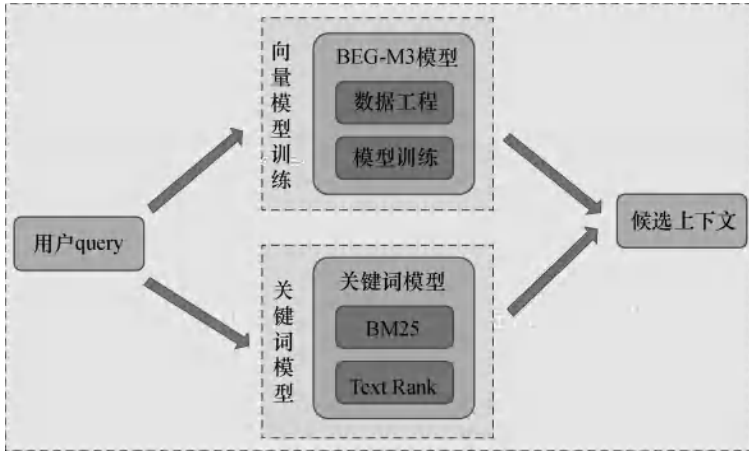


图 2 混合检索模型

1.2 双塔重排模型

混合检索模型采用多路召回策略获取了大量候选上下文集合。然而, 从庞大的候选上下文集合中精确挑选出最相关上下文成为一大挑战。为应对这一难题, 行业普遍采纳重排算法的策略^[14-15]。在此基础上, 设计了双塔重排算法, 该算法融合了 BiLSTM 与 TextCNN 两种模型的优势。双塔架构中的 BiLSTM, 得益于其独特的长期记忆网络结构 LSTM^[16] (Long-Short Term Memory), 能够同时处理向前和向后的信息单元流, 从而在捕捉长文本段落间的复杂依赖关系上展现卓越效能, 尤其是在面对复杂且篇幅较长的文本段落时。与此同时, TextCNN 虽然根植于传统的卷积神经网络框架^[17], 但通过简化设计, 仅使用一

层卷积层和池化层, 这不仅减轻了模型的复杂性, 加速了训练进程, 还通过多尺度卷积核的运用, 实现了精准的特征提取与浓缩, 尤其擅长于从短文本段落中提炼丰富的语义特征, 极大地增强了模型对文本深层次意义的解读与表达, 两者结合, 显著提升了模型对文本深层含义的理解与表达能力。

需要注意的是, 在双塔排序模型中, 采用了 Pair wise Ranking Loss 作为损失函数, 其具体形式如下:

$$\text{loss}(\theta) = - (K2) 1E(x, y_w, y_l) D[\log(\sigma(r_\theta(x, y_w) - r_\theta(x, y_l)))] \quad (4)$$

式中, D 为问题答案的排序数据集; x 为数据集 D 中的问题; K 为每个问题对应的答案数量; y_w 和 y_l 为问题 x 对应的 K 个答

案中的两个, 并且 y_w 的排序比 y_i 高; θ 为模型需要优化的参数。

最后, 采用了集成学习策略来增强双塔排序模型, 该策略结合了两种深度学习模型的优势。融合 BLSTM 生成的语义向量与 TextCNN 得到的语义向量, 形成

一个更加全面的语义综合向量。将这个富含多维度的语义向量, 作为关键输入, 驱动双塔排序模型的训练。模型的训练过程旨在最小化定义的损失函数, 以优化排序性能。详细的双塔排序模型架构如图 3 所示。

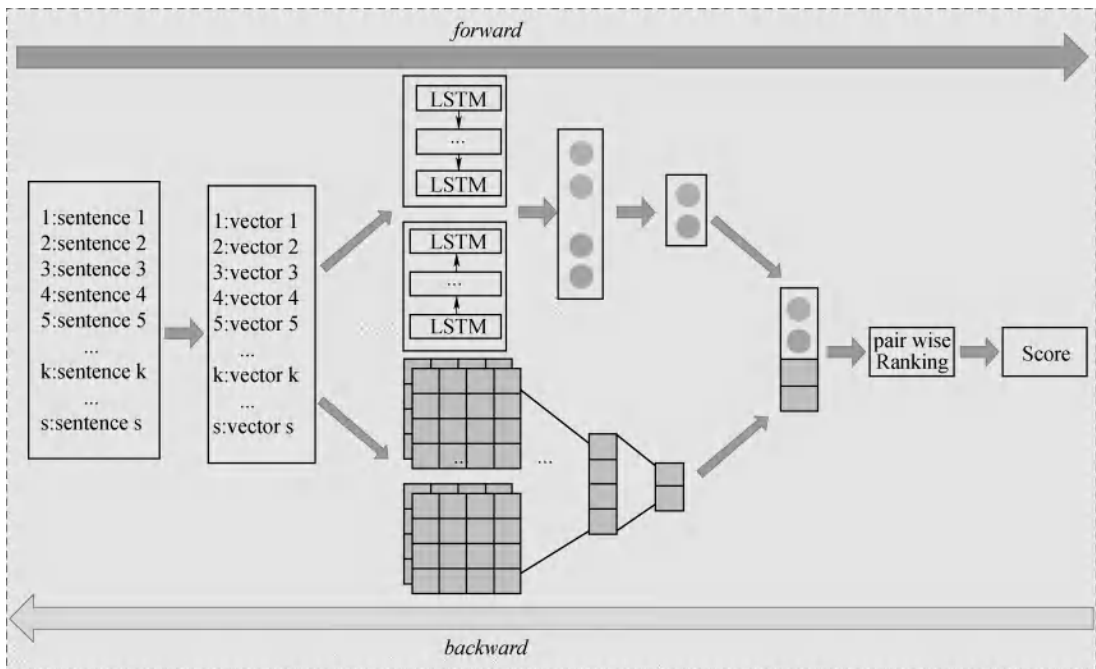


图 3 双塔排序模型架构

1.3 大模型问答

本模块旨在利用大型语言模型的卓越理解力和高效的归纳力, 对经过双塔排序技术处理的上下文列表与军事决策人员的查询进行深度整合和精练概括。整个流程围绕三大关键步骤构建, 旨在确保输出答案不仅精准无误, 而且符合人性化阅读体验。本研究采用的基础大模型为阿里巴巴集团开源的通义千问^[18]。

预处理阶段, 聚焦于将双塔排序后所得的上下文列表转化为模型可识别的输入格式。涉及剔除冗余信息、纠正语法瑕疵、统一专业术语与缩写, 以及适配预定

的序列长度和词汇编码标准, 以此增强模型解析精度与反应速率。

应用阶段, 需要将模型应用于实战场景, 为军事决策者提供迅速且准确的支持服务。用户只需采用自然语言表述查询需求, 模型即可凭借其卓越的语言处理能力, 以简明扼要的语言形式反馈结果, 促进人机交互的高效性与自然性。

后处理阶段, 会对模型的输出结果进行优化处理, 确保其内容结构和表达方式符合人类阅读习惯与认知模式。此环节涵盖语法结构的优化、逻辑关系的理顺以及表述风格的简化, 旨在使军事决策者能够快速吸收信息并据此做出决策。

通过以上三个步骤，能充分利用大型语言模型的强大能力，为军事决策人员提供既精准又人性化的信息支持，从而提升决策效率和质量。

2 实验设计

本章着重介绍 HREDTM 模型的实验设计，内容包括：数据集选择、评估标准、超参数配置、对比实验及结果分析。随后，将细致介绍实验采用的数据集，确立评价指标，披露实验中的超参数设置。最后，通过消融对比实验证明模型的有效性与优越性。

2.1 实验数据集

通过网络搜集与内部资源数据整合，获取了大量高质量的军事业务场景下的专业书籍、学术文章及日常训练记录等语料，并对语料做去重处理以保证其独特性。从这些资料中随机挑选出 70000 篇文献，用于建立和优化 BGE-M3 向量模型，以增强信息的向量表达能力。同时，随机筛选 3000 篇文档用来创建情境问答对，生成了约 60000 个问题与答案对。运用文中第二章第一节介绍的混合检索技术，其中 50000 个问题与答案对被指定用于训练双塔模型，而其余的 10000 对则被保留为测试集，以评估和验证模型的性能和准确性。

2.2 实验评价指标

为了精确评估模型的性能，本研究采用了精确匹配指标^[19] (Exact Match, EM)。具体评价细则详述如下：首先，进行标准化操作，包括统一字符大小写、消除空行和重复内容，确保评估基准的一致性。其次，通过对比模型生成的答案与预设的标准答案是否完全一致，作为判定回

答正确与否的唯一依据。

2.3 实验模型参数

在设计混合检索模型时，通过对 BM25 模型的精细调参，将 k_1 参数设定为 1.5，而 b 参数设置为 0.75，以此来达到优化信息检索效能的目的。对于 TextRank 算法，配置其阻尼系数 d 为 0.85，并执行了 300 轮迭代，以确保算法结果的稳定性和可靠性。

在训练 BGE-M3 词向量模型过程中，选择 1024 作为词向量的尺寸，设定学习率为 0.0001，其余参数保留默认设置，旨在实现训练效率与模型效果之间的良好平衡。

在构建双塔排序模型时，对两部分架构进行了细致配置：BLSTM 和 TextCNN 的隐藏层均设为 128 个单元。统一采用了 0.0001 的学习率和 Adam 优化器来促进学习过程。为了防止过拟合，设置了 dropout 比例为 0.1。每批次训练数据大小定为 128。在 LSTM 层数上，选择了 3 层结构。针对 TextCNN，设计了多尺度特征提取，其卷积核尺寸分别为 3、4、5，每个尺寸的卷积核数量均为 256，以增强模型的表达能力。这样的配置旨在综合提升模型的性能与效率。

2.4 验证内容和结果分析

为了验证 HREDTM 模型的有效性和合理性，设计并实施了一系列对比实验。其中消融实验尤其关键，它被划分为两个关键环节。第一部分致力于分析混合检索机制对于性能提升与精确度维护的贡献，具体聚焦于 BGE-M3 模型与传统关键词检索模型独立及协同工作的效能比较。第二部分深入探究了基于 BiLSTM 和 TextCNN 的双塔排序模型如何通过特征互补机制，增强整个系统的稳定性和泛化性能。以下是

实验的具体设置细节：

实验 1：第一组实验专注评估混合检索模型策略，特别是 BGE-M3 模型与传统关键词检索模型的单独及整合应用。通过控制变量法，对比了仅依赖 BGE-M3 模型、仅采用关键词检索，以及模型融合的混合策略。详细的实验结果数据在表 1 中列出，清晰展示了不同方法间的性能对比。

实验 2：第二组实验集中分析 BiLSTM 和 TextCNN 构建的双塔模型在提升学习效率与模型综合表现方面的潜力。通过对比 BiLSTM、TextCNN 单独运行的结果与它们结合后的双塔模型，利用控制变量法，指出双塔模型在互补性、稳健性及泛化能力上的优势。实验结果充分展示在表 2 中，有力支撑了研究的核心假设。

表 1 HREDTM 模型的混合检索消融实验

方法	EM
BGE-M3 模型+大模型	0.653
关键词模型+大模型	0.612
BGE-M3 模型+关键词模型+大模型	0.681
HREDTM	0.832

表 2 HREDTM 模型的双塔消融实验

方法	EM
混合检索+BiLSTM+ 大模型	0.782
混合检索+TextCNN+大模型	0.754
HREDTM	0.832

此系列实验设计严谨，通过对比内部组件的消融研究，系统地评估和验证了 HREDTM 模型的创新性。

通过分析表 1 的混合检索消融实验结果，得出如下关键结论：① HREDTM 模型在知识库检索任务中展现出了卓越的性能，其精确度高达 0.832，不仅验证了模型设计的合理性和有效性，而且凸显了其在信息检索领域的巨大潜力和实用价值。

② 相较于关键词模型结合大模型，BGE-M3 模型与大模型的整合显示出更优的性能，这证实了在语义理解方面，基于向量的检索超越了传统的关键词冷启动方法。

进一步地，表 2 所展示的双塔消融实验结果揭示：① 双塔架构下，使用 BiLSTM 与 TextCNN 的模型在所有评估指标上均胜出，这表明该模型能同时掌握文本的全局语义和局部细节，超越了仅侧重一面的单一模型，实现了信息的多维度精准获取与筛选，显著提高了模型的泛化性能和上下文理解精度。② 此外，值得注意的是，采用混合检索与 BiLSTM 的组合在精确度上相较混合检索配以 TextCNN 的模型高出将近 3 个百分点。这一发现强调，在处理如军事场景业务下的长文本时，BiLSTM 展现出了更优的处理能力，证实了其在长文本处理领域的优越性。

3 结束语

针对军事场景中从语料中高效获取知识的难题，提出了 HREDTM 模型。该模型融合了混合检索机制与文本长短期语义的深度感知，采用双塔架构，由 BiLSTM 和 TextCNN 构成。模型的工作机制是：首先，借助高效的混合检索策略，准确识别出与军事决策人员的查询紧密相关的候选上下文；其次，双塔架构发挥作用，其中，BiLSTM 负责揭示上下文中的长期依赖关系，而 TextCNN 专注于捕获局部细节，两者协作对候选上下文进行精确排序；最后，将排序后的上下文与军事决策人员的查询一同送入大型模型，以实现信息的高效率整合及知识提取。一系列的消融实验有力证实了 HREDTM 模型的卓越性能和有效应用价值。展望未来，研究方向将侧重

于优化大模型的排序机制，并探索利用蒸馏技术来进一步增强模型的效率与精确度。

参考文献

- 1 OUYANG L, WU J, JIANG X, et al. Training language models to follow instructions with human feedback [J]. *Advances in neural information processing systems*, 2022, 35: 27730–27744.
- 2 ACHIAM J, ADLER S, AGARWAL S, et al. Gpt-4 technical report [J]. *arXiv preprint arXiv*: 2303. 08774, 2023.
- 3 ARORA D, KINI A, CHOWDHURY S R, et al. Gar-meets-rag paradigm for zero-shot information retrieval [J]. *arXiv preprint arXiv*: 2310. 20158, 2023.
- 4 LEWIS P, PEREZ E, PIKTUS A, et al. Retrieval-augmented generation for knowledge-intensive nlp tasks [J]. *Advances in Neural Information Processing Systems*, 2020, 33: 9459–9474.
- 5 BORGEAUD S, MENSCH A, HOFFMANN J, et al. Improving language models by retrieving from trillions of tokens [C] // *International conference on machine learning*. PMLR, 2022: 2206–2240.
- 6 IZACARD G, GRAVE E. Leveraging passage retrieval with generative models for open domain question answering [J]. *arXiv preprint arXiv*: 2007. 01282, 2020.
- 7 KARPUKHIN V, OĞUZ B, MIN S, et al. Dense passage retrieval for open-domain question answering [J]. *arXiv preprint arXiv*: 2004. 04906, 2020.
- 8 SHI F, CHEN X, MISRA K, et al. Large language models can be easily distracted by irrelevant context [C] // *International Conference on Machine Learning*. PMLR, 2023: 31210–31227.
- 9 GAO T, YEN H, YU J, et al. Enabling large language models to generate text with citations [J]. *arXiv preprint arXiv*: 2305. 14627, 2023.
- 10 ASAI A, WU Z, WANG Y, et al. Self-rag: Learning to retrieve, generate, and critique through self-reflection [J]. *arXiv preprint arXiv*: 2310. 11511, 2023.
- 11 CHEN J, AO S, ZHANG P, et al. Bge m3-embedding: Multi-lingual, multi-functionality, multi-granularity text embeddings through self-knowledge distillation [J]. *arXiv preprint arXiv*: 2402. 3216, 2024.
- 12 ROBERTSON S, ZARAGOZA H. The probabilistic relevance framework: BM25 and beyond [J]. *Foundations and Trends® in Information Retrieval*, 2009, 3 (4): 333–389.
- 13 MIHALCEA R, TARAU P. TextRank: Bringing order into text [C] // *Proceedings of the 2004 conference on empirical methods in natural language processing*. 2004: 404–411.
- 14 ZOU L, ZHANG S, CAI H, et al. Pre-trained language model based ranking in Baidu search [C] // *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*. 2021: 4014–4022.
- 15 FAN Y, XIE X, CAI Y, et al. Pre-training methods in information retrieval [J]. *Foundations and Trends® in Information Retrieval*, 2022, 16 (3): 178–317.
- 16 HOCHREITER S, SCHMIDHUBER J. Long shortterm memory [J]. *Neural computation*, 1997, 9 (8): 1735–1780.
- 17 KIM Y. Convolutional Neural Networks for Sentence Classification [J]. *Eprint Arxiv*, 2014.
- 18 BAI J, BAI S, CHU Y, et al. Qwen technical report [J]. *arXiv preprint arXiv*: 2309. 16609, 2023.
- 19 RAJPURKAR P. Squad: 100, 000+ questions for machine comprehension of text [J]. *arXiv preprint arXiv*: 1606. 05250, 2016.

基于两阶段检索增强的信息问答方法**

张 然¹ 江 松¹ 郑明琪¹ 刘 冰¹ 张 兵¹ 陈晓慧^{1*}

摘 要 针对目前大语言模型问答在面临具体领域存在幻觉以及检索增强生成方法在海量数据上检索速率较低的问题,提出一种两阶段检索增强方法。首先使用 BERT 将文本数据集转换为固定长度的词向量;其次使用基于向量的密集检索方法将用户问题转化为语义向量,并在知识库中检索语义相近的背景信息;最后利用基于 Cross-Encoder 架构的模型对检索结果进行重排序,优先展示高质量片段并过滤掉低质量内容。实验结果表明,文章提出的两阶段检索增强方法在命中率和平均倒数排名等指标上表现更佳,可以显著提升大语言模型在问答任务中的准确性和问答效果。

关键词 大语言模型,检索增强生成技术,两阶段检索,智能问答

Two-Stage Retrieval-Augmented Generation Method for Question Answering**

ZHANG Ran¹ JIANG Song¹ ZHENG Ming-Qi LIU Bing¹
ZHANG Bing¹ CHEN Xiao-Hui^{1*}

Abstract This study proposes an two-stage retrieval-augmented generation (RAG) method aimed at mitigating the challenges of domain-specific illusions in Large Language Models (LLM) and retrieval inefficiency in current RAG-based question-answering systems. First, the textual dataset is converted into fixed-length word vectors using BERT; then, the user question is converted into semantic vectors using vector-based intensive retrieval method and semantically similar contextual information is retrieved from the knowledge base; finally, the retrieval results are re-ranked using a model based on cross-encoder architecture to prioritise the display of high-quality snippets and filter out the low-quality content. Experimental results show that the two-stage RAG method proposed in this study performs better in indicators such as hit rate and average reciprocal, which can significantly improve the accuracy and question answering effect of LLM in question answering tasks.

Key words large language model, retrieval-augmented generation, two-stage retriever, intelligent question answering

** 国家自然科学基金 (42371438) 资助

** Supported by National Natural Science Foundation of China (42371438)

* 通讯作者

1. 信息工程大学

1. Information Engineering University

0 引言

随着信息技术的快速发展，数据规模呈现出指数级增长。在信息语义检索任务中，如何从海量数据中更准确、快速地获取到有用的知识成为主要挑战。现有的引擎搜索和数据库搜索方法虽然在一定程度上提升了检索效率，但由于这些方法主要使用关键词进行匹配，面对复杂查询或需要深入理解语义内容的问题往往效果有限。此外，现有的语义检索方法无法高效地实现语义理解和问答总结。这些局限性进一步降低了模型知识获取的效率，且无法充分利用检索到的知识。

自然语言处理技术的发展为智能问答带来了新的可能性。大语言模型（Large Language Model, LLM）能够更有效、准确地理解人类提出的复杂语义问题，为智能问答和文本生成提供了新的技术支持。然而，由于模型自身解码器技术的架构，生成的结果可能存在幻觉和误差。

为了减少幻觉现象并且提供模型回答的参考依据，现有研究多通过融合外部知识来提升模型回答的准确性和真实性，进一步为生成式大模型提供检索增强的事实引导。其中，检索增强生成（Retrieval-Augmented Generation, RAG）方法的研究进展尤为迅速，如自我反思学习检索、重排序模型、前瞻性主动检索增强生成、系统到注意力等方法。检索增强生成方法通过在外部知识数据库检索用户查询内容，较好地解决了 LLM 在实现问答时所表现出的时效性不足、数据安全、出现幻觉等问题。

基于 LLM 的检索增强方法是实现本地知识库问答的关键，但随着本地知识库文档数量的增加，如何精准快速地检索出与

问题相关的文档成为亟须解决的关键问题。为了提升知识检索准确性和检索速率，本文提出一种基于 BCEmbedding（Bilingual and Crosslingual Embedding）内容重排序模型的两阶段检索增强方法。在第一阶段使用向量的密集检索方法，对用户问题和知识库语料进行语义向量提取，然后搜索和用户问题语义相近的背景信息；在第二阶段基于 Cross-Encoder 架构，将正确相关片段尽可能排在靠前位置，并过滤掉低质量的片段。

为验证本文方法的有效性，以公开爬取的能源文本为数据集与其他模型进行对比。实验结果表明，本文提出两阶段检索增强的信息问答方法在命中率（Hit_Rate, HR）和平均倒数排名（Mean Reciprocal Rank, MRR）两个指标上效果更好。通过使用 RAGAS 开源框架进行测评，证明了使用两阶段检索增强方法的大语言模型相较于单阶段大语言模型在综合得分、上下文精度、忠实度和答案相关性上得分更高。

1 相关工作

1.1 基于大语言模型的问答系统

莫拉（Molla）^[1]将问答系统（Question and Answering, QA）定义为一个能回答任意自然语言形式问题的自动机。通过输入自然语言形式的问题后，系统会输出一个简洁的答案或者可能答案的列表。问答系统主要有两种形式：基于知识库的问答和基于文本的问答。

第一种形式为基于知识库的问答系统（Knowledge Base Question Answering, KBQA），其核心是以三元组形式来组织和表示结构化的知识^[2-6]。传统的基于知识库的问答系统对于简单问题的回答可以达

到很好的效果，但对于复杂问题时处理能力十分有限。

第二种形式为基于文本的问答^[7-8] (Text - based Question Answering, TextQA)。TextQA 在处理复杂问题时相对于基于知识库的问答效果更好，其核心是语义解析，无论是问题的语义解析，还是模型训练过程中对于训练集的解析都会直接影响 TextQA 的问答效果。所以在面临复杂的自然语言问题时，TextQA 会出现准确率不高、通用性不强等问题。

随着 LLM 的兴起，智能问答领域经历了显著的技术进步和变革。LLM 以数十亿以上的参数为基础，采用自监督或半监督

学习方法，在大规模未标记文本上进行训练，从而具备了广泛的通用能力，能够有效地执行文本摘要、翻译以及情感分析等多种自然语言处理任务。基于大语言模型的问答系统可以更为高效、准确地理解人类提出的复杂语义问题，并且支持多源异构知识表达和多轮语义交互，可以实现更为智能化的问答体验。

由于 LLM^[9] 非常契合自然语言处理的需求，Fastgpt、Langchain-ChatChat、quivr、DB-GPT 以及 anything-llm 等智能问答框架逐渐兴起，加速了基于 LLM 的智能问答技术的发展。当前国内外常见的开源大模型如表 1 所示。

表 1 国内外常见的开源大模型

名称	发布主体	参数规模 (B)	训练数据
ChatGLM2	清华大学	6/12/32/66/130	6B 级别训练数据为 1.4TB 中英标识符的预训练，中英文比约为 1 : 1
Llama ^[10]	Meta	7/13/33/65	Github、Wikipedia、Books、ArXiv、StackEx chang 等近 4.7TB 数据
Flan T5 ^[11]	Google	0.06/0.22 /0.77/3/11	使用了超过 1800 个不同类型的 NLP 任务进行微调，包括问答、文本生成、文本分类、文本摘要等
PaLM ^[12]	Google	8/62/540	使用了公开可用的文本数据集，其中包括 Wikipedia、Books2TB 等，以及多种编程语言的源代码，共计 7800 亿标记

LLM 显著简化了传统自然语言处理任务，并且在解决复杂任务时展现出强大的自然语言理解能力。如 Wei^[13] 提出了基于 LLM 的信息抽取模型 ChatIE，该模型使用了思维链^[14] 以及上下文学习^[15]，在多个数据集上超过了传统监督模型的性能。

尽管 LLM 因其 Transformer 架构实现了长文本的有效处理，但这种结构仍然存在一些潜在问题。在处理未见过的问题时，LLM 可能会产生幻觉现象^[16]，这包括生成与现有知识源相冲突的信息（内在幻觉）或生成无法通过现有知识源验证的信息（外部幻觉）。这种现象的存在，限制了 LLM 在知识准确性和可靠性方面的应用。

为了解决上述问题，多种解决方案被提出，如 Tree of Thoughts^[17]、Graph - of- Thought^[18]、Chain - of- Thought 和 Program of Thoughts^[19] 等。这些方法在一定程度上减轻了幻觉现象，但仍存在发生事实错误的风险。为了有效应对 LLM 在处理未知问题时可能出现的幻觉现象，将知识库与基于 LLM 的智能问答进行结合，使用知识库提供的丰富、准确的知识信息可以提高问答的准确性和可靠性。

1.2 信息检索增强生成方法

LLM 已经在各个领域得到了广泛应用，但当涉及专业场景或行业细分等垂直

领域时，LLM 往往会遇到专业知识的局限性和数据安全的挑战。这些问题凸显了通用 LLM 在特定领域的局限性，尤其是在需要深入行业知识和数据保护的情况下。面对这些挑战，传统的解决方案如后训练或有监督微调（Supervised Finetuning, SFT）策略，虽然能够提供一定程度的改进，但往往伴随着高昂的成本和资源投入。在这一背景下，MetaAI^[20] 提出的检索增强生成方法成为更好的选择。

检索增强通过结合外部知识库和先进的信息检索机制为 LLM 提供了一种更为精准和可靠的信息生成途径。检索增强技术由文档检索器和大语言模型两部分组成，文档检索器负责从大量文档中找到与输入问题相关的信息，主要使用语义搜索技术来识别和检索相关数据。大语言模型则根据文档检索器检索到的信息生成对输入问

题的回答，图 1 为检索增强的一般实现流程。

提高 RAG 的信息检索效果主要分为五种方法^[20]，向量化存储索引、层次索引、假设问题和 HyDE、检索词块上下文丰富和融合检索。向量化存储索引^[21]将在知识源获取的数据转化为向量化内容从而快速准确地检索出相关内容。层次索引^[22-23]需要先通过摘要索引筛选出相关文档后，再在相关组内进行进一步搜索。

假设问题是利用大语言模型为每个块生成一个问题，并将这些问题嵌入向量中，在运行时针对该问题向量索引进行查询搜索（在索引中用问题向量替换块向量），然后在检索后路由到原始文本块，并将它们作为上下文发送给大语言模型以获得答案，如图 2 所示。这种方法通过查询与假设性问题之间更高的语义相似性，

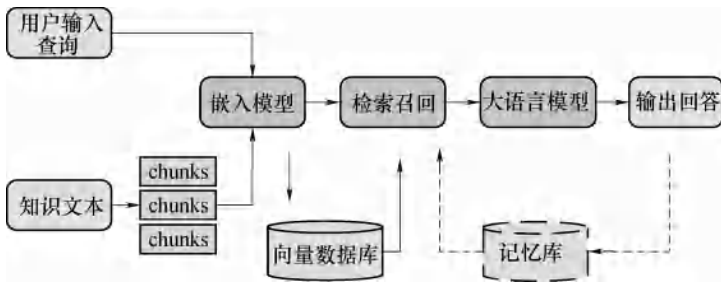


图 1 检索增强流程

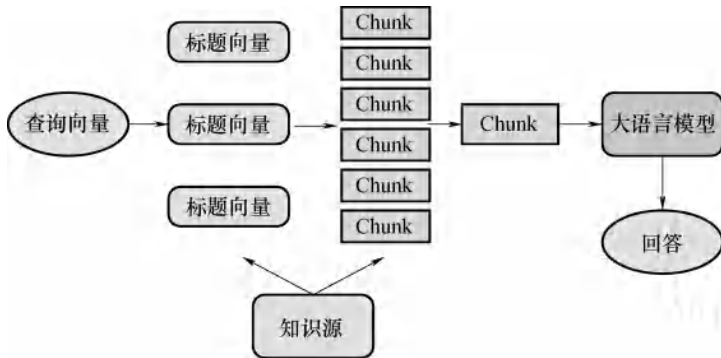


图 2 层次索引流程图

提高了搜索质量。相比于假设问题方法, HyDE^[24]是一种逆向逻辑方法, 该方法使用参数量较小的 LLM 生成假设性回复后, 利用回复向量和查询向量来提高检索质量。

检索词块上下文丰富方法为了在检索较小的词块时获得更好的搜索质量, 整合了词块周围的上下文信息, 从而为 LLM 提供更好的推理基础。如 Lee 等^[25]提出一种上下文稀疏表示方法, 该方法能够捕捉到检索词块的上下文信息, 从而使问答系统能够更好地理解用户的查询意图, 并从大量文档中检索出与查询语义相关性更强的信息。

融合检索方法将基于关键字的传统搜索和基于语义的向量搜索相结合, 将生成的结果集合作为大语言模型的提示词。该方法的核心挑战是如何更好地整合具有不同相似性得分的检索结果。为应对该挑战, 倒数排名融合方法、基于图的融合方法以及多模态融合方法被广泛研究, 如图 3 所示。

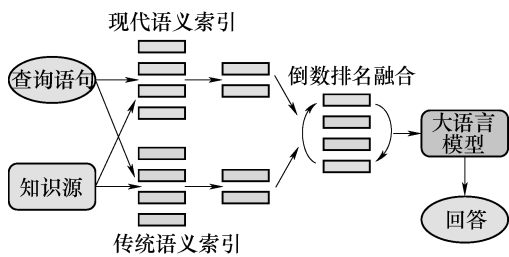


图 3 融合检索流程图

RAG 方法可以避免在解决特定任务时的大 LLM 重训练问题, 还能利用外部数据库持续更新数据并进行离线存储。这种优势很好地解决了 LLM 在实现问答时可能出现的时效性不足以及数据安全等问题。通过整合外部数据, RAG 方法通常能够在专业性强的问题上取得更好的效果。

2 基于两阶段检索增强的信息问答方法

2.1 数据预处理

由于本研究使用的数据为公开渠道爬取的各类能源相关文本数据, 鉴于 TXT 文件更易于解析、导入、自动化处理和存储。因此, 对于收集到的 PDF 数据, 需要进行光学字符识别处理 (Optical Character Recognition, OCR), 然后使用 pdfminer 库将所有 PDF 文件转化为同名 TXT 文件, 最终实现数据的整合与转换。

2.2 数据向量化存储

2.2.1 文本分块

经过数据预处理后, 文档加载器需要对文档知识源做切分操作, 得到大语言模型处理数据的最小单元文本块 chunk。chunk 的大小会对模型检索及问答效果有极大的影响, 文本块太小会造成上下文信息的大量丢失, 反之则会导致模型的检索精度下降。因此, 设置合理的文本块对于保证整个问答系统的效果至关重要。

本研究使用基于 Token 标记切割的文本分块策略。为了找到合理的 chunk_size, 本研究通过设置不同 chunk_size 和 chunk_overlap 的阈值, 采用相同的相似度搜索方式进行对比实验, 以模型召回率和问答准确率作为最终评判标准, 实验结果如图 4 所示。

对测试实验结果进行分析后发现, 词块召回率随 chunk_size 的增大而减小, 当 chunk_overlap 越小, 召回率减小的速度越快。问答准确性随 chunk_size 的增大, 先增大后减小。极值点在 chunk_size 为 400 与 450 之间, 当 chunk_overlap 为 40 时,

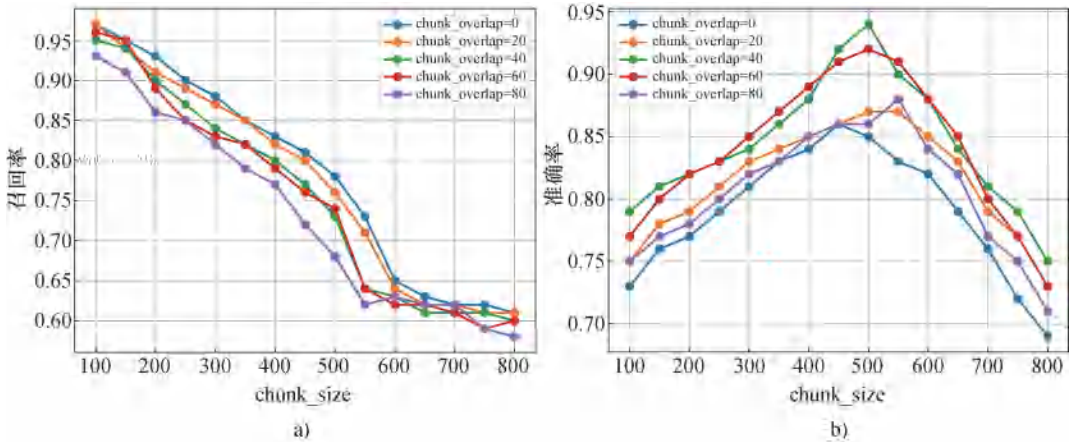


图4 不同 chunk_size 和 chunk_overlap 实验结果

a) 词块召回率随 chunk_size 变化趋势; b) 问答准确率随 chunk_size 变化趋势

准确率表现最佳。因此，将系统文本分块参数 chunk_size 的阈值设置为 400，chunk_overlap 设置为 40。

2.2.2 词向量嵌入

词向量嵌入指的是词语转换为连续向量表示，是计算机理解和处理自然语言的基础。本研究基于 Milvus 向量数据库对大模型产生的嵌入向量进行存储、索引和管理。

Milvus 向量数据库相比于其他向量数据库具有明显优势，首先，Milvus 向量数据库是一个开源的向量数据库，对于数据保密安全有所保障；其次，Milvus 向量数据库能对不同业务的向量进行隔离，达到分开存储的目的，这与本研究基于多知识库检索问答的需求相契合。Milvus 向量数据库词嵌入框架流程如图 5 所示。

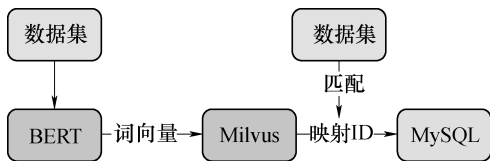


图5 Milvus 实现词嵌入的框架流程

首先使用 BERT 将文本数据集转换为固定长度的词向量，其次使用 Milvus 作为

向量数据库进行存储，最后使用 MySQL 将 Milvus 生成的向量 id 映射到文本数据，实现知识库数据的词嵌入和向量化存储。

2.3 基于 LLM 的语义信息检索与问答

2.3.1 语义信息检索

将用户检索查询语句转变为词向量后，本研究采用基于 Milvus 的近似最近邻搜索算法 (ANNS) 来完成查询语句的语义信息检索。近似最近邻搜索算法相对于精确检索，不再局限于返回最准确的结果，在可接受的范围内，只搜索目标的邻居，通过牺牲准确性来提高检索效率。

在知识库的词向量空间中，随机选择两个点后，以其中垂线来切分整个词向量空间，由此整个词向量空间被分为两部分。而后在两个空间中再选出两个顶点，再用中垂线进行切分，整个词向量空间被分为四部分。直到每一个平面区域最多只有 K 个点为止。

将用户查询语句作为一个新的词向量数据点，通过二叉树检索可以找到该词向

量数据点所在子平面,若子平面中数据点大于等于 K 个,则返回该子平面内距离查询语句词向量最近的 K 个词向量数据点,若小于 K 个,则可以使用优先队列策略,将多棵树放入优先队列,逐一比较距离,返回前 K 个词向量数据点。

2.3.2 基于 LLM 的智能问答

将用户问题和检索到的文档信息按照提示模版输入已有开源模型中得到相应的输出回答。James^[26] 针对评估大模型检索增强生成问答技术提出了一个无参考评估的框架 RAGAS,该框架能够评估检索系统识别相关和重点上下文段落的能力、LLM 以忠实方式利用这些段落的能力,以及生成本身的质量。根据该框架,以本地中文文献的文档数据为测试数据集进行效果评估。

2.4 基于内容重排序模型的检索增强生成

2.4.1 基于内容重排序的两阶段语义检索器

检索模块在 RAG 中扮演着至关重要的角色,它对问答系统的正确率和用户体验有着显著的影响。一个优秀的检索器在检索过程中应尽可能召回与用户问题相关的文本片段,将片段中相关度高、有助于解答的片段排在前列,并且实现低质量文本片段的过滤。

为了提高检索精度,保证文档效果,本文提出一种基于内容重排序的两阶段检索器。如图 6 所示,两阶段检索包含检索和重排两个阶段,能够很好地平衡检索性能和效率。

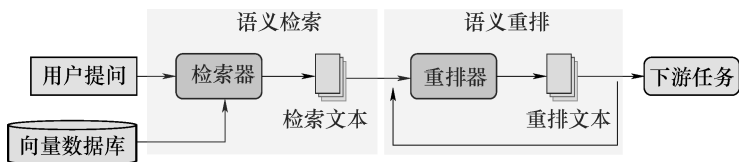


图 6 两阶段检索流程图

在检索阶段采用基于向量的密集检索方法,将用户查询语句提取语义信息后向量化处理作为向导,在选定知识库中进行检索匹配。在召回阶段中选择 dual-encoder 架构的 Embedding 模型,如图 7 所示。使用 dual-encoder 架构的 Embedding 模型可以一次性对知识库中所有文本生成 Embedding 并建立索引存储。在处理用户查询时,无须再进行词嵌入的推理,因此,节省了大量时间开销。这种优化策略确保了在处理千万级别的检索库时能够保持快速的检索速度。

在重排阶段,针对检索阶段初步检索到的信息内容进行重新排序,将价值更高的片段排在前面,同时过滤掉价值较低的

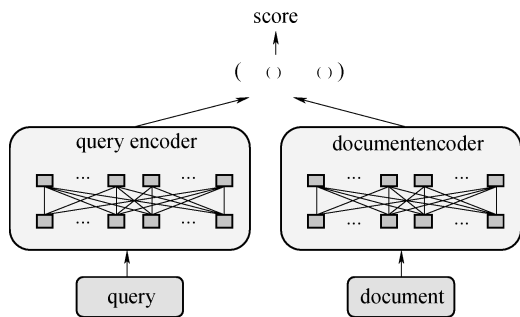


图 7 dual-encoder 架构示意图

文本片段,是提高信息检索效果的重要策略。为了解决信息交互的问题,使用 cross-encoder 架构的 Reranker 模型。cross-encoder 架构如图 8 所示。

Reranker 模型针对不同用户查询的

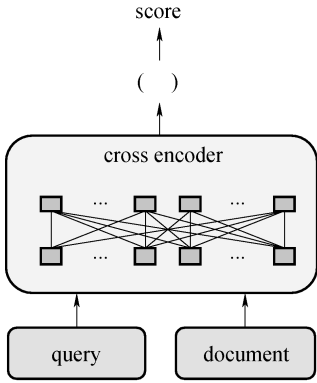


图 8 cross-encoder 架构示意图

query, 需要反复计算信息内容的词嵌入, 然后进行综合评分排序。这种模型能够实现用户查询语句和知识库语料的信息交互, 更准确地识别和提取语义关系。然而, 由于需要频繁计算词嵌入和进行综合评分, Reranker 模型计算效率相对较低, 一般只适用于千级别的数据规模。

两阶段检索方法在检索阶段能够快速定位与用户问题相关的文本片段, 而重排阶段则能够确保将正确相关的片段尽可能排在靠前位置, 并过滤掉低质量的片段, 最终实现平衡检索效果和效率的有效平衡。

2.4.2 基于 BCEmbedding 的内容重排序模型

为了提高两阶段检索增强方法的效果, 本研究采用了国产开源的 BCEmbedding 模型。该模型具备中英双语的跨语种检索能力, 其训练数据涵盖了中英双语和跨语种数据集, 同时训练数据覆盖了多个领域, 包括但不限于教育、医疗、法律、金融、百科、科研论文、客服 (FAQ)、通用问答等多个场景的语料。

使用 BCEmbedding 设计两阶段检索器。在召回阶段, Embedding 模型负责尽

可能多地召回文档; 在精排阶段, Reranker 模型则负责对这些文档进行精细排序和低质量文档过滤。Embedding 模型采用了双编码器结构, 专注于将用户查询的 query 和知识库中的 passage 进行编码, 以计算它们的语义向量相似度。而 Reranker 模型则采用交叉编码器结构, 在精排阶段, 它充分利用用户查询和知识库文本的交互信息, 对召回的段落进行重新排序。

在训练 Embedding 模型的过程中, 本研究发现过于困难的负样本会对模型造成损害, 导致模型困惑, 最终影响模型性能。由于 Embedding 模型的算法性能存在一定上限, 并且许多难负样本之间差异微小且相似度高, 因此, 在训练过程中不采用难样例挖掘技术, 而是将重点放在充分利用 Embedding 模型的召回能力上, 将精细排序和低质量过滤工作留给 Reranker 模型完成。

将 Reranker 模型输出的 (query, passage) 语义相关分数用于段落的排序以及表征语义相关程度, 这样做可以更好地识别和过滤低质量的段落。在 RAG 中, 这种方法对 LLM 回答问题有着显著的帮助。通过提供更为简洁、少干扰信息的语境, 可以有效提高 LLM 的回答质量。

3 实验与结果分析

3.1 实验数据

为了测试本方法在提升 LLM 在特定领域问答方面的有效性, 以全球能源为研究背景构建相应数据集。本研究所用的数据集分为两部分, 一部分是通过网络爬虫对能源相关信息进行数据抓取, 共收集 8819

个 PDF 文档，大小为 44.4GB。另一部分是在知网、arxiv 等权威学术网站检索能源相关主题关键字，共收集 154 个 PDF 文

档，大小为 357MB。之后基于收集的能源文本数据按照图 9 的流程构建新的评测数据集 Energy_Dataset。

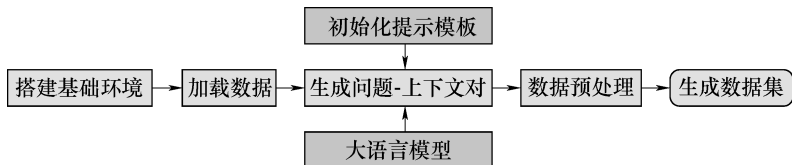


图 9 数据集构建流程图

3.2 模型对比评估

为了衡量模型的检索效率，本研究使用命中率 (Hit_rate) 和平均倒数排名 (MRR) 两个指标作为评估标准。

(1) 命中率：计算前 k 个检索出的文档中正确答案的查询比例。

(2) 平均倒数排名：通过查看每一次查询得到的最高排名的相关文档的排名来评估方法的准确性。对于每个查询，取其最高排名的倒数的平均值。

将本文所提方法与现如今已经开源的 Embedding 和 Reranker 模型进行对比分析，结果如表 2 所示。

表 2 模型检索器评测

模型	无 Reranker [hit_rate/ mrr]	bge-reranker- large [hit_ rate/mrr]	bce-reranker- base_v1 [hit_ rate/mrr]
bge-large- zh-v1.5	68.58/47.12	79.01/63.1	80.63/68.17
Jina AI-v2 -Base-zh	70.40/49.36	80.67/64.04	82.57/69.31
gte-large -zh	58.25/39.12	70.46/57.42	71.81/62.38
bce-embe- dding- base_v1	84.68/62.1	90.70/70.28	92.90/76.69

按列对比可以看出，bce-embedding-base_v1 的表现相比于其他模型具有更高的

命中率和平均倒数排名，按行对比，Reranker 模块可以显著改善检索效果。其中，bce-reranker-base_v1 具备更好的精排能力。综上，bce-embedding-base_v1 和 bce-reranker-base_v1 的组合可以实现最好的检索效果 (92.90/76.69)，比选定的最好组合 (Jina AI-v2-Base-zh + bge-reranker-large, 82.57/69.31)，hit rate 提升 10.33%，mrr 提升 7.68%。由此可以得出两阶段检索相比于单阶段检索具有更强的性能优势。

3.3 模型问答效果测试

使用本文所构建的数据集，采用 RAGAS 开源框架分别测评未应用本文所提方法的开源 LLM 与应用本文方法的开源 LLM 在问答方面的性能。为了证明本文所提方法在提升模型问答效果方面的有效性，本研究使用常见的开源模型作为基线模型进行测评，结果分别如表 3 和表 4 所示。

表 3 基础开源模型测评结果

模型	综合得分	上下文精度	忠实度	答案相关性
Qwen-chat-14B	0.856	0.813	0.888	0.870
Qwen-chat-7B	0.821	0.784	0.843	0.834
Llama2-Chinese-7B-chat-ms	0.782	0.764	0.806	0.797
Chatglm3-6B	0.804	0.786	0.813	0.810

表 4 基于两阶段检索增强的开源模型测评结果

模型	综合得分	上下文精度	忠实度	答案相关性
Qwen-chat-14B	0.892	0.847	0.923	0.912
Qwen-chat-7B	0.851	0.822	0.867	0.892
Llama2-Chinese-7B-chat-ms	0.803	0.780	0.833	0.855
Chatglm3-6B	0.844	0.821	0.852	0.874

通过分析表 3 可知,在开源 LLM 中,Qwen-chat-14B 模型在综合得分、上下文精度、忠实度以及答案相关性评估指标上表现均优于其他开源模。通过对比表 3 和表 2 中同一模型在使用两阶段检索增强后的得分可以看出,两阶段检索增强方法在提升模型问答效果方面发挥了显著作用。其中,Qwen-chat-14B 在 4 个指标上分别提升了 0.036、0.034、0.0350 和 0.0412;QWen-chat-7B 在 4 个指标上分别提升 0.030、0.038、0.024 和 0.058;Llama2-Chinese-7B-chat-ms 在 4 个指标上分别提升了 0.021、0.016、0.027 和 0.058;Chatglm3-6B 在 4 个指标上分别提升 0.040、0.035、0.039 和 0.064。基于两阶段检索增强的信息问答方法将知识库和 LLM 问答结合,显著提升了模型在综合得分、上下文精度、忠实度和答案相关性指标上的得分,通过增加上下文知识以及优化检索策略,不仅提高了模型回答的准确性和可靠性,并且有效降低了模型生成虚假信息倾向,验证了该方法在减少幻觉现象方面的潜力。实验结果证明了两阶段检索对于提升 LLM 问答效果的有效性。

4 结束语

本研究提出了一种两阶段检索增强的方法,基于国产开源 BCEmbedding 模型构

建了一种内容重排序模型。为验证本文方法的有效性,以全球能源公开数据为基础构建了新的评测数据集 Energy_Dataset,验证了两阶段检索对于检索增强生成优化的可行性。最终通过 RAGAS 评测进一步验证两阶段检索的优势。

考虑到本研究所使用的数据集只涵盖文档数据,数据结构较为单一,在未来工作中,可以进一步尝试基于多模态检索增强的生成技术,利用多模态数据的全面性和相互印证性,进一步优化检索增强生成的智能问答效果。

参考文献

- MOLLA D, VICEDO J L. Question Answering in Restricted Domains: An Overview. [J]. Computational Linguistics, 2007, 33 (1): 41-61.
- LEHMANN J, ISELE R, JAKOB M, et al. DBpedia—a large-scale, multilingual knowledge base extracted from Wikipedia [J]. Semantic Web, 2015, 6 (2): 167-195.
- BOLLACKER K, EVANS C, PARITOSH P, et al. Freebase: A collaboratively created graph database for structuring human knowledge [C] // Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD). Canada: ACM, 2008: 1247-1250.
- PELLISSIER T T, VRANDE I D, SCHAFFERT S, et al. From Freebase to Wikidata: The Great Migration [C] // Proceedings of the International World Wide Web Conference (WWW). Canada: ACM, 2016: 1419-1428.
- SAURABH S. BRING rich knowledge of people, places, things and local businesses to your apps [EB/OL]. <https://blogs.bing.com/search-qualityinsights/2017-07/bring-rich-knowledge-of-peopleplaces-things-andlocal-businesses-to-your-apps>.
- NOY N F, GAO Y, JAIN A, et al. Industry-scale Knowledge Graphs: Lessons and Challenges

- [J]. *ACM Queue*, 2019, 17 (2): 20.
- 7 BORDES A, CHOPRA S, WESTON J. Question answering with subgraph embeddings [C] // *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing*. Doha: Association for Computational Linguistics, 2014: 615–620.
 - 8 CHEN B, SUN L, HAN XP. Sequence-to-Action; End-to-end semantic graph generation for semantic parsing [C] // *Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics*. Melbourne: ACL, 2018: 766–777.
 - 9 VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need [J]. *Advances in neural information processing systems*, 2017, 30.
 - 10 TOUVRON H, LAVRIL T, IZACARD G, et al. Llama: Open and efficient foundation language models [J]. *arXiv preprint arXiv: 2302.13971*, 2023.
 - 11 CHUNG H W, HOU L, LONGPRE S, et al. Scaling instruction-finetuned language models [J]. *Journal of Machine Learning Research*, 2024, 25 (70): 1–53.
 - 12 CHOWDHERY A, NARANG S, DEVLIN J, et al. Palm: Scaling language modeling with pathways [J]. *Journal of Machine Learning Research*, 2023, 24 (240): 1–113.
 - 13 WEI X, CUI XY, CHENG N, et al. Zero-shot information extraction via chatting with chatgpt [J]. *arXiv: 2302.10205*, 2023.
 - 14 WEI J, WANG X, SCHUURMANS D, et al. Chain-of-thought prompting elicits reasoning in large language models [C] // *Advances in Neural Information Processing Systems*. Curran Associates, Inc, 2022: 24824–24837.
 - 15 BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners [C] // *Advances in Neural Information Processing Systems*. Curran Associates, Inc, 2020: 1877–1901.
 - 16 SEAN W, ILIA K, STEPHENR, et al. Neural text generation with unlikelihood training [C] // *International Conference on Learning Representations*. Addis Ababa: OpenReview. net; 2020.
 - 17 SHUNYU Y, DIAN Y, JEFFREYZ, et al. Tree of thoughts: Deliberate problem solving with large language models [J]. *arXiv: 2305.10601*, 2023.
 - 18 YAO Y, LI Z C, ZHAO H. Beyond Chain-of-Thought, Effective Graph-of-Thought Reasoning in Large Language Models [J]. *arXiv: 2305.16582*, 2023.
 - 19 WENHU C, XUEGUANG M, XINYIW, et al. Program of thoughts prompting: Disentangling computation from reasoning for numerical reasoning tasks [J]. *arXiv preprint arXiv: 2211.12588*, 2022.
 - 20 GAO Y F, XIONG Y, GAO X, et al. Retrieval-augmented generation for large language models: A survey [J]. *arXiv preprint arXiv: 2312.10997*, 2023.
 - 21 ASAI A, HASHIMOTO K, HAJISHIRZI H, et al. Learning to Retrieve Reasoning Paths over Wikipedia Graph for Question Answering [C] // *International Conference on Learning Representations*. 2020.
 - 22 HOSKING, TOM, HAO T, et al. Hierarchical Indexing for Retrieval-Augmented Opinion Summarization [J]. *arXiv preprint arXiv: 2403.00435*, 2024.
 - 23 GAO Y, XIONG Y, GAO X, et al. Retrieval-Augmented Generation for Large Language Models: A Survey [J]. *arXiv preprint arXiv: 2312.10997*, 2023.
 - 24 ERIC M S, JOHN T, SEBASTIAN R. Learning to Retrieve Reasoning Paths over Wikipedia Graph for Question Answering [J]. *arXiv preprint arXiv: 1911.10470*, 2019
 - 25 LEE, JINHYUK. Contextualized Sparse Representations for Real-Time Open-Domain Question Answering [J]. *arXiv preprint arXiv: 11911.02896*, 2020
 - 26 ES S, JAMES J, ESPINOSA-ANKE L, et al. Ragas: Automated evaluation of retrieval augmented generation [J]. *arXiv preprint arXiv: 2309.15217*, 2023.

基于模仿学习的多智能体追捕决策方法

王焱宁^{1,2} 张锋镝^{1,2} 肖登敏^{3*} 孙中奇⁴ 杜长坤⁵

摘要 针对模仿学习方法通常仅能处理质量类似的固定模态专家轨迹的问题,提出了多专家轨迹生成对抗模仿学习方法与时序差分误差行为克隆方法相结合的混合模仿学习方法。该方法可以直接用于强化学习,同时可以处理多质量的专家轨迹,训练出来的模型较少受到低质量的专家轨迹的影响。结合二维的动静结合目标追捕场景,对混合模仿学习方法进行实验验证。结果表明提出的方法可以吸收专家经验,为后续强化学习的训练提供较好的初始模型。

关键词 模仿学习, 多智能体, 智能决策, 行为克隆

The Multi-Agent Pursuit Decision-Making Method Based on Imitation Learning

WANG Yan-Ning^{1,2} ZHANG Feng-Di^{1,2} XIAO Deng-Min^{3*} SUN Zhong-Qi⁴ DU Chang-Kun⁵

Abstract Addressing the issue that imitation learning methods are typically only capable of processing fixed-modal expert trajectories of similar quality, a hybrid imitation learning method combining multi-expert trajectory generative adversarial imitation learning and temporal difference error behavior cloning is proposed. This method can be directly applied to reinforcement learning and handle expert trajectories of varying quality. Experimental validation of the hybrid imitation learning method is conducted in a 2D combination of static and dynamic target pursuit scenario. The results show that the proposed method can effectively absorb expert experience, providing a good initial model for subsequent reinforcement learning training.

Key words imitation learning, multi-agent, intelligent decision making, behavioral cloning

0 引言

多智能体系统是研究利益不同的智能

体间合作与竞争的理想模型。通过设计合适的合作或竞争机制,多智能体系统能够灵活应对各种复杂环境并共同完成特定任务。在军事战略、工业自动化、机器人等

* 通讯作者

1. 北京航天自动控制研究所 2. 宇航智能控制技术全国重点实验室 3. 中船智海创新研究院有限公司 4. 北京理工大学 5. 中国航天科工集团智能科技研究院

1. Beijing Aerospace Automatic Control Institute 2. National Key Laboratory of Science and Technology on Aerospace Intelligence Control 3. China Ship Intelligence and Marine Innovation Research Institute Co., Ltd 4. Beijing Institute of Technology 5. China Aerospace Science and Industry Corporation Intelligent Technology Research Institute

众多领域中,多智能体系统的研究和应用越来越广泛^[1-2],研究的重要性和潜在价值日益凸显。

在多智能体系统的研究领域,多智能体追捕问题是一个典型问题,具有重要的研究价值。追捕过程中环境是时刻变化的,每个智能体需要获取环境的实时信息,根据实时信息及时做出变换追捕目标、重新组队等决策。因此,在不断变化的环境中,追捕问题是一个备受关注但目前尚未解决的实时知识处理问题,也是研究多智能体合作、协调以及对抗策略进化的常见问题。

1 问题的提出

在面对复杂多变的实际环境时,非学习类的方法如博弈论方法^[3]、人工势场法^[4]等往往难以做出正确且快速的反应。相比之下,强化学习方法凭借其强大的高维度信息感知、理解以及非线性处理能力,可以满足多智能体追捕问题对实时性和灵活性的要求,使得强化学习成为解决追捕问题的理想工具。

利用强化学习方法解决多智能体追捕问题也存在一些挑战。由于强化学习是无经验学习,智能体在训练过程需要不断“试错”以增长经验。在复杂环境中,采用强化学习训练的策略存在训练时间长、收敛速度慢的问题。

人类在成长过程中经常会通过模仿来学习新的技能、知识和行为方式。采用模仿学习的方法,智能体可以通过模仿专家轨迹学习到较理想的行为策略,从而可以避免不必要的试错。针对多智能体追逃问题,如果有历史数据或者专家经验为智能体提供辅助决策,将会提高智能体学习的效率。通过模仿专家示例的轨迹,智能体

可以高效地学习专家的策略,避免不必要的探索,从而缩短训练时间。

本文的主要贡献为:①提出混合模仿学习方法,可以学习多模态的专家数据;②利用多智能体追捕决策场景进行实验验证,为后续多智能体追捕问题方法研究提供思路。

2 混合模仿学习方法

模仿学习方法大致可以分为三类,分别是行为克隆方法(Behavioral Cloning, BC)^[5-6]、逆强化学习方法(Inverse Reinforcement Learning, IRL)^[7-8]和生成对抗模仿学习方法(Generative Adversarial Imitation Learning, GAIL)^[9]。鉴于模仿学习的三种主要方法BC、GAIL以及IRL各有特色,考虑到BC具有简单易实现的优点,而GAIL在模仿效果上表现突出,本文将重点对这两种方法进行深入研究,并将两种方法进行结合构成混合模仿学习方法。

2.1 TD-BC 方法

BC方法通常只能生成一个网络,无法直接用于强化学习训练。TD-BC方法在BC方法的基础上进行改进。TD-BC方法主要有生成专家模型、生成专家数据、训练学生模型三个步骤。下面具体介绍TD-BC方法的实施过程。

1. 生成专家模型

在模仿学习方法中,通常假定专家模型代表了最优策略。专家模型可以基于人为的专家经验构建成决策树的形式,也可以是通过强化学习训练得到的神经网络模型。

2. 生成专家数据

将专家模型与环境进行交互,从而得到专家数据。对于BC方法,专家数据是状

态和动作的二元组, 即 $X = \{(s_1, a_1), (s_2, a_2), \dots, (s_n, a_n)\}$ 。对于 TD-BC 方法, 专家数据是由三元组构成的, 即 $X = \{(s_1, a_1, s'_1), (s_2, a_2, s'_2), \dots, (s_n, a_n, s'_n)\}$ 。其中, s_j 表示 j 时刻的状态, a_j 表示对应的动作, s'_j 表示执行完动作 a_j 后的状态。行为克隆本质是有监督学习, 学习的样本是 s_j , 学习的标签是 a_j 。 s'_j 被用来更新价值网络。

3. 训练学生模型

为了与专家模型进行区分, 定义通过模仿学习方法得到的模型为学生模型。TD-BC 方法的学生模型包含两个网络, 一个策略网络和一个价值网络。

对于策略网络参数的更新, 目标函数为:

$$\theta^* = \arg \min_{\theta} E_{(s, a) \sim \chi} [L(\pi_{\theta}(s), a)] \quad (1)$$

式中, X 为专家数据集; L 为损失函数; s 和 a 分别为专家轨迹数据中的状态和动作; $\pi_{\theta}(s)$ 为策略网络。

如果场景是离散动作空间, 损失函数可以采用最大似然估计。反之, 如果场景是连续动作空间, 损失函数可以采用均方误差函数。由于本文研究的场景为连续动作空间, 因此采用均方误差损失函数更新策略网络。式 (1) 的损失函数 L 可以改写为:

$$L(s, a; \theta) = \frac{1}{2} [\pi_{\theta}(s) - a]^2 \quad (2)$$

采用梯度下降的方法更新策略网络的参数。训练过程中, 损失函数的数值会逐渐减小, 表明策略网络输出的决策逐渐接近专家决策。

对于价值网络参数的更新, 引入了 TD 误差的思想, 这也是 TD-BC 方法得名的原因。具体而言, 定义 TD 误差为^[10]:

$$TD_error = q(s_{i+1}, a_i; w) - q(s_i, a_i; w) \quad (3)$$

式中, $q(s, a; w)$ 为价值网络的输出, 是动作价值函数 $Q_{\pi}(s, a)$ 的估计; $q(s_{i+1}, a_i; w)$ 为下一时刻的动作价值; $q(s_i, a_i; w)$ 为当前时刻的动作价值。

定义价值网络的损失函数为:

$$critic_loss = \frac{\sum_{i=1}^{size} |q(s_i, a_i; w)(i) - TD_error(i)|}{size} \quad (4)$$

式中, $size$ 为更新网络时需要使用的样本数量, 是一个超参数。

2.2 MT-GAIL 方法

GAIL 方法通常只考虑质量相似的专家轨迹, 而 MT-GAIL 方法可以综合考虑多条质量不同的专家数据, 避免采用最差的专家数据进行训练。由于训练过程神经网络不知道哪条专家轨迹是最优的, 可以通过获取每条专家轨迹对应的判别器的准确率作为可靠度系数, 确定如何选择专家轨迹进行训练。将可靠度系数与对应判别器的输出相乘得到模仿学习奖励值, 该值存入经验池, 用于训练策略生成器。算法框架如图 1 所示。

定义三个专家的专家策略分别为 π_{E1} 、 π_{E2} 和 π_{E3} , 使用三位专家策略进行推演得到三条质量不同的专家轨迹。专家轨迹为状态和动作构成的二元组。将策略生成器与环境交互产生的智能体轨迹数据和专家轨迹都作为输入传入对应的判别器中, 在训练过程中不断更新判别器网络和策略生成器网络的参数。判别器的损失函数采用二元交叉熵损失函数, 定义为:

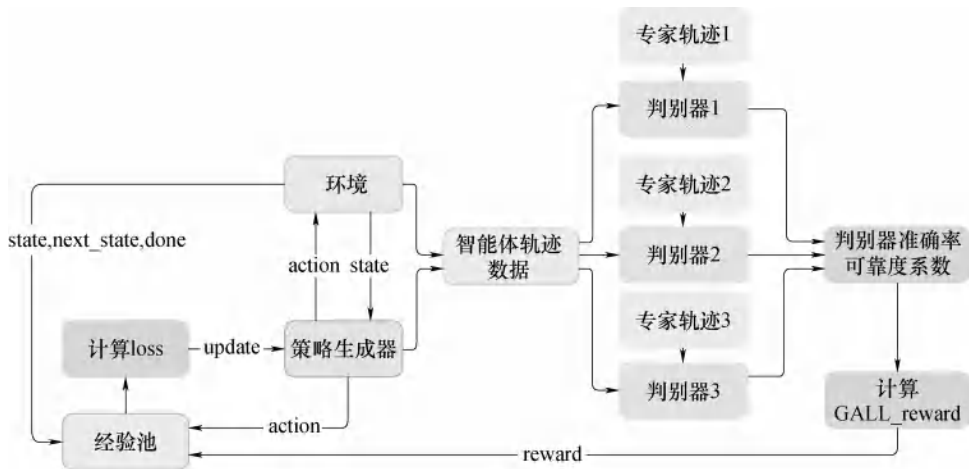


图1 MT-GAIL算法框架

$$L = \frac{\sum_i - [y_i \times \log(D_w(s, a)) + (1 - y_i) \times \log(1 - D_w(s, a))]}{N} \quad (5)$$

式中, y_i 为样本 i 的标签; 定义 1 为正样本, 0 为负样本; $D_w(s, a)$ 为判别器的输出。

在 MT-GAIL 方法中, 定义标签 1 是专家数据样本, 定义标签 0 是策略生成器产生的数据。训练判别器的目标函数为 $\min L(p_E, 1) + \min L(p_{Builder}, 0)$ 。采用梯度下降法更新判别器网络。梯度的更新公式为:

$$\hat{E}_{T_i} [\nabla_w \log(D_w(s, a))] + \hat{E}_{T_E} [\nabla_w \log(1 - D_w(s, a))] \quad (6)$$

式中, T_i 为由策略生成器产生的轨迹数据; T_E 为由专家产生的轨迹数据。

强化学习方法的奖励值通常由环境直接提供。对于模仿学习方法, 通常环境无法直接提供奖励值。考虑到判别器的作用是区分策略网络轨迹数据和专家轨迹数据, 因此, 判别器的准确率可以反馈策略网络模型的优劣。下面介绍根据判别器准

准确率计算奖励值的方法^[11]。

计算每一个判别器的专家准确率和学生准确率, 其中专家准确率用 E_acc 表示, 学生准确率用 L_acc 表示。对应的计算方法为:

$$E_acc = \hat{E}_{T_E} [D_w(s, a) > 0.5] \quad (7)$$

$$L_acc = \hat{E}_{T_i} [D_w(s, a) < 0.5]$$

将专家准确率和学生准确率相加, 得到相应判别器的总体准确率。给总体准确率较高的判别器赋予较高的权重, 给总体准确率较低的判别器赋予较低的权重。权重的计算方法为:

$$E(j)_w = \frac{acc(j)}{acc1 + acc2 + acc3} \quad (8)$$

式中, $acc1, acc2, acc3$ 分别对应判别器的总体准确率; j 为第 j 个判别器。

将判别器的输出作为奖励值的一部分, 奖励值的定义方法为:

$$\sum_{j=1}^3 [E(j)_w^* (-\log(1 - D(j)_w(s, a)))] \tag{9}$$

将环境的状态数据、策略生成器的动作数据以及奖励数据存入经验池中，采用强化学习方法更新策略生成器网络的模型

参数。

2.3 混合模仿学习方法

结合 TD-BC 方法和 MT-GAIL 方法，形成混合模仿学习方法，方法框架图如图 2 所示。

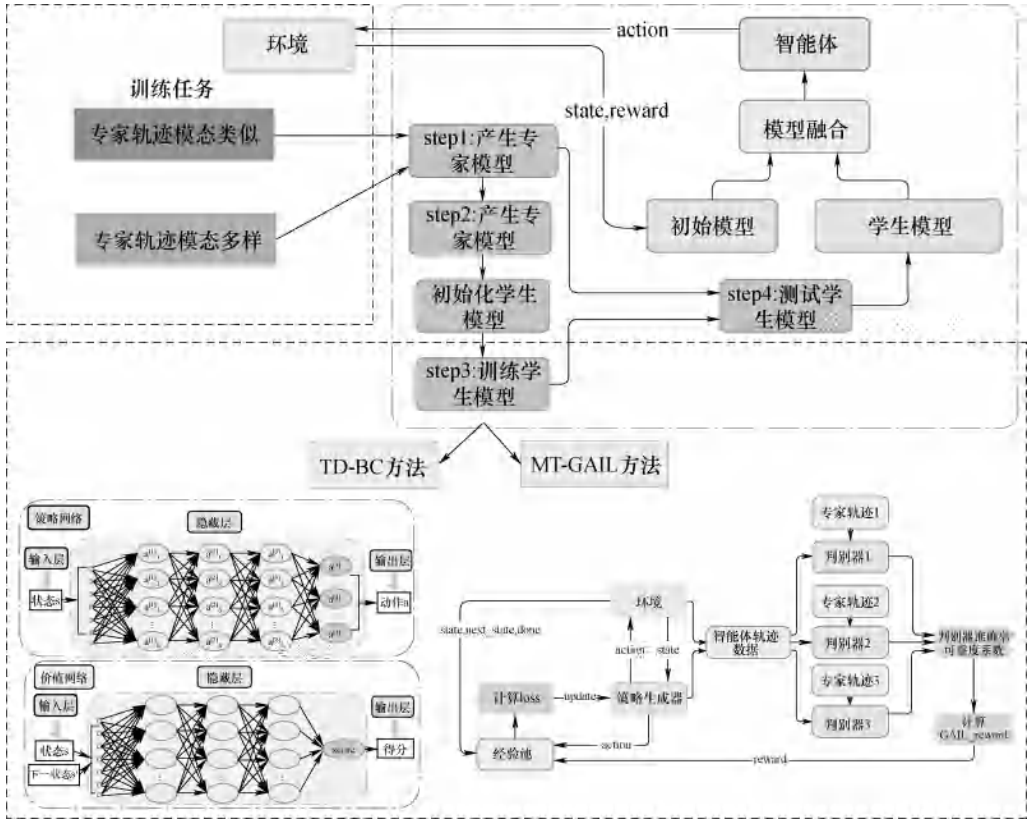


图 2 混合模仿学习方法框架图

3 实验验证

3.1 场景描述

采用混合模仿学习方法模仿智能体在二维平面内追捕动静结合目标的策略。图 3 为仿真场景示意图，图中虚线框部分表示智能体可能出现的初始位置。虚线框内的小球为我方智能体，图中浅色小球为敌

方智能体，虚线圆圈为静态目标。分布在场景中的黑色小球为障碍物。其中静态目标用于模拟实际情景中隐藏不动的敌方目标，动态目标用于模拟可移动的敌方目标。

场景中有 2 个动态目标，3 个静态目标，8 个我方智能体，而模仿学习方法只能模仿固定的策略。因此，采用模仿学习方法训练我方的追捕智能体，敌方的动态目标直接选择强化学习训练得到的较高水平的智能体。

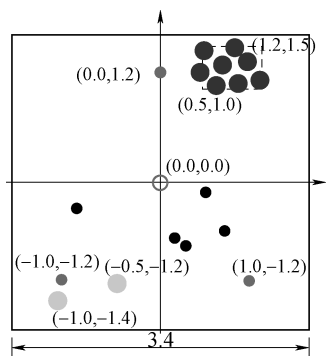


图3 用于模仿学习训练的场景示意图

表1列出了场景中实体的初始位置分布。

表1 实体初始分布情况

实体	横坐标范围	纵坐标范围
障碍物0	(0.1, 0.2)	(-0.6, -0.5)
障碍物1	(-1.0, -0.9)	(-0.3, -0.2)
障碍物2	(0.2, 0.3)	(-0.8, -0.7)
障碍物3	(0.6, 0.7)	(-0.7, -0.6)
障碍物4	(0.4, 0.5)	(-0.2, -0.1)
动态目标0	-1.0	-1.4
动态目标1	-0.5	-1.2
静态目标0	0	1.2
静态目标1	1	-1.2
静态目标2	-1	-1.2
我方智能体0	(0.5, 1.2)	(1.0, 1.5)
我方智能体1	(0.5, 1.2)	(1.0, 1.5)
我方智能体2	(0.5, 1.2)	(1.0, 1.5)
我方智能体3	(0.5, 1.2)	(1.0, 1.5)
我方智能体4	(0.5, 1.2)	(1.0, 1.5)
我方智能体5	(0.5, 1.2)	(1.0, 1.5)
我方智能体6	(0.5, 1.2)	(1.0, 1.5)
我方智能体7	(0.5, 1.2)	(1.0, 1.5)

如图4所示，采用混合模仿学习方法训练含有动静目标的复杂追捕场景。采用TD-BC方法学习我方智能体追捕静态目标的策略，采用MT-GAIL方法学习智能体

追捕动态目标的策略。将学到的模型赋给对应的智能体进行推演。从追捕静态目标的智能体中依次选取智能体模型进行推演得到专家数据，用于TD-BC训练，从追捕动态目标的智能体中选取三个模型进行推演得到专家数据，用于MT-GAIL训练。最终将训练得到的模型赋予对应的我方智能体，从而实现较快学习到追捕动静结合目标的经验。

3.2 收集专家数据

由于场景中我方智能体的初始位置是不固定的，为了使得经过模仿学习训练得到的智能体在不同的初始位置都可以追捕到敌方智能体，需要积累多条专家数据。下面分别介绍MT-GAIL方法和TD-BC方法获取专家数据的过程。

1. MT-GAIL方法获取专家数据

考虑到我方智能体的初始位置分布一致，针对敌方目标以及障碍物的策略也一致，因此，可以认为我方的追捕动态目标的智能体是等价的。场景中追捕动态目标的智能体共有5个，智能体的ID分别为agent3、agent4、agent5、agent6、agent7。不同智能体的决策质量并不相同，从而可以认为利用不同智能体得到专家数据的质量是不同的。因此，可以采用MT-GAIL方法模仿学习不同质量的专家数据，使得学习得到的模型尽可能与高质量的专家策略类似，同时避免受到低质量的专家数据的影响。

结合场景推演50轮，记录不同智能体的环境奖励值。通过环境奖励值评价智能体（专家模型），最终选择其中三个智能体的策略用于MT-GAIL训练。

推演过程的环境奖励值结果如图5所示。图5a为智能体推演过程每轮的环境奖励值，图5b为智能体的累计平均环境奖励值。

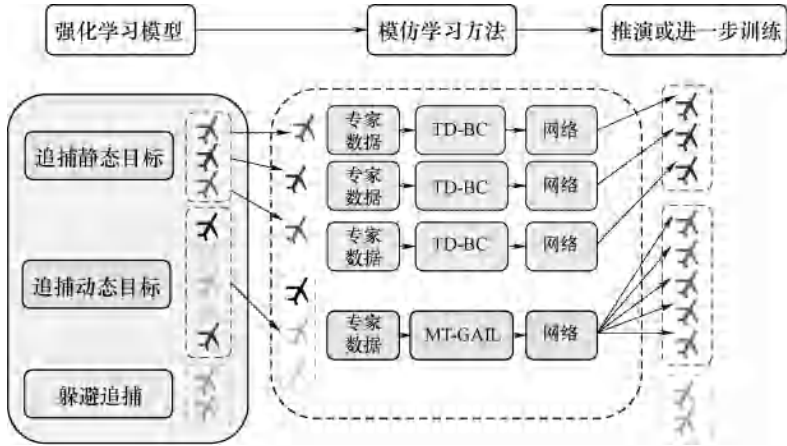


图4 基于混合模仿学习方法训练智能体的框架图

可以看出 agent 5 整体表现良好，具有最高的累计环境平均奖励值。agent 6 整体表现中庸。agent 4 整体表现最差，推演 50 轮的累计平均环境奖励值最低。选择上述三个智能体作为专家策略，与环境进行推演得到专家数据。在推演的 50 轮中，每轮的数据为 200 步，对于同一个智能体，每步的数据为状态空间 36 维，动作空间 5

维。由于专家数据不需要区分轮数，因此，将每一轮得到的状态数据和动作数据进行拼接，得到 10000 组专家数据。最终形成三个专家文件，每个文件中包含拼接好的 10000 组专家轨迹数据。

2. TD-BC 方法获取专家数据

由于场景中追捕静态目标的智能体不是等价的，所以追捕静态目标的三个智能

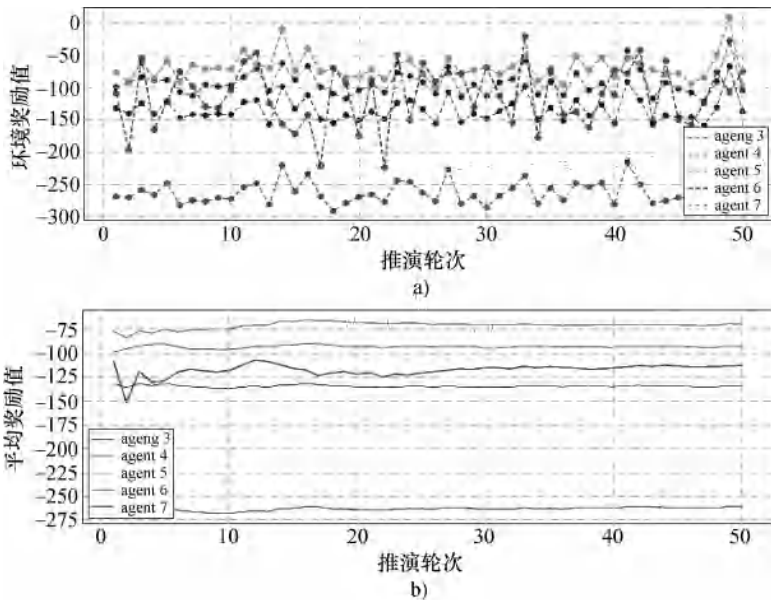


图5 推演过程智能体的环境奖励值

a) 智能体每轮环境奖励值；b) 智能体平均环境奖励值

体需要单独训练。基于每个智能体获取专家数据的方法为：基于强化学习模型结合场景推演 50 轮，每轮的数据为 200 步。对于每一个智能体，每步的数据为状态空间 36 维，动作空间 5 维，下一时刻的状态空间 36 维。由于专家数据不需要区分轮数，因此，将每一轮得到的对应数据进行拼接，得到 10000 组专家数据。最终形成三个文件，分别用于存储状态数据、动作数据和下一时刻的状态数据。每个文件都包含 10000 组数据。针对 agent 0、agent 1、agent 2 分别采用上述方法获取专家数据，用于 TD-BC 训练。

3.3 算法训练结果

1. MT-GAIL 方法训练效果

利用专家数据采用 MT-GAIL 方法进

行训练，累计训练 300 轮，得到智能体网络模型和判别器网络模型。

训练过程的损失曲线如图 6 所示。可以看出，训练过程中网络的损失逐渐减小到 0，表明学生模型的策略与专家经验基本吻合。智能体的 critic 网络的损失值也在允许的范围内，仅需要通过后续强化学习训练就可以使得网络的损失减小到 0。

2. TD-BC 方法训练结果

利用专家数据采用 TD-BC 方法训练，累计训练 20000 轮，得到学生模型。训练过程不同智能体的曲线如图 7 所示。可以看出，训练过程中价值网络和策略网络的损失逐渐减小到 0，表明学生模型的策略与专家经验基本吻合。

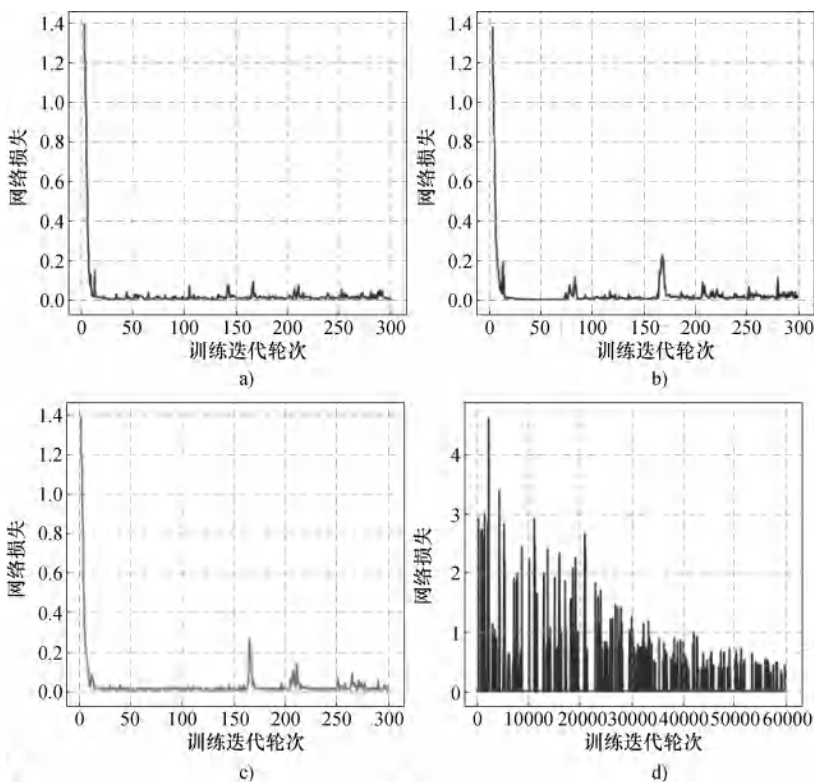


图 6 追捕动态目标训练过程网络损失值变化情况

a) 判别器 0 网络损失；b) 判别器 1 网络损失；c) 判别器 3 网络损失；d) 价值网络损失

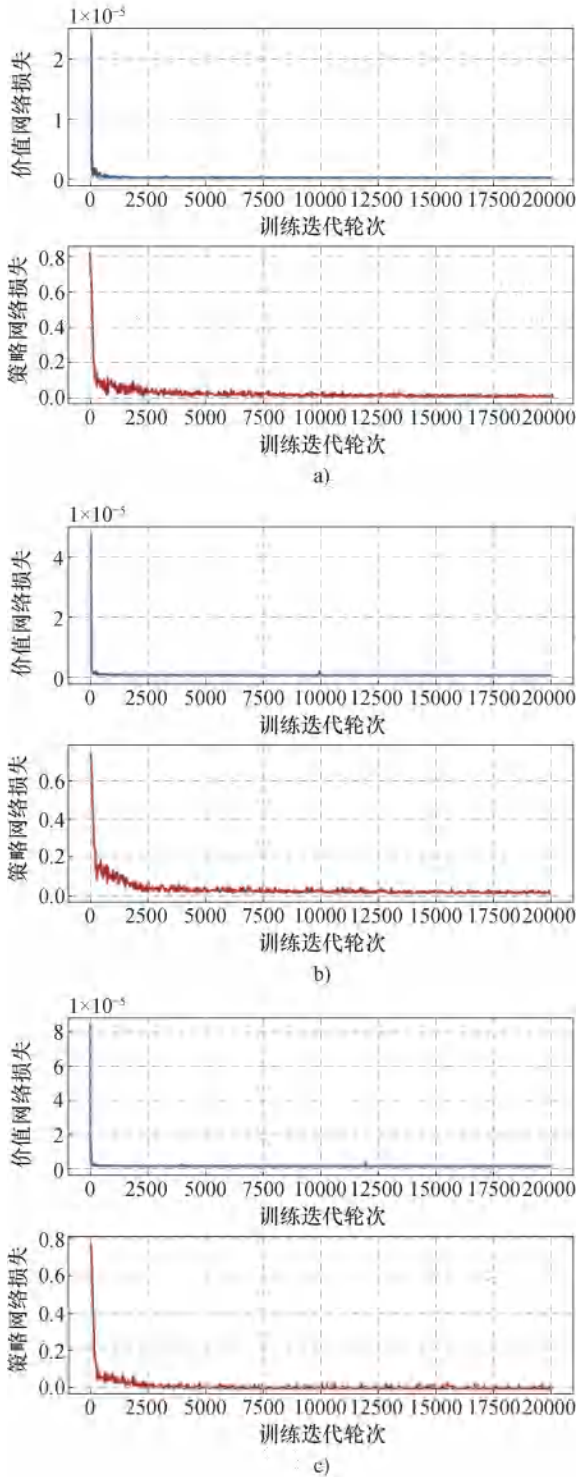


图7 追捕静态目标训练过程网络损失值变化情况

a) 智能体 0 网络损失值; b) 智能体 1 网络损失值; c) 智能体 2 网络损失值

3. 推演效果

在加载了 TD-BC 和 MT-GAIL 方法得到的学生模型后, 将其与环境进行交互, 生成推演的可视化效果, 如图 8 所示。从图中可以观察到, 通过采用模仿学习方法, 智能体已经初步展现出了追捕静态目标和动态目标的能力。这充分证明了模仿学习方法在快速学习专家经验方面的有效性, 使得智能体能够在短时间内学习到基本的追捕技巧。在推演过程中, 智能体有时会出现超出边界的问题。这表明虽然模仿学习方法能够帮助智能体学习到基本的追捕经验, 但其在处理一些复杂或特殊情况时, 还存在一定的局限性。因此, 需要进一步使用强化学习方法对智能体进行训练, 以优化其行为策略, 并减少超出边界等问题的发生。

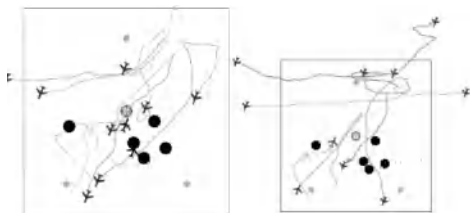


图 8 推演过程可视化结果

采用 MT-GAIL 方法得到的模型可以直接用于强化学习训练。但是 TD-BC 方法得到的模型本质是单智能体模型, 此时 TD-BC 方法得到的价值网络无法直接用于多智能体强化学习训练。所以需要针对学生模型产生的价值网络进行修改, 保证 TD-BC 方法产生的单智能体策略网络和价值网络可以用于多智能体算法中。

图 9 展示了加载模仿学习模型后, 通过进一步进行强化学习训练 30 轮所获得的可视化效果。从图中可以明显看出, 仅经过 30 轮的强化学习训练, 智能体便成功地掌握了在保持不穿越边界的前提下, 追捕

动态目标和静态目标的能力。这一结果充分展示了强化学习在微调和优化智能体动作方面的有效性, 同时也凸显了模仿学习与强化学习相结合的潜在优势。

以 agent 5 为例, 分别对比仅采用强化学习方法训练 30 轮, 加载模仿学习方法继续用强化学习训练 30 轮和直接采用强化学习方法训练 300 轮的模型效果。将上述模型推演 50 轮, 记录每一轮的环境奖励值, 并计算推演 50 轮的累计环境平均奖励值。

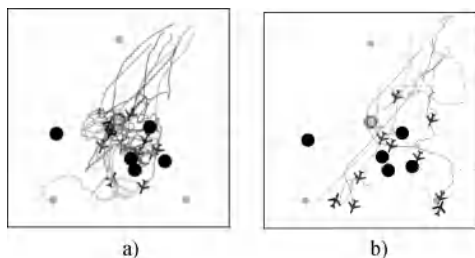


图 9 加载模型训练 30 轮后的可视化结果
a) 追捕动态目标成功; b) 追捕静态目标成功

推演过程的环境奖励值如图 10 所示, 横坐标表示推演轮次。位于下方的细线表示仅采用强化学习方法训练 30 轮的模型效果, 此时的模型发挥较不稳定。位于中间的虚线表示采用强化学习方法训练 300 轮的效果, 此时模型较为稳定。位于上方的粗曲线表示加载模仿学习的模型并训练 30 轮的效果。此时的模型效果较好, 且大多数情况优于强化学习训练 300 轮的模型效果, 说明模仿学习方法学习到了专家经验。

4 结束语

本文提出了 TD-BC 和 MT-GAIL 方法相结合的混合模仿学习方法, 该方法生成的模型可以直接用于强化学习训练, 从而提高智能体的训练效率。同时该方法可以处理多质量的专家轨迹, 使得模型较少受

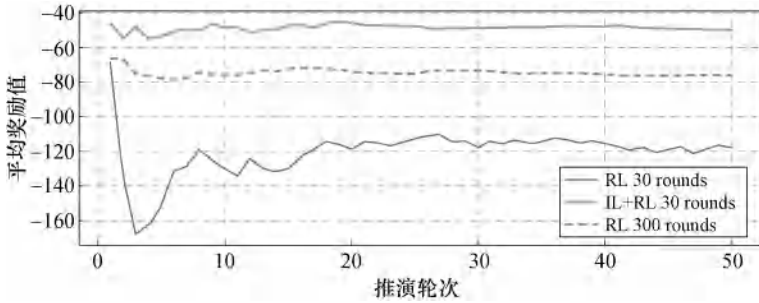


图 10 不同训练方法的环境奖励值对比

到低质量的专家轨迹的影响。结合多智能体目标追捕任务，对本文提出的混合模仿学习方法进行了实验验证。结果表明方法可以汲取专家经验，为强化学习模型训练提供一个较高起点。

参考文献

- 1 温广辉, 杨涛, 周佳玲, 等. 强化学习与自适应动态规划: 从基础理论到多智能体系统中的应用进展综述 [J]. 控制与决策, 2023, 38 (5): 1200-1230.
- 2 张梦钰, 豆亚杰, 陈子夷, 等. 深度强化学习及其在军事领域中的应用综述 [J]. 系统工程与电子技术, 2024, 46 (4): 1297-1308.
- 3 郝建业, 邵坤, 李凯, 等. 博弈智能的研究与应用 [J]. 中国科学: 信息科学, 2023, 53 (10): 1892-1923.
- 4 KHATIB O. Real-time obstacle avoidance for manipulators and mobile robots. In Proceedings of the 1985 IEEE International Conference on Robotics and Automation (ICRA) [C] //Piscataway: IEEE. 1985: 500-505.
- 5 POMERLEAU D A. Efficient training of artificial neural networks for autonomous navigation [J]. Neural Computation, 1991, 3 (1): 88-97.
- 6 BOJARSKI M, TESTA D D, DWORAKOWSKI D, et al. End to end learning for self-driving cars [J]. arXiv, 2016.
- 7 PFLUEGER M, AGHA A, SUKHATME S G. Rover-IRL: Inverse reinforcement learning with soft value iteration networks for planetary rover path planning [J]. IEEE Robotics and Automation Letters, 2019, 4 (2): 1387-1394.
- 8 ANDREW Y N, STUART J R. Algorithms for inverse reinforcement learning. In Proceedings of the 17th International Conference on Machine Learning (ICML) [C] //New York: Association for Computing Machinery. 2000: 663-670.
- 9 JONATHAN H, STEFANO E. Generative adversarial imitation learning. In Proceedings of the 30th International Conference on Neural Information Processing Systems [C] //Red Hook, NY, USA: Curran Associates Inc. 2016: 4572-4580.
- 10 XIAO D M, WANG B, SUN Z Q, et al. Behavioral cloning based model generation method for reinforcement learning. In Proceedings of the 2023 China Automation Congress (CAC) [C] //Piscataway: IEEE. 2023: 6776-6781.
- 11 XIAO D M, WANG B, SUN Z Q, et al. Imitation learning method of multi-quality expert data based on GAIL. In Proceedings of the 5th China Symposium on Cognitive Computing and Hybrid Intelligence (CCHI) [C] //Piscataway: IEEE. 2023: 8642-8647.

基于三段式检索增强框架的 NL2SQL 技术研究

马瑞祥^{1*} 郜洪奎¹ 雷达¹ 郎彬¹ 瞿崇晓¹

摘要 为提升垂直领域跨场景多主题数据分析效率，提出三段式检索增强框架（TREF）。TREF 整合数据库技术、大模型和提示词工程，特别是引入意图匹配检索、相似结构检索和领域知识检索三种机制，缓解自然语言转 SQL 意图理解和领域适应性不足问题。实验表明，三种机制均能独立提升正确性，同时融合三种机制效果最佳，军事测试集上正确率提升 37%。文章证实无须额外领域训练，TREF 框架能够有效提升 NL2SQL 领域应用能力，对军事指挥及数据分析场景具有重要价值。

关键词 三段式检索增强框架，自然语言转 SQL，意图理解，领域适应

Research on NL2SQL Technology by a Tri-Stage Retrieval-Enhanced Framework

MA Rui-Xiang^{1*} GAO Hong-Kui¹ LEI Da¹ LANG Bin¹ QU Chong-Xiao¹

Abstract To enhance cross-scenario, multi-topic data analysis efficiency in vertical domains, a Tri-stage Retrieval-Enhanced Framework (TREF) is proposed. Integrating database technology, large language model services, and prompt engineering, TREF incorporates intent matching, structural similarity, and domain knowledge retrieval to address NL2SQL's limitations in intent understanding and domain adaptability. Experimental results demonstrate individual mechanism contributions to SQL conversion accuracy, with their combined application achieving a 37% relative accuracy increase on a specialized military dataset. This study confirms TREF's effectiveness in boosting NL2SQL usability without dedicated domain training, holding significant implications for military operations and data-intensive applications.

Key words tri-stage retrieval-enhanced framework, NL2SQL, intent understanding, domain adaptation

0 引言

在信息化技术高速发展的背景下，军事领域参谋人员从不同系统中收集分析战场环境、装备人员等数据的效率有待提

升。自然语言转 SQL（Natural Language to SQL, NL2SQL）技术是一种新型的人员与数据库交互的高效方式。NL2SQL 是自然语言处理（NLP）与数据库技术的交叉领域，旨在将自然语言查询转化为可执行的 SQL 查询，非技术人员也能便捷地与数据

* 通讯作者

1. 中国电子科技集团公司第五十二研究所

1. The 52nd Research Institute of China Electronics Technology Group Corporation

库进行交互，提升数据分析的易用性。该研究领域的兴起，源于大数据时代对灵活、高效信息检索的需求，以及对日益增长的非技术用户群提供友好数据服务需求，在智能问答系统、搜索引擎、智能助手等场景具有广泛的应用场景。NL2SQL 技术自提出以来，经历了从规则基础方法到统计学习模型，再到深度学习方法的演进，但是随着业务需求的日益复杂，特别是在处理复杂业务情况的数据库分析任务时，NL2SQL 存在如下问题：

(1) 意图理解不足：复杂业务场景下如何精准理解用户意图，准确获取相关数据表，完成 SQL 查询语句的转化是一个难点。

(2) 领域适应能力差：用户自然语言查询涉及的业务知识，模型没有显式学习的情况下如何正确理解，精准完成 SQL 转换是一个难题。

为缓解上述问题，本文基于开源大模型设计了三段式检索增强框架 (TREF)，提升军事领域复杂业务场景下的 SQL 查询转换精度和系统适应性。

1 问题定义

在军事指挥作业场景中，参谋人员需要对气象环境要素、装备设施情况、作战人员信息等数据信息进行分析，需要使用不同软件系统对不同数据库进行数据查询、管理、分析。本文提出的 NL2SQL 技术对底层数据库进行打通，参谋人员只需要通过自然语言进行交互即可自动生成对应 SQL，完成数据查询分析的意图，提升作战指挥的效率。

NL2SQL 技术本质上是文本序列生成问题，即对于给定长度为 m 的文本序列 $X = \{x_1, x_2, \dots, x_m\}$ 和长度为 p 的文本

序列 $C = \{c_1, c_2, \dots, c_p\}$ ，生成对应的文本 $Y = \{y_i \mid (c, \theta, x)\}$ 。其中， C 为数据表文本字符集合， X 为输入问题字符集合， θ 为超参数， Y 为生成的数据库语言 SQL 字符集合。

2 相关工作

NL2SQL 技术主要解决人员与数据库交互的问题，旨在允许非技术专业的用户能够方便、高效地利用自然语言直接查询数据库，降低数据访问的门槛。目前学术界对数据表内容、增强词表示学习以及引入大语言模型做了诸多研究。2020 年，Zhang 等^[1]提出表内容融合的 Text2SQL 生成 (F-SQL) 框架，通过门控机制融合数据表内容与数据表结构信息，以更好地理解数据表模式；同时，Zhang^[2]等做了进一步研究，基于 BERT 预训练语言模型改进了列值提取的问题，提出多任务学习下的数据表 Text2SQL 生成 (M-SQL) 模型，该方法将列值提取过程分为列名匹配和列值提取两个部分，有效解决了传统方法无法提取查询结果中包含多个不同列值的复杂问题。2023 年，Hao 等^[3]提出基于耦合与解耦的 NL2SQL 特征表示学习 (CFCDC) 方法，该方法解决了模型忽略 SELECT 和 WHERE 之间的显式关联以及单个子句内不同 SQL 任务之间隐式关联问题，通过多任务学习和特征解耦策略，显著提升了在结果的准确性。Gao 等^[4]在 NL2SQL 任务中引入了一种新的综合解决方案，作者引入大语言模型工具，对提示工程进行深入研究，通过监督微调进一步提升性能。Zheng 等^[5]针对用户可能无法提出完整问题的情况做了文本到 SQL 自动补全研究，设计关系感知的桥接网络 (RHB-Net)，通过历史查询融合和动态上下文构建的优

化策略，有效解决不完整查询的 SQL 预测问题。2024 年，Zhang 等^[6] 提出开放域 Text-to-SQL 的多跳表格检索（MURRE）方法，通过多跳表检索和重写策略，解决单一检索步骤无法兼顾的模式链接问题，尤其是领域实体不匹配、形近语义不相关的情况，显著提高了文本转自然语言的效果。Li 等^[7] 提出增强提示的两轮 SQL 精练与交叉一致性（PET-SQL）方法，第一阶段引入参考增强表示，包含模型信息和数据表中随机抽样值指导大模型生成初步 SQL；第二阶段利用精简后的模式信息引导大模型生成最终 SQL。作者提出了一个后处理模块，通过大模型进行交叉一致性验证，进一步提升 SQL 结果生成的正确性。

目前已有多项研究对 NL2SQL 的框架

和方法进行改进，但是对于如何精确高效地定制领域特定 NL2SQL 能力，以及如何不显式训练领域知识的条件下精准捕获用户意图的相关研究仍处于空白。如何提升 NL2SQL 领域适应性，不增加领域训练成本的情况下准确把握用户数据查询意图是该领域仍需解决的难题。

3 三段式检索增强框架原理

基于三段式检索增强框架（Tri-stage Retrieval-Enhanced Framework, TREF）基于 LLM-NL2SQL 技术框架进行定制开发和优化，整体包括数据库技术单元、大模型技术单元和提示词工程单元，技术架构图如图 1 所示。

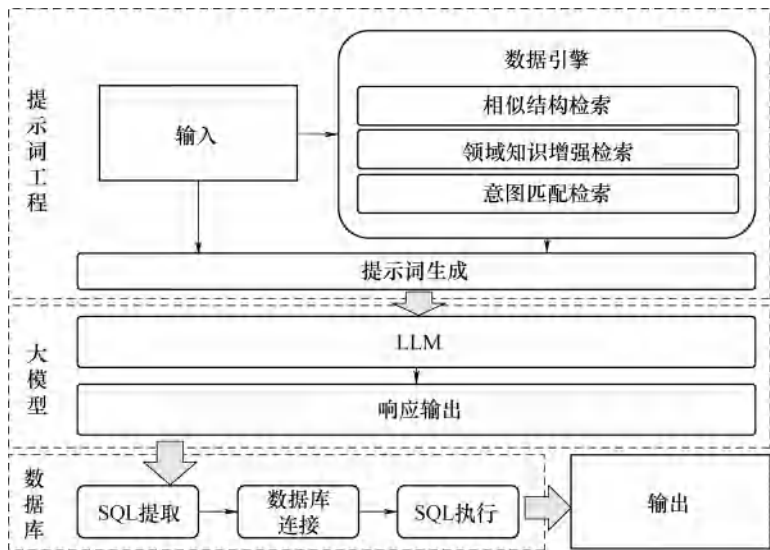


图 1 TREF 技术架构图

目前工业界基于 LLM-NL2SQL 技术方案多引入数据表结构信息，本文提出的 TREF 框架同时引入意图匹配检索、相似结构检索和领域知识检索三种机制，更为有效地缓解自然语言转 SQL 意图理解和领域适应性不足问题。接下来对 TREF 框架

原理进行详述。

3.1 数据库模块

数据库单元作为框架的核心组件之一，致力于实现对多种数据库的广泛兼容性，适配 MySQL、Oracle 等主流数据库以

及国产数据库。数据库单元主要包括 SQL 提取、数据库连接、SQL 执行三个部分。

(1) SQL 提取：该模块通过标准化接口接收大模型单元生成的结果，提取 SQL 指令部分。

(2) 数据库连接：该模块设计注重灵活性和稳定性，支持数据库类型的扩展，具备连接数据库功能，辅助支撑执行单元运行 SQL。

(3) SQL 执行：在对于数据库中使用生成的数据库语言进行执行查询操作，提供数据反馈。

3.2 大模型模块

该模块主要对大模型进行管理和服务部署，旨在理解用户自然语言表述的数据查询需求，结合上下文的相关知识生成正确的 SQL 指令。本文使用开源大模型 Baichuan^[8]进行集成。

3.3 提示词工程模块

该模块是框架最为核心的组件，旨在理解用户自然语言表述的数据查询需求，结合上下文的相关知识生成大模型引导指令。具体工作原理是结合领域知识库深度分析用户查询意图，结合意图匹配和相似结构检索精准定位数据表和数据字段，缓解错误 SQL 生成的现象，尤其是处理复杂、多维度的数据查询请求，提高查询的准确性。

3.3.1 意图匹配检索

意图匹配检索单元旨在优化用户输入与数据表的相关性查询，过滤上下文无关数据表信息，提高数据表、列字段选取的精准度。主要工作流程图如图 2 所示，接下来对关键环节进行介绍。

数据表：主要包括两个部分，首先对每个数据表和表字段进行中文注释，辅助

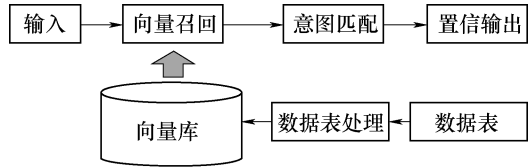


图 2 意图匹配检索工作流程图

理解表和字段；其次梳理数据表的业务属性，进行意图类别标注。例如，人员相关、气象相关、装备相关等意图。

数据表处理：使用开源文本表征模型 BGE^[9]对数据表中文文本注解进行语义表征，借助 Faiss^[10]向量库进行索引构建，辅助支撑向量检索。

向量召回：对输入文本使用文本表征模型 BGE 进行语义向量表征，使用 IndexFlatL2 测量搜索向量与索引向量的欧式距离，选取最相关的 Top10 结果进行返回。

意图匹配：对输入文本进行意图分类，本文通过设计提示词引导大模型进行多意图分类，过滤不相关数据表，最终选取相关性大于 0.7 且意图相同的 TOP3 数据表进行输出。

3.3.2 相似结构检索

该单元维护结构化模板库，接收到查询请求时对相似结构库进行语义相关性检索，挑选相关性高的数据库语言语法示例，主要工作流程图如图 3 所示，单元功能原理与上节相同，接下来主要对相似结构数据进行介绍。

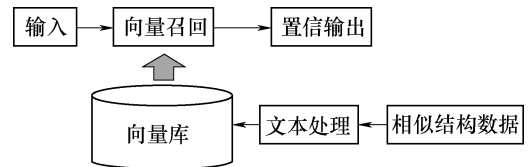


图 3 相似结构检索工作流程图

相似结构数据：这类数据的本质是结构化模板，特点是包含自然语言转数据库语言的逻辑，设计目的用于捕获查询需求。

1. 模板 1

相似结构：盛行什么_

模板意图：统计不同要素的频率；

模板 SQL：select _count (*) from _

group by_ ；

2. 模板 2

相似结构：_情况

模板意图：用于分析某列数据的极值和平均值，适用于趋势分析或基本统计；

模板 SQL：select MIN(_), MAX(_), AVG(_) from_where_ ；

通过这种方式，将用户潜在的数据分析意图提供至上下文中，作为语法示例提高 SQL 转化的精准度。例如，用户询问“××过去一周盛行什么风向？”会将 select_count (*) from_group by_相似结构 SQL 数据增加至上下文中增强提示。

3.3.3 领域知识检索增强

该单元设计用于维护业务知识库，提供潜在业务背景知识，辅助理解用户意图不明确和业务逻辑复杂的场景，提升生成 SQL 的准确性。主要工作流程图如图 4 所示，其中文本处理、向量召回等单元原理前文已做介绍，此处不做过多赘述。

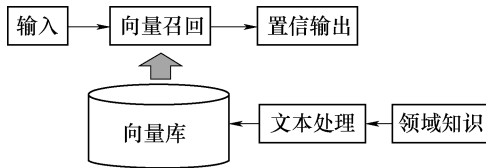


图 4 领域知识增强检索工作流程图

领域知识：主要维护业务相关的知识，形成领域知识库，例如：

(1) 天气情况通常包括风速、温度、气压、能见度、湿度、风力信息。

(2) A 类装备使用条件需查询湿度、风力、风向信息。

(3) ××员工作经验包括参加工作时间、曾使用装备名称、曾使用装备类型、

现使用装备名称、现使用装备类型。

(4) 适飞判断需使用风力预报信息和装备适飞风力等级信息。

通过这种方式，将依赖的业务知识注入上下文进行领域知识提示，保障数据表、字段选择的完整性。

4 实验结果与分析

4.1 数据介绍

实验数据源自真实生产环境，业务领域较为广泛，涉及人员管理、气象要素分析、装备设施管理等场景，涵盖了丰富的问题类型和 SQL 结果。为保证测试数据集的正确性，本文使用人工生成方式对测试数据进行生成。通过严格的收集与重复数据剔除过程，共收集测试集 100 条，供实验测试使用。示意数据如下：××区近××年平均××量是多少？查询使用××装备的×××员有哪些？

4.2 评价指标

为评估 TREF 方法的效果，本文使用正确率 (Accuracy, Acc) 作为核心评估指标。

$$Acc = \frac{N_{correct}}{N} \quad (1)$$

考虑到 SQL 复杂多样但是执行结果相同的特点，并没有使用字符串比较指标。通过对比模型生成 SQL 的执行结果与预设标准答案是否一致，作为判定生成正确与否的依据。 $N_{correct}$ 表示执行结果与预设结果相同的样本数量， N 表示全部测试样本数量。

4.3 实验结果

为了验证本文引入意图匹配检索、相似结构检索、领域知识检索的有效性，本

文设置了 5 组实验进行对比，详细实验设置和实验结果如下：

实验 1（基准方法）：使用 LLM - NL2SQL 框架，使用 BGE 模型对数据表进行检索，选取 TOP3 结果添加至上下文，使用开源 Baichuan 大模型进行 SQL 生成。

实验 2（基准方法+意图匹配检索）：在基准方法的基础上，对数据表检索结果进行意图匹配判断，选取 TOP3 结果添加至上下文，使用开源 Baichuan 大模型进行 SQL 生成。

实验 3（基准方法+领域知识检索）：在基准方法的基础上，对领域知识库进行检索，选取置信度大于 0.8 的领域知识结果添加至上下文，使用开源 Baichuan 大模型进行 SQL 生成。

实验 4（基准方法+相似结构检索）：在基准方法的基础上，对相似结构模板库进行检索，选取置信度大于 0.8 的模板结果添加至上下文，使用开源 Baichuan 大模型进行 SQL 生成。

实验 5（基准方法+全部）：在基准方法的基础上，同时引入意图匹配、领域知识检索、相似结构检索单元，使用开源 Baichuan 大模型进行 SQL 生成。

通过对表 1 结果的分析，可以得出如下结论：

表 1 实验结果

实验	方法	正确率 (Acc)
1	基准方法	0.50
2	基准方法+意图匹配检索	0.70
3	基准方法+领域知识检索	0.63
4	基准方法+相似结构检索	0.60
5	TREF（基准方法+全部）	0.87

(1) 同时引入意图匹配检索、相似结构检索、领域知识检索的 TREF 方法效果最优，正确率较基准模型提升 37%。

(2) 单独引入意图匹配检索机制正确率提升最大，较基准模型提升 20%，间接说明匹配用户查询意图减少无关数据表在 SQL 生成过程中的重要性。

(3) 单独引入领域知识检索单元对结果具备提升作用，正确率较基准模型提升 13%，间接说明领域知识在指导生成 SQL 过程中具有正向作用。

(4) 单独引入相似结构检索单元对结果具备提升作用，正确率较基准模型提升 10%，间接说明相似结构模板的引入对自然语言转 SQL 的过程具有正向作用。

综上所述，本文提出的 TREF 方法融合了三种有效的策略，在未训练的情况下能够显著提升大模型领域 SQL 生成正确性。

参考文献

- ZHANG X, YIN F, MA G, et al. F-sql: fuse table schema and table content for single-table text2SQL generation [J]. IEEE Access, 2020, 8: 136409-136420.
- ZHANG X, YIN F, MA G, et al. M-SQL: Multi-task representation learning for single-table Text2SQL generation [J]. IEEE Access, 2020, 8: 43156-43167.
- HAO C, ZHANG X, GAO C, et al. Feature Representation Learning for NL2SQL Generation Based on Coupling and Decoupling [J]. CoRR, 2023, abs/2306.17646.
- GAO D, WANG H, LI Y, et al. Text-to-sql empowered by large language models: A benchmark evaluation [J]. VLDB Endow, 2024, 17 (5): 1132-1145.
- ZHENG B, BI L, XI R, et al. RHB-Net: A Relation-aware Historical Bridging Network for Text2SQL Auto-Completion [C] //Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval. 2023: 1458-1467.

- 6 ZHANG X, WANG D, DOU L, et al. Multi-Hop Table Retrieval for Open-Domain Text-to-SQL [J]. CoRR, 2024, abs/2402.10666.
- 7 LI Z, WANG X, ZHAO J, et al. PET-SQL: A Prompt-enhanced Two-stage Text-to-SQL Framework with Cross-consistency [J]. CoRR, 2024.
- 8 YANG A, XIAO B, WANG B, et al. Baichuan 2: Open large-scale language models [J]. CoRR. 2023.
- 9 XIAO S, LIU Z, ZHANG P, et al. C-pack: Packaged resources to advance generalchinese embedding [J]. CoRR, 2023.
- 10 DOUZE M, GUZHVA A, DENG C, et al. The faiss library [J]. CoRR, 2024.

基于输入扰动的多模态大语言模型 不确定性估计

荆诗雨^{1,2} 陈 炜^{1,2} 龚闪闪^{1,2} 张星辉^{1,2} 崔 星^{1,2*}

摘要 针对多模态模型输入特点,提出了基于视觉-语言输入扰动的不确定性估计算法。通过模型对应输出波动判断模型对该输出的置信度,从而有效探测模型属性。针对视觉输入,提出利用自然噪声扰动视觉图像来增强预测熵对不确定性估计的性能。从语言输入角度提出反问重写策略,生成验证性问题对预测熵进行矫正。该算法在三个先进的多模态大语言模型上利用视觉问答任务进行评估,实验结果表明该算法对模型输出的正确性预测超过基线方法。

关键词 多模态大语言模型, 不确定性估计, 扰动探测, 可信大语言模型

Towards Input Perturbation-Based Uncertainty Estimation for Multi-Modality Large Language Models

JING Shi-Yu^{1,2} CHEN Wei^{1,2} GONG Shan-Shan^{1,2} ZHANG Xing-Hui^{1,2} CUI Xing^{1,2*}

Abstract An uncertainty estimation algorithm based on visual-language input perturbations is proposed for multi-modal model inputs. Input perturbations effectively probe the model's properties: if output fluctuations are small when perturbations occur, the model's confidence in the output is high; otherwise, it is low. For visual input, natural noise perturbation is used to enhance prediction entropy performance for uncertainty estimation. For language input, a rephrasing strategy generates verification questions to correct prediction entropy. The algorithm is evaluated on advanced multimodal large language models using visual question answering tasks. Experimental results show the algorithm significantly outperforms baseline methods.

Key words multi-modality large language models, uncertainty estimation, perturbation probe, trustworthy large language models

0 引言

近年来,大语言模型取得了卓越进

展,通过数据量和模型的扩增,大语言模型展现出越来越强大的语言理解和生成能力以及泛化能力^[1]。多模态大语言模型将大语言模型与其他模态的信息进行结合,

* 通讯作者

1. 中兵智能创新研究院有限公司 2. 群体协同与自主实验室

1. China North Artificial Intelligence & Innovation Research Institute 2. Collective Intelligence & Collaboration Laboratory

以大语言模型经过大量训练后掌握的先验知识为基础, 并进行跨模态的信息理解和生成, 从而具备多模态信息综合处理能力^[2]。多模态大语言模型具有广泛的应用前景, 如在智能系统试验领域^[3], 利用多模态大语言模型, 从多层次、多阶段综合的角度, 探索智能系统试验数据分析的新模型和新方法; 在军事领域^[4], 多模态大模型可以处理复杂的战场情报信息, 进而为作战人员提供决策支持, 例如, 大模型可对处理后的战场信息进行深入的分析, 实现对信息的关联、挖掘、预测等, 提高综合研判能力, 协助指挥员了解敌情、掌握敌方行动意图, 协助指挥员更快做出决策, 制定合理的战术和战略。因此, 多模态大语言模型具有广阔的发展前景及应用潜力。

随着多模态大语言模型的应用范围不断扩大, 模型预测的不确定性变得更加重要, 尤其是在一些实际任务和安全性问题中发挥着越来越关键的作用。例如, 在无人系统领域^[5], 不确定性估计在风险最小化中起着重要的作用, 无人系统作为现实世界中感知、决策、计划和行动的主体, 缺乏对视觉语言模型预测结果的量化估计会导致任务的失败等严重后果。因此, 估计多模态大语言模型的不确定性变得越来越重要。

1 相关工作

1.1 多模态大语言模型

多模态大语言模型是一类接收多种模态数据(例如, 图片和文字)作为输入的大模型, 目前常见的多模态大语言模型有 LLaVa、Qwen-vl-chat、Otter 等。LLaVa (Large Language and Vision Assistant) 模型^[6]提出

了视觉指令微调的概念, 通过将指令微调扩展到多模态领域, 为构建通用的视觉助手奠定基础。LLaVa 模型利用开源的 LLM 模型 (LLaVa) 和生成的多模态指令遵循数据, 充分发挥了预训练 LLM 和视觉模型的能力。Qwen-vl-chat (Large Vision Language Model, LVLM) 模型^[7]是以 Qwen-7B 为基座的大语言模型, 该模型引入视觉编码器 ViT-Visual Encoder, 并通过位置感知的视觉语言适配器 Position-aware Vision-Language Adapter, 将视觉信息直接融合到语言模型的解码器层中, 使得模型支持视觉信号输入。Otter 模型^[8]支持基于 OpenFlamingo 模型的多模态上下文指令调优, 并整合了不同来源的数据, 包括语言、图像和视频, 该模型在遵循用户指令和展示高水平推理能力方面表现较好, 支持多模态上下文学习和视觉问答任务。

1.2 多模态大语言模型的不确定性估计

深度神经网络的不确定性估计 (Uncertainty Estimation, UE) 一般用于衡量模型输出的可靠程度^[9]。根据不确定性的来源进行划分, 神经网络的不确定性可分为偶然不确定性 (Aleatoric Uncertainty)^[10]和认知不确定性 (Epistemic Uncertainty)^[11]。其中, 偶然不确定性一般来自数据内部, 例如, 图像在采样时所引入的自然噪声, 是一类不可避免的不确定性。而认知不确定性一般来自模型本身, 例如, 不合理的训练设置或质量较低的训练数据。目前, 不确定性估计算法主要依靠多次采样来近似模型输出的后验分布, 包括 Monte-Carlo Dropout^[12-14]、Deep Ensemble^[15-17]。

然而, 多模态大语言模型给不确定性估计带来新的挑战。首先, 多模态大语言

模型使用自回归 (Auto-regression) 模式进行解码, 也即根据当前的上下文信息预测下一个词元的概率分布^[18]。这导致模型的输出空间几乎是无限的, 也即自由形式输出 (Free-form Generation)。模型输出可能由一个词元组成, 也可能由多个词元组成, 而传统的神经网络输出空间一般是固定的, 例如, 多分类网络的输出为固定的标签空间 (label space)^[19]。如何在自由形式输出下对大模型进行不确定性估计是一个新的挑战。其次, 多模态大语言模型以多种模态的数据作为输入, 每一种模态都有其自身的不确定性, 这会造成不确定性的叠加, 提高模型整体不确定性估计的困难^[20]。目前大模型的不确定性估计还处于早期研究阶段。Semantic Entropy (SE)^[21] 首先提出分析自由格式输出下大语言模型的语义空间, 并估计语义空间中语义簇的密度, 提高了不确定性估计的效果。Shifting-Attention-to-Relevance (SAR)^[22] 进一步指出, 由于“语言冗余” (Linguistic Redundancy) 的存在, 模型解码出的词元在语义表达上并不是等价的, 因此, 不确定性估

计需要考虑词元的重要性。INSIDE^[23] 将模型的不同采样结果构建成相似度矩阵, 并从矩阵中抽取特征值和特征向量来表征模型输出空间中的语义一致性, 进而提高了模型不确定性估计。Deg^[24] 同样利用模型输出的语义一致性来评估不确定性。不同的是, Deg 采用了黑盒的形式, 通过计算模型输出的杰卡德 (Jaccard) 相似度矩阵^[25], 然后从该相似度矩阵中抽取特征值和特征向量来计算语义一致性。

2 基于扰动探测的不确定性估计

本章详细描述所提出的基于输入扰动的多模态大语言模型不确定性估计算法。首先, 给出了多模态大语言模型中预测熵 (Predictive Entropy, PE) 的定义, 作为不确定性估计的基线方法。其次, 对多模态模型的输入扰动给出定义。最后, 本章形式化描述基于输入扰动的多模态模型不确定性估计算法。图 1 为本文所提出的基于输入扰动的不确定性估计算法示意图。

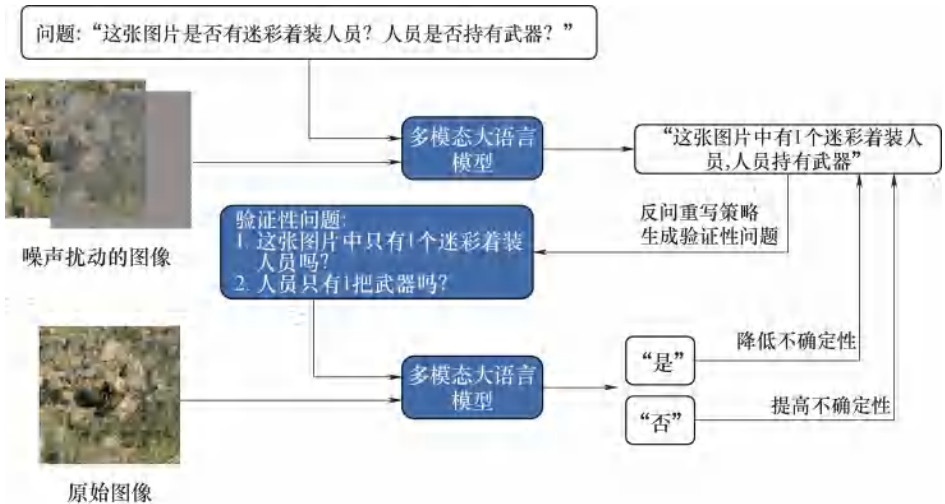


图 1 基于输入扰动的不确定性估计方法示意图

2.1 多模态大语言模型的预测熵

本文主要研究多模态模型中视觉-语言模型 (Vision-Language Model) 的不确定性估计, 并以视觉问答任务 (Vision Question Answering, VQA) 为主。预测熵^[26]是一种在大模型中常见的不确定性估计方法。给定一个视觉语言模型, 定义一个模型输入为 $X = (x_v, x_l)$, 其中 x_v 表示输入中的视觉信息, 即图片, x_l 表示该输入中的文本信息, 例如, 针对该图片的一个问题。定义输入 X 的正确答案为 Y^* 。假设将输入 X 传入该模型后, 模型的输出为:

$$Z = \{z_1, z_2, \dots, z_N\} \quad (1)$$

式中, N 为该输出包含的词元数量。那么, 模型在解码第 i 个词元, z_i , 时的概率分布可以表示为:

$$z_i \sim p_\theta(z_i | Z_{<i}, X) \quad (1 \leq i \leq N) \quad (2)$$

式中, θ 为该视觉语言模型的参数; $Z_{<i}$ 为模型已经解码出的前 $i-1$ 个词元序列。此时, 模型在生成 Z 上的预测熵 (PE) 可以被定义为下列形式:

$$\begin{aligned} PE(Z, X, \theta) &= -p_\theta(Z) \log(p_\theta(Z | X)) = \\ &= \sum_i -p_\theta(z_i | Z_{<i}, X) \log p_\theta(z_i | Z_{<i}, X) = \\ &= \sum_i -p_\theta(z_i | Z_{<i}, x_v, x_l) \\ &= \log p_\theta(z_i | Z_{<i}, x_v, x_l) \end{aligned} \quad (3)$$

从式 (3) 可知, 预测熵是一种 token 信息熵的累加。该方法能有效地描述大模型在解码过程中每个词元的不确定性, 并用加和的形式表达整个输出的不确定性^[27]。预测熵越大表示模型输出不确定性越高; 反之, 不确定性越低。本文将以预测熵作为基线方法, 研究如何利用输入扰动增强预测熵的不确定性估计性能。

2.2 多模态大语言模型的输入扰动

输入扰动 (Input Perturbation, IP) 是

一种有效的模型性质探测方法^[28]。本文所提出的利用输入扰动来探测模型不确定性是由语义一致性假设所启发, 即当输入发生微小变化时 (例如, 给输入施加一个不改变原语义的变化), 观察模型对应的输出是否有较大的波动: 当模型输出有较大波动时, 表示模型对原输出的不确定性较高; 反之, 模型不确定性较低。具体地, 对于输入 x , 定义一个不改变 x 语义的扰动为 δ , 即:

$$s(x, x + \delta) < \varepsilon \quad (4)$$

式中, $s(\cdot, \cdot)$ 为一个语义距离度量, 例如, $L-2$ 距离; ε 是一个扰动预算, 即扰动 δ 所带来的对 x 的语义变化不能超过 ε 。那么, δ 就可以定义为 x 的一个“微小”扰动。此时, 多模态大语言模型的预测熵在视觉输入扰动 δ 下可以被定义为:

$$\begin{aligned} PE_\delta(Z, X, \theta) &= \\ &= \sum_i -p_\theta(z_i | Z_{<i}, X + \delta) \\ &= \log p_\theta(z_i | Z_{<i}, X + \delta) \end{aligned} \quad (5)$$

考虑到模型输入由多种模态构成, 如何为不同的模态配置合适的扰动方式是至关重要的。对于视觉输入 x_v , 由于视觉信号的扰动空间是无限大且无法被穷尽的, 因此, 需要对扰动噪声加以限制。本文主要考虑在 x_v 上叠加三种扰动噪声, 包括高斯噪声 (Gaussian Noise)、泊松噪声 (Poisson Noise)、运动模糊 (Motion Blur)。同时, 每种噪声强度 (severity) 由噪声分布的方差控制, 本文选择了五种噪声强度 (severity 从 1~5, 噪声强度按比例增大)。这些自然噪声在现实世界中十分常见, 利用自然噪声扰动所估算出的模型不确定性可以较好地泛化至现实世界中^[29]。

在 VQA 任务中, 多模态大语言模型的语言输入 x_l 一般是一个针对视觉输入 x_v 的

询问 (Query), 如给定一张图片, 询问“这张图片中有多少戴帽子的人”。相较于视觉信息, 语言输入的扰动空间更小且等语义变换更加困难, 这是因为视觉输入的空间是连续的。例如, RGB 图像一般被归一化为 $[0, 1]$, 在该连续空间上有无限多的变化可以不改变输入信号 x_v 的原语义。相反, 语言输入是基于词元的, 而词元来自离散词表。在词元层面施加扰动会显著改变 x_l 的原语义, 导致扰动所估计的不确定性出现误差^[30]。为了解决该问题, 提出一种反问重写 (Interrogative Rewriting, IR) 策略。IR 是一种通过结合模型输出来构造验证性问题, 并利用验证性问题来探测模型不确定性的扰动方法。具体来说, 假设模型针对输入 (x_v, x_l) 的输出为 Z , IR 直接构建验证问题 $I_{x_l, Z}$, 例如, 询问 Z 是否为问题 x_l 的答案。该验证问题一般为“是/否 (Yes/No)”问题, 也即模型只能回答“是/否”。此时, 模型对 $I_{x_l, Z}$ 的输出表达了模型对其原输出, 即答案 Z 的不确定性: 若模型对问题 $I_{x_l, Z}$ 的输出为“是”, 则表明模型对其原输出 Z 的一种肯定, 此时模型不确定性应当降低; 若模型的输出为“否”, 则表明模型反对了其原输出 Z , 此时模型不确定性应当被提高。形式化地, 经 IR 策略矫正的预测熵可以被描述为:

$$PE^{IR} = PE(Z, X, \theta) - p_\theta$$

$$(y = \text{Yes} \mid x_v, I_{x_l, Z}) \quad (6)$$

式中, $p_\theta(y = \text{True} \mid x_v, I_{x_l, Z})$ 为模型对验证问题 $I_{x_l, Z}$ 的回答为“是 (Yes)”的概率。因此, 模型对验证性问题越肯定, 矫正后的不确定性越低。

2.3 基于输入扰动的不确定性估计

视觉输入扰动和语言输入扰动是独立

模块, 它们既可以单独使用也可以整合到一起, 进一步提高不确定性估计性能。本文定义基于视觉扰动的预测熵为 $PE_V = PE_\delta(Z, X, \theta)$; 定义基于语言扰动的预测熵为 $PE_L = PE_{IR}$; 基于视觉和语言联合扰动的预测熵定义为:

$$PE_{VL} = PE_V(Z, X, \theta) - p_\theta$$

$$(y = \text{Yes} \mid x_v, I_{x_l, Z}) \quad (7)$$

在后续实验分析中将沿用上述表示指代对应算法。

3 实验

本章将提供详细的实验设置和实验结果, 包括模型和数据集的选择、评价指标、总体方法效果评估, 以及消融实验。

3.1 模型与数据集选择

本文主要采用三种先进的多模态大语言模型进行实验评估, 包括 LLaVa-v1.5-7b、Otter-9b 和 Qwen-vl-chat。LLaVa-v1.5-7b 专注于理解和生成自然语言与视觉内容, 适用于需要处理图文混合信息的应用。Otter-9b 拥有更强大的计算能力, 能够处理更大规模的数据和更复杂的任务, 适合需要高精度和高效能的应用场景。Qwen-vl-chat 则在多轮对话和上下文理解方面表现出色, 能够在复杂对话中提供准确且连贯的回答。

在数据集方面, 本文主要选择目前较为流行的 SEED-Bench v1^[31] 数据集。SEED-Bench v1 数据集是一个专门设计用于评估和改进多模态语言模型的基准数据集。它包含了约 2 万个问题, 覆盖了多种类型和类别, 包括选择题、填空题和开放式问题等。由于利用完整的数据集进行不确定性估计对计算资源需求较高, 本文在

SEED-Bench v1 上随机选择了 1000 个问题用于性能评估。

3.2 评价指标

本文通过预测模型生成结果的正确性来评估不确定性估计的效果。理想情况下,不确定性估计算法应该为错误答案赋予较高的置信度,而为正确答案赋予较低的置信度。因此,不确定性估计的评价可以转换成针对模型生成结果正确性的二分类问题。本文主要使用 AUROC (Area Under the Receiver Operating Characteristic Curve) 表示随机正确生成结果的预测不确定性低于随机错误生成结果的概率。AUROC 等于 0.5 意味着所计算出的不确定性值与模型输出的正确性无任何关系,即不确定性值与随机猜测没有区别。相反, AUROC 等于 1 则意味着正确输出的不确定性始终小于错误输出。

3.3 语言输入扰动测试

本节将讨论语言输入扰动对多模态大语言模型不确定性估计的影响。表 1 给出了经语言输入扰动矫正的 PE , 即 PE_L 和原始 PE 方法在三个多模态大语言模型上的对比。由表 1 可知, LLaVa-v1.5-7b 与 Qwen-vl-chat 两个多模态模型效果较好, 在 SEED-Bench v1 VQA 数据集上分别达到了 63% 和 64.9% 的精准度。对应地, 原始

表 1 语言输入扰动对不确定性估计的影响

模型	精度	数据集	PE	PE_L
LLaVa-v1.5-7b	63.0%	SEED-Bench v1	75.5	76.8
Qwen-vl-chat	64.9%	SEED-Bench v1	74.5	76.9
Otter-9b	30.3%	SEED-Bench v1	58.0	58.8

注: PE 表示基线方法预测熵; PE_L 表示本文所提出的语言扰动矫正后的预测熵。

的 PE 方法达到了接近 75% 的 AUROC 值。经过语言扰动后, AUROC 值在这两个模型上均出现了较大提升。具体来说, PE_L 相较于 PE 在 LLaVa-v1.5-7b 上提高了 1.3% AUROC, 在 Qwen-vl-chat 上提高了 2.4% AUROC。Otter-9b 模型在该数据集上只能达到 30.3% 的精度, 这表明 Otter 有较弱的视觉问答能力。对应地, PE 在 Otter 模型上达到了 58% AUROC。经过语言扰动后, PE_L 相比于 PE 在 Otter 模型上提高了 0.8% AUROC。从上述两类实验可知, 语言扰动不确定性估计能为 PE 带来持续的提升, 无论是在模型表现较好时 (例如, LLaVa 和 Qwen), 还是在模型表现较差时 (例如, Otter), 这表明所提出的方法具有较强的普适性, 能为现实世界中的多种场景带来稳定提升。

3.4 视觉输入扰动测试

本小节研究视觉输入扰动对不确定性估计的影响。如前文所述, 本文主要使用高斯噪声、泊松噪声和运动模糊噪声作为扰动来源, 并设置三种扰动强度。图 2 给出了输入扰动对不确定性估计的影响。

整体来看, 噪声扰动对不确定性估计性能有较为明显的提升。这三种噪声在不同噪声强度下基本都能超过原始 PE 性能。在扰动强度上, 对于高斯噪声和泊松噪声, 较小的扰动强度能更为有效地提高不确定性。例如, 在噪声强度为 1 时, 高斯噪声扰动和泊松噪声扰动能将 PE 从 75.5% AUROC 提升至 76.5% AUROC 左右, 带来 1% AUROC 的提升。对于运动模糊噪声, 相比于低强度扰动, 中等强度的噪声扰动能带来更好的提升。然而, 对于高噪声扰动, 即 severity 等于 3 的情况下, 视觉扰动并没有显著提高多模态

模型的不确定性估计。

从语义一致性角度分析,该现象是合理的。高噪声扰动意味着视觉信息产生了较大的变化,此时所估算的就不再是原视觉信息的不确定性,而是添加扰动后语义信息发生改变的新视觉信息的不确定性。因此,在高扰动强度下,不确定性估计并没有被提高。然而,适量噪声扰动能有效提高不确定性估计的性能。

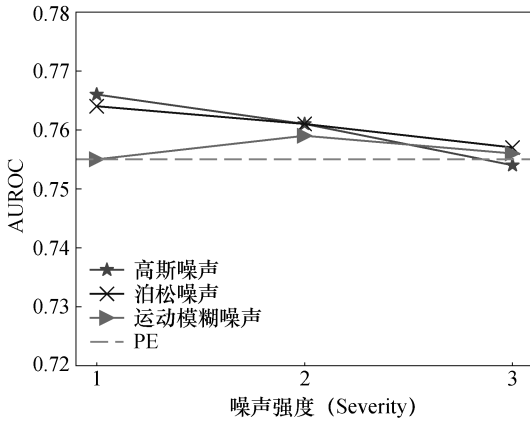


图2 视觉输入扰动对不确定性估计的影响

3.5 联合视觉-语言扰动性能测试

从前文结果分析可知,单独使用视觉扰动和语言扰动都对多模态大语言模型的不确定性估计产生积极影响。本小节探究这两种方法的结合是否能进一步增强不确定性估计的效果。表2给出了 LLaVa-v1.5-7b 模型在同时利用视觉扰动和语言扰动时,不确定性估计性能的变化。从实验可知,这两种扰动方法是独立且能够被同时使用的。同时使用这两种方法能进一步将多模态模型的不确定性性能从 76.8% AUROC 进一步提升至 77.9% AUROC,带来了 1.1% AUROC 的提升,与原始的 PE 相比提升了 2.4% AUROC。

表2 视觉扰动和语言扰动多模态模型的不确定性估计

模型	PE	PE_V	PE_L	PE_{VL}
LLaVa-v1.5-7b	75.5	76.6	76.8	77.9

4 结束语

本文研究了在输入扰动发生时,多模态大语言模型的不确定性估计效果。在视觉扰动方面,本文发现适度地添加自然噪声能有效地提高模型不确定性估计效果。在语言扰动方面,本文提出了一种简单的“反问重写(IR)”策略,通过将模型输出转换成简单疑问句,并以“是/否”类问题来探测模型对其原始输出的确定度。实验验证了语言扰动能有效提高模型不确定性估计。本文进一步研究视觉扰动和语言扰动的融合,发现所提出方法的融合能进一步为不确定性估计带来显著提升。本文所提出的方法实现简单便捷,适用性强,可以作为多模态大语言模型不确定性估计的方法应用于现实世界中,可以为军事、无人系统等领域的实际任务提供支撑。

参考文献

- 赵朝阳,朱贵波,王金桥. ChatGPT 给语言大模型带来的启示和多模态大模型新的发展思路[J]. 数据分析与知识发现, 2023, 7(3): 26-35.
- 刘静,郭龙腾. GPT-4 对多模态大模型在多模态理解、生成、交互上的启发[J]. 中国科学基金, 2023, 37(5): 793-802.
- 秦龙,武万森,刘丹,等. 基于大语言模型的复杂任务自主规划处理框架[J]. 自动化学报, 2024, 50(4): 862-872.
- 蔡磊,孟宪波,韩冬梅,等. 大模型在军事垂直领域的应用[J]. 舰船科学技术, 2024, 46(5): 171-175.

- 5 WANG L, MA C, FENG X, et al. A Survey on Large Language Model based Autonomous Agents [J]. *Frontiers of Computer Science*, 2024, 18 (6): 186345.
- 6 LIU H, LI C, WU Q, et al. Visual instruction tuning [C] // *Advances in neural information processing systems*. 2024.
- 7 BAI J, BAI S, YANG S, et al. Qwen-vl: A frontier large vision-language model with versatile abilities [J]. *arXiv preprint arXiv: 2308.12966*, 2023.
- 8 LI B, ZHANG Y, CHEN L, et al. Mimic-it: Multi-modal in-context instruction tuning [J]. *arXiv preprint arXiv: 2306.05425*, 2023.
- 9 GAWLIKOWSKI J, TASSI C R N, ALI M, et al. A Survey of Uncertainty in Deep Neural Networks [J]. *Artificial Intelligence Review*, 2023, 56 (1): 13-89.
- 10 EYKE H, AEGEMAN W. Aleatoric and epis-temic uncertainty in machine learning: an introduction to concepts and methods [J]. *Machine Learning*, 2021, 110 (1).
- 11 JAIN M, LAHLOU S, NEKOEI H, et al. DEUP: Direct Epistemic Uncertainty Prediction [J]. *arXiv: 2102.08501*, 2021.
- 12 GAL Y, AHRAMANI Z. Dropout as a Bayesian Approximation: Representing Model Uncertainty in Deep Learning [C] // *International Conference on Machine Learning*. JMLR, 2016.
- 13 程曦, 张志勇. 基于人工神经网络的复杂介质中波的传播不确定性分析方法 [J]. *电子与信息学报*, 2021, 43 (12): 3662-3670.
- 14 POP R, FULOP P. Deep ensemble bayesian active learning: Addressing the mode collapse issue in monte carlo dropout via ensembles [J]. *arXiv preprint arXiv: 1811.03897*, 2018.
- 15 LALSHMINARAYANAN B, PRITZEL A, BLUNDELL C. Simple and scalable predictive uncertainty estimation using deep ensembles [C] // *Advances in neural information processing systems*. 2017.
- 16 GANAIE M A, HU M, TANVEER M, et al. Ensemble deep learning: A review [J]. *arXiv: 2104.02395*, 2021.
- 17 RAHAMAN R. Uncertainty quantification and deep ensembles [C] // *Neural Information Processing Systems*. 2021.
- 18 TOUVRON H, LAVRIL T, IZACARD G, et al. LLaMA: Open and efficient foundation language models [J]. *arXiv pre-print arXiv: 2302.13971*, 2023.
- 19 ABADR M, POURPANAH F, HUSSAIN S, et al. A review of uncertainty quantification in deep learning: Techniques, applications and challenges [J]. *Information Fusion*, 2021: 76.
- 20 BROWN K, HUIYAN F, TALBERT D. Uncertainty quantification in multimodal ensembles of deep learners [J]. In the thirty-third international flairs conference, 2020.
- 21 KUHN L, GAL Y, FARQUHAR S. SEMANTIC Uncertainty: Linguistic Invariances for Uncertainty Estimation in Natural Language Generation [C] // *InThe Eleventh International Conference on Learning Representations*. 2022.
- 22 DUAN J, CHENG H, WANG S, et al. Shifting attention to relevance: Towards the uncertainty estimation of large language models [J]. *arXiv preprint arXiv: 2307.01379*, 2023.
- 23 CHEN C, LIU K, CHEN Z, et al. INSIDE: LLMs' Internal States Retain the Power of Hallucination Detection [C] // *In The Twelfth International Conference on Learning Representations*. 2023.
- 24 LIN Z, TRIVEDI S, SUN J. Generating with confidence: Uncertainty quantification for black-box large language models [J]. *arXiv preprint arXiv: 2305.19187*, 2023.
- 25 田星, 郑瑾, 张祖平. 基于词向量的 Jaccard 相似度算法 [J]. *计算机科学*, 2018, 45 (7): 186-189.
- 26 KADAVATH S, CONERLY T, Askill A, et al. Language models (mostly) know what they know [J]. *arXiv preprint arXiv: 2207.05221*, 2022.
- 27 MALININ A, GALES M. Uncertainty estimation in auto-regressive structured prediction [J]. *arXiv preprint arXiv: 2002.07650*, 2020.
- 28 邢海花, 陈焕东, 林红燕. 基于输入扰动的分层混合模糊-神经网络敏感性分析 [J]. *软件*, 2013, 34 (2): 52-55.

- 29 HENDRYCKS D, BASART S, MU N, et al. The many faces of robustness: A critical analysis of out-of-distribution generalization [C] //InProceedings of the IEEE/CVF international conference on computer vision. 2021.
- 30 LI B, WANG R, WANG G, et al. Seed-bench: Benchmarking multimodal llms with generative comprehension [J]. arXiv preprint arXiv: 2307.16125, 2023.
- 31 VAN A J, SMITH L, TEH YW, et al. Uncertainty estimation using a single deep deterministic neural network [J]. InInternational conference on machine learning, 2020, 21: 9690-9700.

基于算子融合和向量化访存的大语言模型部署优化研究**

明刚¹ 张艳霞¹ 李旭胜¹ 叶子扬¹ 冯力¹
邢焕来¹ 朱宗海^{1*}

摘要 随着自然语言处理模型参数量的增加，推理效率和资源利用效率成为大语言模型部署的关键挑战。为了应对这一挑战，文章利用算子融合技术和向量化访存技术优化模型推理速度和资源利用率。实验过程中，选用 LLaMA-7B 和 LLaMA-13B 作为基础模型，并通过使用 Wikitest 数据集进行实验评估未优化模型与优化模型的推理时间和困惑度 (Perplexity, PPL)。实验结果显示，所提出的优化方法能够在困惑度保持不变的情况下，有效地减少推理时间，并保持优化后的模型预测准确性。同时，文章通过理论分析和实验证明所提出的算子融合技术和向量化访存技术能有效提升模型推理效率，为未来大规模自然语言处理模型的部署和应用提供了有效的优化路径。

关键词 算子融合，向量化访存，大语言模型，推理性能

Optimization of Large Language Model Deployment Based on Operator Fusion and Vectorized Visits**

MING Gang¹ ZHANG Yan-Xia¹ LI Xu-Sheng¹ YE Zi-Yang¹ FENG Li¹
XING Huan-Lai¹ ZHU Zong-Hai^{1*}

Abstract As the number of natural language processing model parameters increases, reasoning efficiency and resource utilization efficiency become key challenges in the deployment of large language models. To address this challenge, this paper utilizes operator fusion and vectorized access techniques to optimize model inference speed and resource utilization. During the experiments, LLaMA-7B and LLaMA-13B are selected as the base models, and the reasoning time and perplexity (PPL) of the unoptimized and optimized models are evaluated through experiments using the Wikitest dataset. The experimental results show that the proposed optimization method can effectively reduce the inference time and maintain the prediction accuracy of the optimized model while the perplexity remains constant. Meanwhile, this paper demonstrates through theoretical analysis and experiments that the proposed operator fusion technique and vectorized access technique can effectively improve the model inference effi-

** 四川省科技计划资助 (2024NSFSC1472)

** Supported by Sichuan Science and Technology Program (2024NSFSC1472)

* 通讯作者

1. 西南交通大学

1. School of Computing and Artificial Intelligence, Southwest Jiaotong University

ciency, and provide an effective optimization path for the deployment and application of large-scale natural language processing models in the future.

Key words operator fusion, vectorized access, large-scale language model, inference performance

0 引言

近年来,随着大型语言模型(Large Language Model, LLM)^[1]的兴起,其在自然语言处理任务中的应用已成为人工智能领域的热点^[2]。随着MLC-LLM^[3]、LLaMA.cpp^[4]等项目的出现,提高了LLM在消费级显卡甚至个人计算机上的推理速度,降低了大模型部署对硬件资源的需求,从而使更多人从大模型中获益^[5]。如在CMU陈天奇团队的MLC项目中,不管是Nvidia RTX还是AMD Radeon消费级显卡都取得了很不错的推理速度。相比于MLC,LLaMA.cpp是一个相对早期的LLM推理引擎开源项目,其架构设计通过CPU/GPU进行混合来加速推理任务,甚至可以仅依靠CPU完成推理。然而,随着LLM规模的增大和任务的复杂性,LLaMA.cpp在处理大规模模型时面临内存需求和计算效率方面的挑战。

2023年12月,上海交大IPADS实验室发布了PowerInfer开源项目,该项目在LLaMA.cpp基础上基于LLM推理中的高局部性特征^[6],设计了一种全新的推理方式。该局部性具体表现为神经元激活的幂律分布,即少数“热”神经元在不同输入下保持激活,而大多数“冷”神经元根据具体输入变化。PowerInfer充分利用了这一特点,设计了一种GPU-CPU混合推理引擎,通过将热激活的神经元预加载到GPU中,而将冷激活的神经元计算在CPU上,从而显著降低了GPU内存需求和CPU-GPU数据传输。目前该项目也已经

在LLaMA2-7B模型上实现了Nvidia和AMD GPU的支持。

为了进一步提升LLaMA模型的推理效率,本文研究了一种基于算子融合^[7]和向量化访存^[8-13]的优化方法。算子融合通过将多个计算算子合并为单个算子,从而减少计算过程中的冗余操作和内存访问的技术。向量化访存则是利用处理器的向量处理能力,即通过一次操作处理多个数据元素,从而减少内存访问次数,提高数据吞吐率。这两种方法在提升计算效率以及减少内存使用方面,对大规模模型的优化具有重要意义。

本文首先分析了LLaMA模型的结构及其主要计算瓶颈,其次接着介绍了算子融合和向量化访存的基本原理和实现方法,并从理论上分析了技术的可行性,最后通过实验验证了该优化方法的有效性。通过算子融合和向量化访存的应用,LLaMA模型在推理速度和内存使用方面得到了提升,为大型语言模型的高效部署提供了一种可行的解决方案。

1 LLaMA 模型架构

LLaMA模型代表了一种先进的人工智能技术,能够在自然语言处理(Natural Language Processing, NLP)任务上表现出卓越的能力,如文本生成、问答、对话交互、机器翻译以及其他基于语言的理解和生成任务。LLaMA模型家族包含了多个不同参数规模的模型版本,这些模型的参数量从70亿(7B)至650亿(65B)不等^[14]。这些模型设计借鉴了Chinchilla^[15]

模型的研究成果，注重在有限的训练数据和计算资源条件下实现最佳性能表现。值得注意的是，虽然 LLaMA 模型在参数量上可能小于某些其他顶尖模型，但在实际应用中却展现出了极高的效率和性能，例如，130 亿参数的 LLaMA 模型在很多基准测试上的性能可与 OpenAI 的 GPT-3 相媲美^[16]，而更大规模的 650 亿参数模型甚至超越了 Google 的 PaLM 模型的部分性能^[17]。

尽管 LLaMA 系列模型以其卓越的性能和广泛的应用潜力在人工智能领域独树一帜，展现出了非凡的语言理解和生成能

力。然而，庞大的模型规模和计算密集型的特点，对部署环境提出了极为严苛的要求，严重阻碍了 LLaMA 系列模型在算力有限的个人电脑（PC）上的部署。鉴于此现状，上海交大 IPADS 实验室研究发现了大语言模型内在的幂律规律，在此规律上开发了 PowerInfer 推理框架，该框架能在保证模型性能的同时，显著提升推理速度，从而极大地缓解了在资源受限环境下部署大型语言模型的困境，为大模型的普及应用开辟了一条崭新的路径。图 1 所示是 PowerInfer 中 LLaMA2 模型的结构。

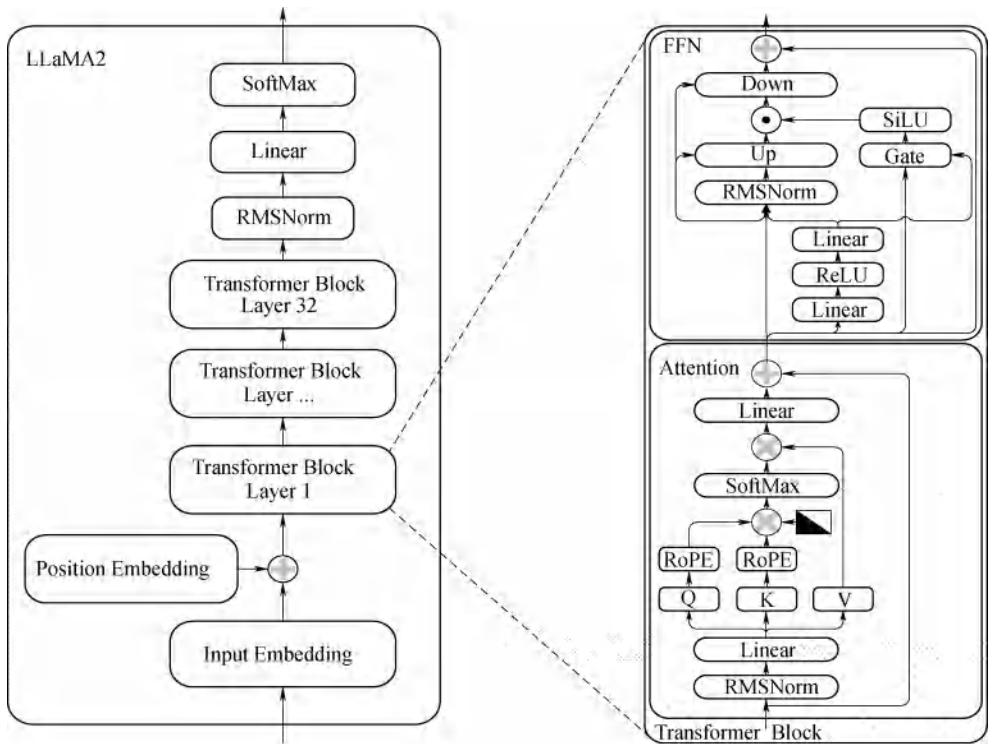


图 1 PowerInfer LLaMA2 模型结构

LLaMA 作为一种 Decoder-Only 结构，只用了 Transformer 的 Decoder 部分。由于 Decoder - Only 架构采用了 Masked Attention，其对应输出为满秩的下三角矩阵，因此，可以有效避免低秩问题会带来表达能力的下降，使得模型的表达能力

不受影响。LLaMA 和 LLaMA2 模型结构基本一致，LLaMA2 结构如图 1 左半部分所示，其中每个 Decoder 层如图 1 右半部分所示。主要是将 Transformer 中的 Layer-Norm 换成了 RMSNorm，Multi - Head Attention 换成了 GQA（LLaMA 是 MQA），

Positional 换成了 RotaryEmbedding (RoPE 相对位置编码)^[14]。

PowerInfer 为了充分利用神经元激活的幂律分布, 在原来的 LLaMA2 模型 FFN (Feed Forward Net) 中添加了一个小的预测神经网络 MLP (Multilayer Perceptron)^[18]。该网络具备前瞻性预测能力, 能够依据当前输入数据, 精准预判 FFN (全连接前馈网络) 架构下 Up、Gate 及 Down 各功能模块内神经元的激活状态, 从而在推理流程中, 动态识别并聚焦于关键神经元的活动, 显著提升计算效率与响应速度。

2 优化策略

2.1 算子融合

算子融合 (Operator Fusion) 作为一种有效的优化技术, 常用于深度学习和其他计算密集型任务中。算子融合的基本操作是将多个连续的操作或算子合并成一个单一的算子, 从而达到减少计算和内存开销的目的。通过使用算子融合技术, 可以提高执行效率, 并减少数据传输和临时存储的需要, 从而极大地提高缓存利用率。作为一种直接的优化方法, 其核心思想是“少动数据多计算”, 通过这种方式达到了有效利用计算资源的目的^[19]。算子融合的主要优势体现在: ①减少内存访问; ②降低计算开销; ③优化内存使用; ④提高硬件利用率。这些方面的显著成效使得算子融合成为深度学习模型优化的关键手段。

在传统的模型计算中, 算子之间的数据传递通常需要频繁访问内存, 每次访问都会带来额外的延迟和带宽消耗。而算子融合通过将多个独立操作合并为一个整体操作, 减少了模型计算过程中的内存访问

次数, 有效地降低了延迟和带宽开销, 并极大地提升整体计算速度。此外, 合并后的算子可以共享中间结果, 避免了重复计算。例如, 将卷积操作和激活函数融合为一个操作后, 不仅减少了计算量, 还进一步优化了计算资源的利用。算子融合还能通过减少中间结果的存储需求, 降低内存占用, 这对于嵌入式设备或移动设备等资源受限的环境尤为重要。通过减少内存的占用, 算子融合在这些设备上运行深度学习模型时表现出更高的效率和性能。针对专为大规模并行计算设计的 GPU 和 TPU, 算子融合技术能更好地利用这些硬件资源, 减少因小算子之间的同步和调度带来的性能损失, 从而进一步提高硬件利用率^[20]。

综上所述, 算子融合将多个独立的计算操作或算子合并为一个更大的操作或算子, 从而达到提高计算效率和减少内存访问次数为目标。此外, 通过减少数据在内存和缓存之间的传输次数, 算子融合降低了内存访问的成本。同时, 算子融合利用计算设备的计算能力更有效, 提高了硬件的利用率。在深度学习等领域, 算子融合简化了复杂的计算图结构, 优化了模型的训练和推断效率。在编译器优化和图像处理等领域, 算子融合技术被广泛应用, 显著提升了代码生成和数据处理的速度与效率。

2.2 向量化访存

向量化访存技术是计算机科学领域中用于提高内存访问效率的一种方法, 特别是在 GPU 相关的并行计算架构中。向量化访存技术的核心在于利用处理器的向量处理能力, 通过一次操作处理多个数据元素, 从而减少内存访问次数, 提高数据吞吐率。

向量化访存是指在并行计算中，多个处理器核心或线程同时访问连续的内存位置，以减少内存访问的次数。在 GPU 中，一个 warp（一组 32 个线程）可以被设计为同时访问连续的内存地址^[21]，这样 GPU 的内存系统可以将这一组连续的访问合并成一个单一的内存事务，从而显著减少所需的内存带宽。

在非向量化访存中，每个线程或处理器核心独立访问内存，即使访问的是相邻的内存位置，每次访问也会产生一个独立的内存事务。相比之下，在向量化访存中，一组连续的访问可以被合并成一个事务，降低了内存访问的开销。以下是关于向量化访存的分析。

假设有一个 GPU，每个线程访问 4 字节的数据（例如，一个浮点数）。考虑一个 warp（32 个线程）访问全局内存的情况。

在没有使用向量化访存技术的情况下，每个线程访问一个单独的地址，因此，会有 32 次独立的内存访问，总数据量为： $D = 32 \times 4\text{bytes} = 128\text{bytes}$ ，总事务数为： $N_{non_vec} = 32$ ；而在使用向量化访存的情况下，所有 8 个线程，每个线性访问连续 16 个字节的地址，因此，会有 8 次独立的内存访问，即总数据量还是 $D = 128\text{bytes}$ ，总事务数 $N_{vec} = 8$ 。

在带宽利用率方面，非向量化访存的带宽利用率：

$$B_{non_vec} = \frac{D}{N_{non_vec}} \times (\text{事务开销}) \quad (1)$$

向量化访存的带宽利用率：

$$B_{vec} = \frac{D}{N_{vec}} \times (\text{事务开销}) \quad (2)$$

带宽利用率对比：

$$\frac{B_{vec}}{B_{non_vec}} = \frac{N_{non_vec}}{N_{vec}} = 4 \quad (3)$$

式中，事务开销为完成一次内存事务所需的时间或资源消耗。

从上面的公式可以看出，对于相同的总数据量，向量化访存的带宽利用率是非向量化访存的 4 倍。换句话说，向量化访存能显著减少内存访问的次数，从而提高内存带宽的利用率，减少延迟，最终提升整体的计算性能。

2.3 算子融合算法设计

算子融合算法设计旨在将相邻的计算操作合并为更大的单元，以减少计算图复杂度和内存访问开销，提升算法效率和硬件利用率。本文将 Transformer Block 中的不同部分的部分算子融合成一个较大的算子，为了简单起见，以两个算子的融合为例进行详细分析。

假设有两个独立的算子 O_1 和 O_2 ，分别具有计算复杂度 C_1 和 C_2 。每个算子都需要读取和写入数据，输入矩阵表示为 X ，而权重矩阵表示为 W 。那么 O_1 接收输入矩阵 X 和权重矩阵 W_1 ， O_2 接收 O_1 的输出和权重矩阵 W_2 ，假设读写数据的复杂度分别为 M_r 和 M_w 。那么，这两个算子单独执行时的总计算复杂度为：

$$T_{original} = 2M_r + C_1 + M_w + 2M_r + C_2 + M_w \quad (4)$$

可以简化为：

$$T_{original} = C_1 + C_2 + 4M_r + 2M_w \quad (5)$$

当融合这两个算子为一个复合算子 O_{fused} 时，假设融合后的算子的计算复杂度为 C_{fused} ，它等于两个算子的计算复杂度之和，即 $C_{fused} = C_1 + C_2$ 。因此，融合后的总计算复杂度为：

$$T_{fused} = 3M_r + C_{fused} + M_w \quad (6)$$

算子融合可以减少数据移动的次数，从而降低计算复杂度。具体变化为：

$$\begin{aligned}
\Delta T &= T_{original} - T_{fused} \\
&= (C_1 + C_2 + 4M_r + 2M_w) \\
&\quad - (3M_r + C_{fused} + M_w) \\
&= M_r + M_w \quad (7)
\end{aligned}$$

从上面的公式可以看出，使用了算子融合，可以减少一次中间计算结果的读取和写入时间，同时节省中间计算结果的存储空间。

算子融合本身不会改变模型的表达能力。它仅改变了模型的执行路径，优化了计算效率。因此，融合后的模型仍然能够学习和表示与融合前相同的函数映射，即：

$$f_{fused}(X) = f_2(f_1(X)) \quad (8)$$

算子融合可能会导致模型参数的重新组织，但不会改变参数的总数。例如，对于两个连续的全连接层，融合后的权重矩阵 W_{fused} 可以表示为：

$$W_{fused} = W_2 \cdot O_1(W_1) \quad (9)$$

这里， W_{fused} 的形状和元素取决于 W_1 和 W_2 的形状和元素，但其参数总数不变。算子融合通过重新组合权重矩阵，提高了计算效率，但没有增加模型的参数复杂度。

2.3.1 QK^T/scale 算子的融合

算子融合中的 QK/scale 是指在自注意力机制 (Self-Attention)^[22-23] 中常用的一种优化技术，它结合了注意力矩阵计算中的三个基本步骤：QK (Query 和 Key 的乘积)、Scale (缩放)、Softmax^[24]。这些步骤通常用于 Transformer 模型中，用于计算输入序列中每个位置的注意力分布。

在自注意力机制中，每个输入向量 (通常是来自前一层的输出) 都有三种线性变换形式：Query (查询)、Key (键) 和 Value (值)。QK 操作即是将每个输入向量作为 Query 和 Key 来计算相似度，通常表示为乘积：

$$AttentionScores = Query \times Key^T \quad (10)$$

这里的乘积结果表示了 Query 向量和 Key 向量之间的相似度，也可以理解为注意力分数的初步计算结果。

缩放操作是为了控制注意力分数的大小，通常通过除以一个常数来实现。常见的做法是将注意力分数除以 Query 或 Key 向量的维度的平方根 (通常是 $\sqrt{d_k}$ ，其中 d_k 是 Key 向量的维度)。这一步骤的目的是确保不同维度的向量在计算注意力分数时具有相似的量级，有助于稳定模型的训练和推理过程。

这两个步骤 (QK、Scale) 被合并为一个更大的操作单元，合并前后的情况如图 2 所示。

这种算子融合有助于降低计算图的复杂度，减少了在不同步骤之间数据的传输和存储开销，从而提高模型推理的速度和效率。

2.3.2 FFN 中 Linear 与 ReLU 算子融合

LLM 体系结构包括多个 Transformer 层，每个层都包含一个自注意力块和一个 FFN (前馈网络) 块。在模型开始服务前，PowerInfer 首先会对模型进行离线分析，通过将模型在通用数据集中进行推理获取每一层输入与激活神经元之间的激活关系，进而为稠密模型每一层训练一个小的预测路由模块 (MLP 块) 来预测每一个输入会激活的神经元，MLP 块只计算路由激活的神经元，MLP 是由两个 Linear、一个 ReLU (Rectified Linear Unit)^[25] 块组成的，算子融合将第一个 Linear 与 ReLU 融合，其融合前后对比如图 3 所示。

将 Linear 与 ReLU 操作进行融合，直接在计算流程中整合 ReLU 激活函数，而不是作为单独的后续步骤。ReLU 函数定义为：

$$f(x) = \max(0, x) \quad (11)$$

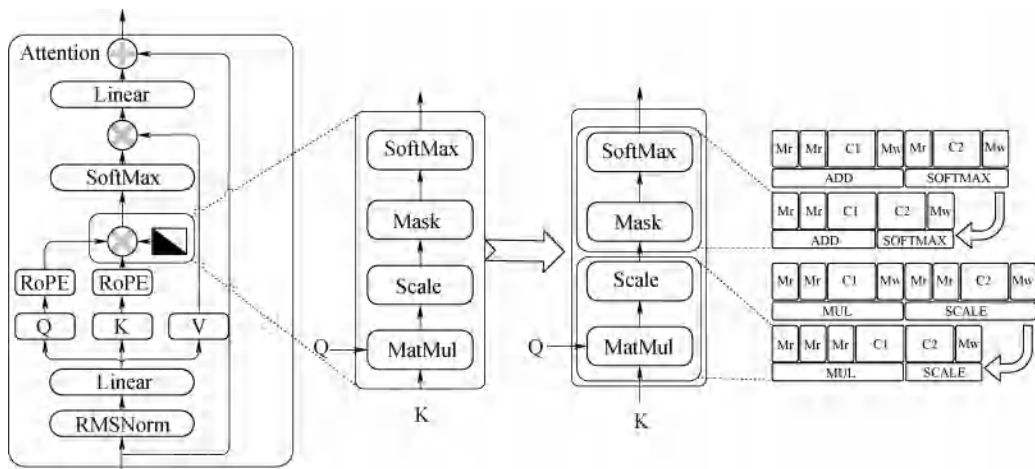


图 2 算子融合示意图

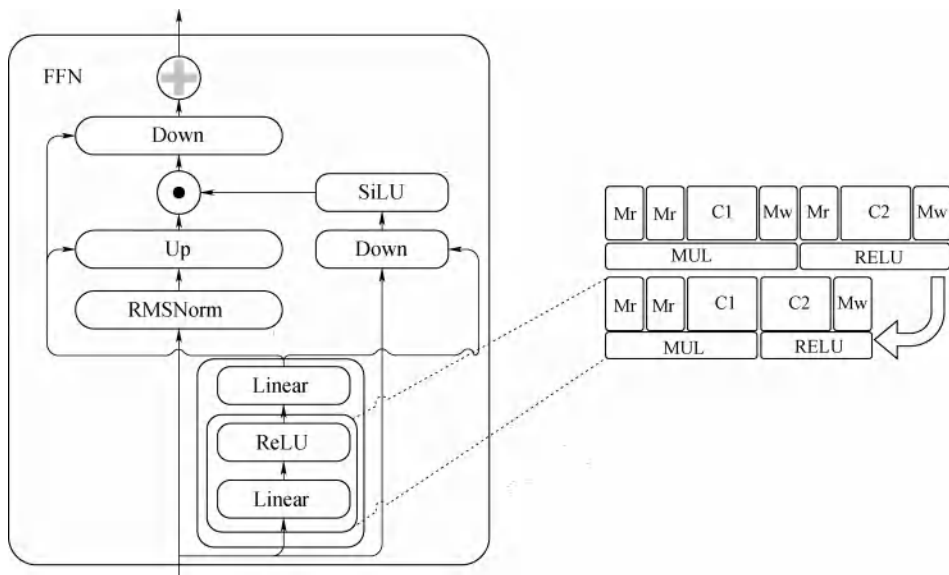


图 3 Linear 与 ReLU 算子融合

经过算子融合后的计算公式为：

$$f(\mathbf{W} \times \mathbf{I}) = \max(0, \mathbf{W} \times \mathbf{I}) \quad (12)$$

式中， \mathbf{W} 为 Linear 的权重矩阵； \mathbf{I} 为 Linear 的输入。

2.3.3 Masked 与 softmax 算子融合

在 LLaMA 的自注意力层中，通常需要对注意力分数应用掩码，以防止模型访问未来位置的信息。这一步骤涉及将掩码矩阵（通常为一个包含 0 和 $-\infty$ 的矩阵）与

注意力分数矩阵相加。掩码矩阵的形状通常与注意力分数矩阵相同。

在加上掩码操作后，得到的注意力分数矩阵需要经过 Softmax 函数处理，将注意力分数转换为每个位置的概率分布。Softmax 函数的计算公式如下：

$$\text{Softmax}(A_{ij}) = \frac{e^{A_{ij}}}{\sum_k e^{A_{ik}}} \quad (13)$$

式中, A 为加上掩码后的注意力分数矩阵; A_{ij} 为矩阵中第 i 行第 j 列的元素。

3 实验与结果

实验环境为: CPU Intel (R) Core (TM) i7-12700K, GPU NVIDIA RTX3090, 所有对比实验均在此环境下进行。在实验过程中, 首先, 分别对使用了算子融合技术和未使用算子融合技术的运算效果进行了比较。其次, 将两类算子加入 PowerInfer 框架中进行对比分析。最后, 在两类算子中应用向量化访存技术, 并将其加入 PowerInfer 框架中进行对比分析。

3.1 算子对比

为了更为直观地观察几类算子融合带来的效果, 试验将几类算子从推理框架中拆分出来。在运算操作的效率方面, 分别进行了算子融合和未进行算子融合的运算操作的对比分析。实验过程中, $QK^T/scale$ 的效果分别在一个 $[128, 1, 32]$ 的张量和一个 $[128, 512, 32]$ 的张量中进行验证, Linear 与 ReLU 的效果分别在一个 $[1, 2048]$ 的向量和一个 $[2048, 2048]$ 的矩阵中进行验证, Masked 与 Softmax 会在一个 $[32, 1, 32]$ 的张量上进行验证。实验结果如表 1 所示。

表 1 算子运算效果对比

算子	未融合算子/ μs	融合算子/ μs
$QK^T/scale$	99	91
Linear 与 ReLU	216	207
Masked 与 Softmax	80	73

从表 1 的结果可以看出, 融合算子的计算效率相较于非融合算子, 计算效率有明显提升。在实际的 LLaMA 推理过程中, 由于存在大量相同的算子, 这样多数量算

子进行叠加产生的效果反应在最终的推理效果中也较为明显。

3.2 Powerinfer 结合算子融合

为进一步验证算子融合与 Powerinfer 推理框架相结合的效果, 在实验过程中, 本文使用 LLaMA-7B 和 LLaMA-13B 作为基础大语言模型并在 wikitest 数据集上进行实验。评估指标包括推理时间、困惑度 (Perplexity, PPL)^[26] 得分。

首先, 加载未经算子融合优化的基准 LLaMA 模型和经过算子优化的相同大小 LLaMA 模型。其次, 分别对这两个模型使用 wikitest 数据集进行推理。在算法推理过程中, 将数据集分成批次, 记录每个批次的推理时间和内存使用量。最后, 计算模型在 wikitest 数据集上的困惑度 (PPL), 其中困惑度的计算公式为:

$$PPL = \exp\left(\frac{L_{total}}{N_{total}}\right) \quad (14)$$

式中, L_{total} 为累加的损失值; N_{total} 为总词数。最终结果如表 2 所示。

如表 2 的实验结果所示, 算子融合优化对大模型 LLaMA-7B 和 LLaMA-13B 的性能产生了明显影响。在提示评估阶段 (prompt eval), 优化前后的模型处理每个 token 的时间接近。具体表现为 LLaMA-7B 从 19.74ms/token 增加到 19.84ms/token, LLaMA-13B 从 23.10ms/token 减少到 22.84ms/token。这是在模型推理过程中的正常现象, 因为包括 prompt eval、generate eval 以及 PPL 在内, 都会出现微小增加或者减少。此外, 算子融合优化并未改变模型的困惑度 (PPL), LLaMA-7B 和 LLaMA-13B 在优化前后的困惑度均保持不变, 分别为 6.60 和 5.84。实验结果表明模型在语言理解和生成能力方面保持稳定。

表 2 Powerinfer 结合算子融合

指标类型	未优化模型		优化模型	
	LLaMA-7B	LLaMA-13B	LLaMA-7B	LLaMA-13B
prompt eval/(ms/token)	19.74	23.10	19.84	22.84
generate eval/(ms/token)	50.06	59.82	49.12	58.31
PPL	6.66	5.82	6.60	5.84

在生成评估阶段 (generate eval), 算子融合优化展现出了显著的优势, 优化后的模型处理每个 token 的时间减少, LLaMA-7B 从 50.06ms/token 减少到 49.12ms/token, LLaMA-13B 从 59.82ms/token 减少到 58.31ms/token。这表明算子融合优化在减少不必要的中间数据传输和存储, 提高计算效率方面发挥了重要作用。生成评估阶段的效率提升对于大模型的实际应用至关重要, 特别是在需要实时响应和高吞吐量的场景中, 这种优化能够显著提高系统的响应速度和处理能力。整体而言, 算子融合优化在生成阶段实现了预期的性能提升, 同时保持了模型的困惑度 (PPL) 不变, 验证了其有效性和可靠性。

3.3 向量化访存

基于上述结合了算子融合技术的 PowerInfer 框架, 再结合向量化访存技术, 分

别对两类融合算子进行对比实验。在实验过程中, 与上文相同, 使用 LLaMA-7B 和 LLaMA-13B 作为基础大语言模型并在 wikitest 数据集上进行实验。评估指标同样包括推理时间、困惑度 (PPL) 得分。

结果如表 3 所示, 通过进一步结合向量化访存优化, 可以显著地对大模型 LLaMA-7B 和 LLaMA-13B 的性能产生影响。在提示评估阶段 (prompt eval), 优化后的模型在处理每个 token 的时间上有所减少, 具体表现为 LLaMA-7B 从 19.74ms/token 减少到 18.41ms/token, LLaMA-13B 从 23.10ms/token 减少到 20.90ms/token。同时, 值得注意的是, 序列化访存优化并未对模型的困惑度 (PPL) 产生影响, LLaMA-7B 和 LLaMA-13B 在优化前后的困惑度均保持不变, 分别为 6.62 和 5.83。实验结果表明, 向量化访存能保持模型在语言理解和生成能力方面的稳定。

表 3 Powerinfer 结合算子融合与序列化访存

指标类型	未优化模型		优化模型	
	LLaMA-7B	LLaMA-13B	LLaMA-7B	LLaMA-13B
prompt eval/(ms/token)	19.74	23.10	18.41	20.90
generate eval/(ms/token)	50.06	59.82	44.88	53.22
PPL	6.66	5.82	6.62	5.83

在生成评估阶段 (generate eval), 向量化访存优化同样展现出了显著的优势, 优化后的模型处理每个 token 的时间有所减少, LLaMA-7B 从 50.06ms/token 减少到 44.88ms/token, LLaMA-13B 从

59.82ms/token 减少到 53.22ms/token。结果表明向量化访存优化在减少访存次数, 提高计算效率方面发挥了重要作用。整体而言, 向量化访存优化在提示评估阶段和生成阶段实现了预期的性能提升, 同时保

持了模型的困惑度 (PPL) 不变, 验证了其有效性和可靠性。

4 结束语

为了应对模型规模扩大带来的计算和内存挑战, 本文提出了结合算子融合和向量化访存技术的方法, 通过减少计算图复杂度和优化内存访问, 优化了大规模语言模型 LLaMA 的部署性能。实验结果表明, 算子融合技术和向量化访存技术有望提升模型的推理速度和资源利用率。实验过程以 LLaMA-7B 和 LLaMA-13B 模型为对象, 在 wikitest 数据集上进行了详尽的实验对比, 评估了优化前后的推理时间和困惑度 (PPL) 表现。

此外, 实验结果展示了算子融合优化与向量化访存优化的优势, 这两种方法在提升 LLaMA 模型推理效率方面展现出的稳健效果, 尤其在确保优化方案的稳定性和安全性方面效果显著, 是提升模型推理速度的有效途径。这些优化手段能够缩短大模型的推理时间, 在促进大规模模型于资源受限环境中的高效部署方面扮演着不可或缺的角色, 在 LLaMA-7B 和 LLaMA-13B 模型上的优化成果都较为显著。

总体而言, 算子融合技术和向量化访存技术在确保模型性能的前提下, 展示了优化推理效率的潜力。未来的研究应进一步结合更多的优化方法和硬件特性, 探索更有效的部署策略, 以进一步提升大规模自然语言处理模型的运行效率和实际应用效果, 为大规模 AI 模型在各类应用中的广泛普及提供更有力的技术支持和保障。

参考文献

1 CHANG Y, WANG X, WANG J, et al. A survey

on evaluation of large language models [J]. ACM Transactions on Intelligent Systems and Technology, 2024, 15 (3): 1-45.

2 ZHAO C, ZHU G, WANG J. Implications of ChatGPT for linguistic macromodeling and new development ideas for multimodal macromodeling [J]. Data Analysis and Knowledge Discovery, 2023, 7 (3): 26-35.

3 LI Y, WEN H, WANG W, et al. Personal llm agents: Insights and survey about the capability, efficiency and security [J]. arXiv preprint arXiv: 2401.05459, 2024.

4 SHEN H, CHANG H, DONG B, et al. Efficient llm inference on cpus [J]. arXiv preprint arXiv: 2311.00502, 2023.

5 TOUVRONH, LAVRIL T, LZACARD G, et al. Llama: Open and efficient foundation language models [J]. arXiv preprint arXiv: 2302.13971, 2023.

6 SONG Y, MI Z, XIE H, et al. Powerinfer: Fast large language model serving with a consumer-grade gpu [J]. arXiv preprint arXiv: 2312.12456, 2023.

7 NIU W, GUAN J, WANG Y, et al. Dnnfusion: accelerating deep neural networks execution with advanced operator fusion [C] //Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation. 2021: 883-898.

8 FENG J, HE Y, PAO Q. Evaluation of compilers' capability of automatic vectorization based on source code analysis [J]. Scientific Programming, 2021, 2021 (1): 3264624.

9 HAJ-ALI A, AHMED N, WILLKE T, et al. Neurovectorizer: End-to-end vectorization with deep reinforcement learning [C] //Proceedings of the 18th ACM/IEEE International Symposium on Code Generation and Optimization. 2020: 242-255.

10 ADIT N, SAMPSON A. Performance left on the table: an evaluation of compiler autovectorization for RISC-V [J]. IEEE Micro, 2022, 42 (5): 41-48.

11 DAGHAGHI S, MEISBURGER N, ZHAO M, et al. Accelerating slide deep learning on modern

- cpus: Vectorization, quantizations, memory optimizations, and more [J]. *Proceedings of Machine Learning and Systems*, 2021, 3: 156–166.
- 12 MUTLU O, GHOSE S, GÓMEZ-LUNA J, et al. A modern primer on processing in memory [M] // *Emerging computing: from devices to systems: looking beyond Moore and Von Neumann*. Singapore: Springer Nature Singapore, 2022: 171–243.
- 13 PENG X, SHI X, DAI H, et al. Capuchin: Tensor-based gpu memory management for deep learning [C] // *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*. 2020: 891–905.
- 14 TOUVRON H, MARTIN L, STONE K, et al. Llama 2: Open foundation and fine-tuned chat models [J]. *arXiv preprint arXiv: 2307.09288*, 2023.
- 15 HOFFMANN J, BORGEAUD S, MENSCH A, et al. Training compute-optimal large language models. *arXiv 2022* [J]. *arXiv preprint arXiv: 2203.15556*, 2022, 10.
- 16 MING Z. Research and discussion on big model evaluation methods in artificial intelligence [J]. *Big Data and Artificial Intelligence*, 2023, 4 (5): 19–21.
- 17 CHOWDHERY A, NARANG S, DEVLIN J, et al. Palm: Scaling language modeling with pathways [J]. *Journal of Machine Learning Research*, 2023, 24 (240): 1–113.
- 18 LIU Z, WANG J, DAO T, et al. Deja vu: Contextual sparsity for efficient llms at inference time [C] // *International Conference on Machine Learning*. PMLR, 2023: 22137–22176.
- 19 ZOU L, GONG X, ZHOU Q. Memory Management and System Optimization [J]. *Journal of Hebei Institute of Technology*, 2003, 25 (3): 63–66.
- 20 GUO L, ZHAO J, ZHAO J. Architecture design and optimization strategy of heterogeneous AI computing power operation platform [J]. *Information and Communication Technology and Policy*, 2022, 48 (3): 7.
- 21 HIJMA P, HELDENS S, SCLOCCO A, et al. Optimization techniques for GPU programming [J]. *ACM Computing Surveys*, 2023, 55 (11): 1–81.
- 22 HAN K, WANG Y, CHEN H, et al. A survey on vision transformer [J]. *IEEE transactions on pattern analysis and machine intelligence*, 2022, 45 (1): 87–110.
- 23 AGARAP A. Deep learning using rectified linear units [J]. *arXiv preprint arXiv: 1803.08375*, 2018.
- 24 SHAW P, USZKOREIT J, VASWANI A. Self-attention with relative position representations [J]. *arXiv preprint arXiv: 1803.02155*, 2018.
- 25 JOULIN A, CISSÉ M, GRANGIER D, et al. Efficient softmax approximation for GPUs [C] // *International conference on machine learning*. PMLR, 2017: 1302–1310.
- 26 PAL A, KARKHANIS D, ROBERTS M, et al. Giraffe: Adventures in expanding context lengths in llms [J]. *arXiv preprint arXiv: 2308.10882*, 2023.

基于智能体工作流的体系智能架构研究

李 广¹ 肖 一¹ 胡鹏举¹ 聂 璐^{1*} 赵晓宁¹

摘 要 文章提出了一种基于智能体工作流的体系智能架构,旨在通过构建面向作战 OODA 流程的智能体来实现作战的自主性和协同性。该架构引入了作战规则知识库、智能体管理器、工具管理器以及智能体 workflow 编排引擎,通过合适的提示工程、思维链架构、工具调用框架实现了智能体与模拟指挥控制系统的深度结合。设计了基于智能体工作流的作战流程运用实验,构建模拟了作战流程,表明该架构能够在作战任务中提高指挥员决策效率和准确性,为未来军事智能体系运用提供了有效支撑。

关键词 智能体, 工作流, 体系智能, 智能架构, 编排引擎

C2 System Intelligence Architecture Based on Agentic Workflow

LI Guang¹ XIAO Yi¹ HU Peng-Ju¹ NIE Lu^{1*} ZHAO Xiao-Ning¹

Abstract This paper proposes a system intelligence architecture based on agent workflows, aimed at achieving autonomy and synergy in combat operations by constructing agents oriented towards the OODA (Observe, Orient, Decide, Act) loop. The architecture introduces a combat rule knowledge base, an agent manager, a tool manager, and an agent workflow orchestration engine. It integrates agents deeply with a simulated command and control system through appropriate prompt engineering, chain-of-thought architecture, and tool invocation framework. An experiment utilizing a combat process based on agent workflows was designed to simulate combat procedures, demonstrating that this architecture can improve the efficiency and accuracy of command decision-making in combat tasks, thus providing effective support for the application of future intelligent military systems.

Key words agent, workflow, system intelligence, intelligent architecture, orchestration engine

0 引言

在过去的十年中,人工智能(AI)技术经历了飞速的发展,从简单的规则系统和基本的机器学习算法,逐步演变为今天的复杂深度学习和大规模预训练模型^[1]。

这种迅猛的进步不仅改变了战场技术研究的方向,更在多个军事应用领域带来了革命性的变化。尤其是近年来大模型(Large Models)的兴起,正在引发着以大模型为基础,大量不同垂类应用井喷式涌现,多样的 AI 新物种相继诞生,这也标志着人工智能进入了一个新的“寒武纪”时代^[2]。

* 通讯作者

1. 中国航天科技集团中国航天科技创新研究院

1. China Academy of Aerospace Science and Innovation (CASI), China Aerospace Science and Technology Corporation

人工智能领域的大模型也在技术能力和应用范围上实现了质的飞跃。这些大模型,如 GPT-4、BERT 和 DALL-E,不仅具备了前所未有的计算能力和学习能力,还展示了在语言理解、图像生成、复杂决策等方面的超凡表现。随着研究的不断深入,能够解决相应任务的智能体在军事领域也将发挥越来越大的作用,加速军事领域的新一代变革。

1 智能应用范式变革

人工智能技术的发展将为未来战争的形态带来范式的变革,相较于人类而言,人工智能可以发挥越来越关键的作用。

1.1 机器智能的优势

随着人工智能技术的快速进步,特别是大规模预训练模型的广泛应用,机器在许多特定任务中展现出了超越人类的智能水平^[3]。

一是在计算能力方面,现代计算机具备极高的计算能力,能够在极短时间内执行大量复杂计算。GPU 和 TPU 等专用硬件的出现进一步增强了这一能力,使得训练和运行复杂神经网络成为可能。相比之下,人类大脑虽然在某些认知任务上表现出色,但在处理大量数据和执行高频计算时远不及机器。二是在大数据处理与学习方面,机器学习模型能够处理和分析海量数据,从中提取模式和数据洞察。大数据时代的到来为这些模型提供了丰富的训练素材,使其能够在许多领域达到甚至超越人类专家的水平。例如,在目标影像分析中,深度学习模型通过分析大量标注数据,能够比指挥员更早地、更快地发现目标。三是在持续改进方面,机器学习模型可以通过不

断的训练和优化持续改进其性能^[4]。随着新数据的不断加入,模型能够动态适应和学习,保持其高效性和准确性。相比之下,人类的学习速度和记忆能力受到生理限制,无法持续以同样的速度进行自我提升^[5]。

1.2 人工智能应用的底层逻辑

人工智能的三要素是数据、算力、算法,人工智能应用就是在三要素基础上,建立数据之间的关联,预测可能的结果。数据是人工智能的基石,机器学习模型通过大量的数据进行训练,能够从中提取有价值的特征和模式。数据的丰富性、多样性、准确性直接决定了模型的表现。算法是将数据转化为有用信息的工具,是 AI 系统的核心,决定了如何从数据中提取特征、进行建模和做出预测,指导计算机如何处理数据的规则和步骤,它决定了机器如何从数据中提取有用的信息并做出决策。算力是人工智能的驱动力^[6]。算力指的是计算机处理数据的能力,包括计算速度、存储能力、通信能力等。在人工智能应用中,算力是支撑数据和算法运行的重要平台。随着数据量的爆炸式增长和算法复杂度的不断提高,对算力的需求也在不断增加^[7]。

人工智能的底层逻辑是在三要素基础上,通过数据的积累和处理,识别特征之间的相关性,建立知识之间的关联,并利用这些相关性进行认知、决策和行动。

1.3 智能体的进化论与个体劣势

军事领域要求人工智能可以辅助指挥官进行更快的决策。能够自主感知环境、做出决策并执行特定任务的人工智能系统可以称作智能体 (Agent)^[8]。大模型的出

现为智能体的构建提供了一种新思路，即大模型智能体（LMA）。智能体通过行动能够不断收集外界的反馈，同时能够利用反馈去改进自身，得到更优的能力，类似于生物的进化，逐步提升智能水平，最终在某些方面超越人类智能。其特征表现在如下方面：

(1) 自我进化与适应。机器智能通过持续学习和优化，实现自我进化。这一过程类似于生物进化中的自然选择和适应，机器通过从数据中学习，不断改进和提升其性能。

(2) 智能协作与生态。不同类型的智能机器将形成一个复杂的智能生态系统。在这个系统中，各类智能体相互协作，共

同学习和进化，推动智能应用的多样化和高效化。

(3) 人机协同与共融。在机器智能进化的过程中，人类将与智能机器逐步融合，通过充分利用机器的计算和数据处理能力，人类可以更高效地完成复杂任务，实现人机协作的最大化^[9-12]。

智能的体系运用需要完善的支撑与下一代运用模式。虽然智能能够在三要素基础上发挥更大的作用，但是单智能个体的能力并不能为体系运用带来能力的跃升，需要构建一种高效的智能体系运用架构，将多种智能体的能力进行组合，并将智能体融入体系运用流程，促进智能能力生成，如图 1 所示。

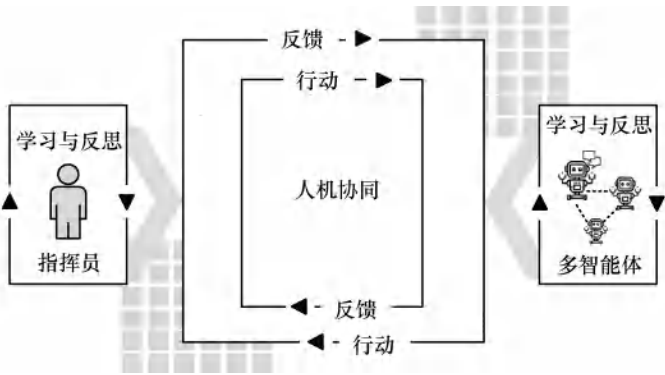


图 1 多智能体与指挥员协同模式

2 作战应用智能体与 workflow

2.1 智能体系与作战应用智能体

智能体系是通过现代化智能生产工具，将智能算法、模型赋能作战体系运用流程各个环节，全面增强态势认知能力、辅助决策能力、自主行动能力，加速OODA循环闭合流程的技术体系。

作战应用智能体是在传统智能体基础

上，通过接入战场指挥控制系统，构建并利用知识库、工具库，根据设定任务感知当前环境，自主进行规划决策、执行决策并完成任务的人工智能系统。

作战应用智能体是智能体系的重要组成部分，智能体系能够为作战应用智能体约束使用条件，多个作战应用智能体在体系中，多智能体可以通过协作的方式，担任不同的角色，接收不同数据、任务，智能体之间可以进行信息交互，通过这种方式来发挥出智能的体系效能，如图 2 所示。



2.2 作战应用智能体的局限性

作战应用智能体的个体化运用存在一定局限性。一是任务单一性和灵活性不足，作战环境复杂多变，任务需求多样。单个智能体通常专注于某一特定任务，如情报收集或目标打击。这种任务单一性导致智能体在面对多任务或需要灵活应对的作战环境时表现出明显的局限。二是感知与认知能力的限制，单个智能体的感知能力受限于其能力配置和算法设计，可能难以全面感知复杂战场环境。此外，单个智能体的认知能力有限，难以应对动态变化的战术形势和敌方策略。三是决策与执行的独立性约束，单个智能体在决策和执行过程中往往是独立操作的，缺乏与其他智能体或人类指挥官的有效协同。这种独立性可能导致局部最优而整体不协调的情况。例如，在复杂的战术行动中，需要多种不同的感知模型针对战场态势进行多维度的判别，如地形地貌、目标识别、态势预测等，需要多个智能体之间协同有序地进行组合决策，但单个智能体的独立决策可能导致协同不力，降低整体作战效能，如图3所示。



2.3 智能体工作流

为了克服单个智能体的局限性，智能体工作流 (Agentic Workflow) 通过多个智能体的协同工作，实现更高效和灵活的任务处理。在安德鲁 (Andrew Ng) 博士的近期研究中提到，智能体工作流有四种关键的设计方法，分别是反思 (Reflection)、工具使用 (Tool Use)、规划 (Planning) 和多智能体协作 (Multi-Agent Collaboration) 等^[13]。

2.3.1 反思

反思是指智能体在执行任务后对自己的表现进行评估和改进。例如，一个用于生成代码的智能体可以在生成代码后，自动检查代码的正确性、风格和效率，并给出改进建议。然后，智能体根据这些反馈重新生成改进后的代码。这种反思过程能够显著提高任务完成的质量和效率。

2.3.2 工具使用

智能体可以通过使用外部工具来增强其能力。例如，智能体可以利用搜索引擎获取实时信息，使用代码分析工具检查代码的正确性，或使用数据处理工具分析大量数据。这种工具集成方法不仅提高了智能体的任务处理能力，还弥补了单个智能体在特定任务中的能力不足。

2.3.3 规划

规划涉及智能体在执行任务前进行详细的计划和步骤设计。通过规划，智能体可以预见可能的挑战和障碍，制定应对策略，从而提高任务完成的成功率和效率。智能体可以通过规划来安排各个步骤的顺序和优先级，确保任务高效完成。例如，在态势认知任务中，智能体需要先对情报数据进行分析分类，然后根据类别调用相应的工具完成细分类别的目标识别，然后

整合各个工具的调用结果，再通过认知模型得到目标的关联关系等。

2.3.4 多智能体协作

多智能体协作指的是多个智能体之间的分工合作，共同完成复杂任务。每个智能体负责特定的子任务，彼此之间共享信息和资源，通过协作实现整体目标。多智能体系统（Multi-Agent System, MAS）中不同智能体可以专注于不同的任务模块，可以处理单个智能体无法胜任的复杂任务和动态环境^[14-15]。

3 体系智能架构

为了解决智能体在体系中的高效组合运用问题，本文提出了一种基于智能体工作流的体系智能架构。

体系架构组成如图 4 所示。硬件层包含基本的硬件资源，如 CPU、GPU、存

储、内存、传感器外设等，提供基本的硬件支撑；系统层包含操作系统、云原生环境、云计算环境、集群调度等，将硬件资源接入并进行虚拟化，为上层提供 PaaS 服务；运行环境依赖包含智能算法、模型以及软件等运行时所需的基本运行环境，主要为智能的应用提供服务。为了将智能体在体系中进行高效运用，结合智能体的工作模式，智能体应用层将包含三个管理器，即知识管理器、智能体管理器、工具管理器。

知识管理器。负责与业务相关的具体知识管理，能够针对文档、PDF、图像、表格等文件进行切分并向量化存储，为智能体的知识检索提供检索增强生成（RAG）服务。知识管理器的关键在于能够快速实现对已有知识的向量化存储，可以接入大语言模型（LLM）实现知识的高效索引。



图 4 体系智能架构组成

智能体管理器。能够管理接入系统的大模型智能体，包含上下文管理、记忆管理、调度管理等。上下文管理负责处理 LLM 生成过程中的上下文信息和状态的关键模块。它的主要功能包括上下文快照、恢复以及上下文窗口管理。上下文快照和恢复功能允许系统在智能体请求被调度器挂起时（即使 LLM 尚未完成对当前请求的响应生成），保存当前生成过程的状态。这样一旦资源再次可用，系统就可以从之前保存的状态恢复生成过程，从而继续生成响应，确保了临时挂起不会丢失进度，优化了资源的使用效率^[10]。

工具管理器。负责管理智能体可以调用的工具，包含建立统一的工具描述规范、对工具进行分类形成集合、建立工具能够执行的沙盒环境，以及提供用户自定义工具的能力，用于与用户的业务系统相关的工具设置。工具为智能体提供了丰富的能力，如果将智能体比作大脑，那么工具将成为智能体的眼睛与手足，让智能体可以感知外界并与之进行直接交互。

智能体编排引擎。负责实现与管理智

能体的行为与功能，并且可以与其他系统进行直接互动。通过逻辑关系、流程引擎、调试工具和提示嵌入等需求设计模块，智能体编排引擎定义了智能体的操作逻辑和流程控制。模型设计部分包括参数提取、代码执行、校验和解释器，确保智能体模型的准确性和有效性。工具设计部分通过工具 API 网关，提供了必要的工具和接口支持，实现智能体与外部系统的无缝交互。整体而言，智能体编排引擎在整个架构中起到中枢作用，确保智能体能够按照预定的逻辑和流程高效、准确地运行，同时支持在安全隔离的环境中进行调试和测试，从而不断优化和改进智能体的性能和功能。

体系智能架构统一应用程序编程接口（API）网关。作为一个提供标准化接口的枢纽组件，可管理和协调体系智能系统中的各个模块。通过定义统一的 API，支持将智能体工作流以 API 的方式实现对外服务，同时可以进行权限的管理，实现模块之间的数据传输和功能调用，确保系统的模块化、可扩展性和互操作性，如图 5 所示。

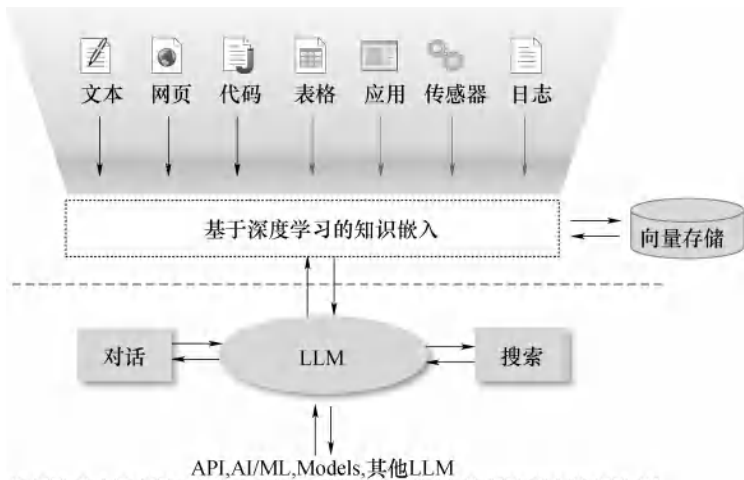


图 5 智能体与知识的交互

4 实验与验证

为了验证智能体 workflow 在指挥控制流程中的作用，搭建了如图 6 所示的实验验证系统。其构成包含模拟指控系统、智能服务平台、算力平台（搭载 Qwen2）以及云端通过 API 调用的 GPT-4o 模型。

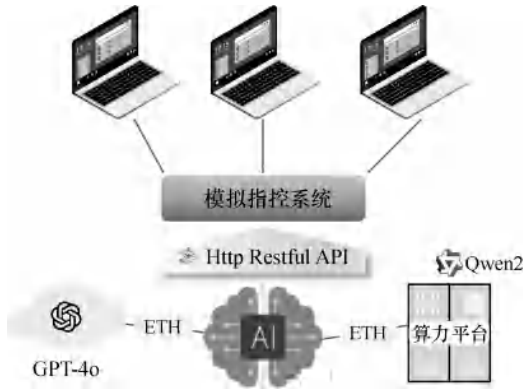


图 6 实验验证系统构成

表 1 我方资源池构建状态

类型	编号	状态	位置	时间窗口
侦察无人机	rd1	可用	A 基地	08:00—12:00
侦察无人机	rd2	使用中	B 基地	10:00—14:00
攻击无人机	ad1	可用	C 基地	06:00—10:00
攻击无人机	ad2	维护中	D 基地	14:00—18:00
侦察卫星	rs1	运行中	轨道	00:00—24:00
侦察卫星	rs2	维护中	轨道	00:00—24:00
常规导弹	cm1	可用	E 基地	08:00—20:00
常规导弹	cm2	使用中	F 基地	12:00—16:00
远程火箭	lrr1	可用	G 基地	09:00—17:00
远程火箭	lrr2	维护中	H 基地	15:00—19:00

4.1 实验设计

作战流程中，通常可以将作战活动分为 OODA，即观察、判断、决策、行动。本实验中，将通过构建虚拟的作战资源池、敌方目标列表、我方作战资源装备不同状态，包含可用、维修、使用中，通过问题的形式模拟发现目标到生成方案以及方案下发的过程。

我方作战资源池构建如表 1 所示。
敌方目标列表信息如表 2 所示。

表 2 敌方目标列表

编号	类型	位置
敌方步兵目标	步兵	A 区
敌方装甲车目标	装甲	B 区
敌方防空目标	防空	C 区

为了更好地对智能体的行为进行约束，智能体设计时加入了作战规则知识库，用于辅助智能体进行工具选择、方案生成等。

4.2 实验验证

智能体的反思通过 ReAct 框架进行工具使用的设计。智能体的迭代次数上限设置为 5 次，其初始提示词设计如图 7 所示。

能够看出，通过智能体的设计 workflow 设计，智能体能够自主按照任务需求进行工具迭代使用，同时能够将工具使用的结果进行统一输出，可以支撑智能体的体系化运用，如图 8、图 9 所示。

```

# 职位描述: 作战参谋助手
## 角色
我的主要目标是根据指挥官的要求进行相应的分析,告知指挥官需要关注的重要信息,帮助指挥官进行决策。
## 技能
### 技能1: 使用目标分析工具获取敌方目标状态。
### 技能2: 使用获取资源接口查询我方现有作战资源。
### 技能3: 使用方案生成接口生成可行行动方案。
### 技能4: 使用指令下发接口进行相关指令的下发。
## 工作流程
首先通过目标分析工具获取目标信息,其次根据我方作战资源情况,以时间窗口约束进行作战方案的生成,最后完成指令的下发。
## 限制
- 使用的语言应与用户的语言相同。
- 使用项目符号和Markdown语法给出结构化回答,逐步思考。

```

图7 智能体提示词设计



根据敌方目标情况,我方资源情况,生成作战方案。

Used combat-planmatch_get v

Used combat-plantime-window_get v

Used resources_get v

Used combat-plantime-window_get v

Used resources_get v

根据敌方目标情况和我方作战资源情况,生成了以下作战方案:

作战方案:

- 对敌方步兵目标 (ID: et1) 实施长程火箭弹打击:
 - 使用长程火箭弹 (ID: lrr1) 位于Base G进行打击。
 - 时间窗口: 09:00-17:00。
- 对敌方装甲目标 (ID: et2) 实施攻击无人机打击:
 - 使用攻击无人机 (ID: ad1) 位于Base C进行打击。
 - 时间窗口: 06:00-10:00。

指令下发:

- 下发长程火箭弹 (ID: lrr1) 从Base G对敌方步兵目标 (ID: et1) 进行打击。
- 下发攻击无人机 (ID: ad1) 从Base C对敌方装甲目标 (ID: et2) 进行打击。

以上是根据目标分析和我方资源情况生成的作战方案和指令下发。

图8 智能体 workflow 生成方案测试



图9 智能体 workflow 下发指令测试

5 结束语

通过设计基于智能体工作流的体系智能架构，结合作战 OODA 流程验证了智能体 workflow 在指挥控制流程中进行应用的可行性。通过引入作战规则知识库、智能体管理器和工具管理器，实现了智能体在作战运用过程中的自主性。智能体在态势感知、规划决策和任务执行方面表现出色，能够自主进行工具选择和方案生成，有效支撑复杂作战任务的体系化运用。该研究为未来智能体系的广泛应用提供了有力支撑，并为智能体技术在作战流程的进一步发展提供了基础。

参考文献

- 1 WANG F Y, MIAO Q H, LI X, et al. What does ChatGPT say: The DAO from algorithmic intelligence to linguistic intelligence [J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10 (3): 575-579.
- 2 孙柏林. ChatGPT: 人工智能大模型应用的千姿百态 [J]. 计算机仿真, 2023, 40 (7): 1-7.
- 3 缪青海, 王兴霞, 杨静, 等. 从基础智能到通用智能: 基于大模型的 GenAI 和 AGI 之现状与展望 [J]. 自动化学报, 2024, 50 (4): 674-687.
- 4 卢经纬, 郭超, 戴星原, 等. 问答 ChatGPT 之后: 超大预训练模型的机遇和挑战 [J]. 自动化学报, 2023, 49 (4): 705-717.
- 5 BAI J Z, BAI S, CHU Y F, et al. Qwen technical report [J]. arXiv preprint arXiv: 2309.16609, 2023.
- 6 王飞跃. 数字教师与平行教育: 关于 ChatGPT 之后教学变革的探讨 [J]. 智能科学与技术学报, 2023, 5 (4): 454-463.
- 7 数据+算力+算法, 人工智能的三大基石 [EB/OL]. <https://cloud.tencent.com/developer/article/2396016>.
- 8 XI Z, XIN G, WEI H, et al. The Rise and Potential of Large Language Model Based Agents: A Survey [J]. arXiv, 2023.
- 9 KAI M, XU S, YE R, et al. AIOS: LLM Agent Operating System [J]. arXiv preprint arXiv: 2403.16971, 2024.
- 10 ZHANG J P, PU J, X J R, et al. HiVeGPT: Human-machine-augmented intelligent vehicles with generative pre-trained transformer [J]. IEEE Transactions on Intelligent Vehicles, 2023, 8 (3): 2027-2033.
- 11 MIAO Q H, ZHENG W B, LV Y S, et al. DAO

- to HANOI via DeSci: AI paradigm shifts from AlphaGo to ChatGPT [J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10 (4): 877–897.
- 12 田永林,王雨桐,王建功,等. 视觉 Transformer 研究的关键问题: 现状及展望 [J]. 自动化学报, 2022, 48 (4): 957–979.
- 13 ANDREW N G. Agentic Workflow [EB/OL]. <https://www.deeplearning.ai/the-batch/issue-242/>.
- 14 XUE X, YU X N, WANG F Y. ChatGPT chats on computational experiments: From interactive intelligence to imaginative intelligence for design of artificial societies and optimization of foundational models [J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10 (6): 1357–1360.
- 15 WANG F Y, LI J J, QIN R, et al. ChatGPT for computational social systems: From conversational applications to human-oriented operating systems [J]. IEEE Transactions on Computational Social Systems, 2023, 10 (2): 414–425.

基于综合智能推理链方法（IIRC）的芯片技术文档解析与模型生成

许一品¹ 陈泓材¹

摘要 为了从输入的芯片技术文档中提取参数并生成该芯片的 PSPICE 模型代码，提出了一种结合检索增强生成（Retrieval-Augmented Generation, RAG）和思维链（Chain of Thought, CoT）的方法。首先通过 OCR 获取技术文档内容。其次利用 RAG 的检索和生成能力对 OCR 后的文本进行分类和信息检索，结合思维链方法进行逐步推理和任务分解。最后通过大语言模型，生成对应芯片的 PSPICE 代码。实验结果表明，该方法能够高效、准确地从复杂文档中提取并生成所需代码，为电子设计自动化提供了新的解决方案。

关键词 检索增强生成，思维链，芯片技术文档，PSPICE 模型代码，信息检索，大语言模型，电子设计自动化

Chip Technical Document Parsing and Model Generation Based on Integrated Intelligent Reasoning Chain Method (IIRC)

XU Yi-Pin¹ CHEN Hong-Cai¹

Abstract To extract parameters from input chip technical documents and generate PSPICE model code, a method combining Retrieval-Augmented Generation (RAG) and Chain of Thought (CoT) is proposed. First, OCR is used to obtain the content of the technical documents. Then, the RAG's retrieval and generation capabilities are used to classify and retrieve information from the OCR text, combined with CoT for step-by-step reasoning and task decomposition. Finally, a large language model generates the corresponding chip's PSPICE code. Experimental results show that this method can efficiently extract and generate the required code from complex documents, providing a new solution for electronic design automation.

Key words Retrieval-Augmented Generation, Chain of Thought, chip technical documents, PSPICE model code, information retrieval, large language model, electronic design automation

0 引言

现代芯片的技术文档包含大量详细的

技术规格、参数和应用信息，内容复杂且冗长^[1]。这种复杂性给人工读取和解析带来了巨大挑战。工程师必须花费大量时间和精力来解读这些文档，且解析过程中容

1. 东南大学自动化学院

1. School of Automation, Southeast University

易出现人为错误, 从而影响设计和测试的准确性^[2-3]。这种局面急需一种高效、精准的自动化方法来替代传统的人工解析。此外, 在芯片和电路设计中, 电路模型的构建至关重要。因此, 能够从复杂的文档中自动提取必要信息并直接生成电路模型的方法, 将大大提升设计效率和准确性。

1 问题的提出

1.1 人工智能技术的发展

近年来, 人工智能技术, 尤其是大语言模型 (Large Language Model, LLM) 的迅猛发展, 为解决这一问题提供了新的途径^[4-8]。在人工智能的浪潮中, 检索增强生成 (Retrieval - Augmented Generation, RAG) 技术以其独特的优势成为研究和应用的热点^[9]。RAG 技术通过结合大型语言模型的强大生成能力和高效的信息检索系统, 为用户提供了一种全新的交互体验, 能够在处理复杂文档时提供更为准确和详细的答案^[10]。RAG 系统不仅可以快速检索海量数据中的关键信息, 还能够生成连贯且具有上下文理解的文本内容, 使其在多个应用领域展现出强大的潜力^[11]。

然而, 随着技术的深入应用, 一系列挑战也逐渐浮现。现有的 RAG 系统在处理海量数据时面临着效率和准确性的双重压力。尽管 LLMs 能够生成流畅的文本, 但在面对复杂、非结构化的数据时, 它们往往难以准确把握和召回关键信息^[11]。此外, RAG 系统在数据管理和理解方面也存在局限, 这导致了所谓的“垃圾输入, 垃圾输出” (Garbage In, Garbage Out, GIGO) 问题, 即如果输入数据质量不高, 那么生成的答案也很难达到预期的准确性。尤其是针对复杂的芯片技术文档, 现

有的 RAG 技术在参数的准确定位查找和生成特定格式的输出方面, 仍面临显著挑战。复杂的技术文档需要精确的解析和数据提取能力, 而传统 RAG 方法在处理这些任务时表现有限, 迫切需要更为先进的方法来解析精度和生成效果^[12]。

1.2 思维链提示方法的应用

为了进一步提升文档解析的效果, 研究者们提出了多种思维链提示方法来提升 LLM 的推理能力和准确性, 包括 Zero - shot CoT、Manual CoT 和 Few - shot CoT 等^[13-14]。这些方法通过预设的推理步骤, 帮助模型更好地理解 and 处理复杂问题。然而, 这些方法在直接应用于芯片技术文档解析时, 仍存在一定的局限性^[15]。

Kojima 等在 2022 年的研究中表明, LLMs 已经具有相当好的零样本推理能力, 其生成的推理过程已经反映了思维链推理。所以他提出了 Zero - shot CoT, 这一方法不需要训练数据集, 通过提示模型生成合理的推理过程来解答问题。Zero - shot CoT 的优势在于其灵活性和广泛适用性, 然而它依赖于模型的自主推理能力, 面对高度复杂和专业化的技术文档时, 模型可能无法生成准确的推理过程。这种方法在处理芯片技术文档中涉及的复杂技术参数时表现欠佳, 因为这些文档需要高度专业化的知识背景和细致的推理步骤^[16-17]。

Manual CoT 通过手动设计推理过程来引导模型的推理能力, 表现出了更强的性能。研究者们通过精心设计的问题和推理链示范来帮助模型进行推理。然而, 手动设计推理步骤需要大量的人力和时间成本, 并且难以应对不同类型文档的多样性。在芯片技术文档解析中, 不同文档的格式和内容差异很大, 手动设计推理步骤难以覆盖所有可能的情况。此外, 手动设

计的推理链也难以适应动态变化的技术需求^[18]。

Few-shot CoT 通过提供少量示例来提示模型生成合理的推理过程。虽然这种方法在某些领域效果不错，但在处理特定领域内的复杂解析需求时仍面临挑战。其效果依赖于示例的质量和覆盖范围，在芯片技术文档解析中，不同文档的复杂性和专业性要求使得提供足够且高质量的示例变得困难。此外，Few-shot CoT 方法仍然需要一定量的训练数据，而芯片技术文档解析中可能无法获得足够的高质量训练数据^[19-20]。

1.3 研究目的和研究内容

综上所述，传统的 RAG 方法和思维链提示方法在芯片技术文档解析方面都存在一定的局限性，主要体现在参数的准确定位查找和生成特定格式的输出方面、模型自主推理能力的不足、手动设计的高成本和示例指导的局限性。为了更好地解析芯片技术文档，可能需要结合领域专家知识和自动化技术，以实现更准确和高效的解析效果。

为了解决上述问题，本文提出了一种结合 RAG 和思维链方法的综合智能推理链方法，即 IIRC。综合智能推理链方法采用的 RAG 技术结合了大型语言模型的生成能力和高效的信息检索系统，能够快速从大量文档中提取关键信息并生成连贯的文本内容，并且 IIRC 结合了 Zero-shot CoT、Manual CoT 和 Few-shot CoT 等多种推理链方式，充分利用其各自的优势，通过简单的指推断、指引和少量的示例，实现了高效、准确的芯片分类和参数查找。该方法通过动态调整推理链，根据具体问题的复杂性灵活应对，确保输出结果的高质量 and 可解释性。实验结果表明，IIRC 方法在芯片技术文档解析与 PSPICE 模型生成中具

有显著优势，为解决复杂文档解析问题提供了新的思路。

2 综合智能推理链方法

综合智能推理链方法通过采用 RAG 框架，结合 Zero-shot CoT、Manual CoT、Few-shot CoT 三种思维链提示方式，显著提升了文档解析的灵活性、准确性和适应性，适用于芯片技术文档参数解析和模型生成。该方法通过 RAG 实现对输入芯片技术文档的高效信息检索和增强文本生成。Zero-shot CoT 赋予模型在无示例情况下自主生成推理步骤的能力，增强了其在未知领域的适用性；Manual CoT 利用专家预先设计的逻辑步骤，确保了模型在处理特定任务时的精确性和一致性；Few-shot CoT 通过少量示例引导模型理解任务要求，进一步提升了模型在复杂场景下的表现。通过整合这三种 CoT 方法，IIRC 能够有效提升 LLM 的理解能力，应对芯片技术文档的复杂解析任务，实现高质量的数据提取和 PSPICE 模型生成。图 1 为芯片技术文档解析与模型生成的流程图，下面详细介绍 IIRC 方法的具体步骤及其在芯片分类与模型生成中的应用。

如算法 1 所示，首先，用户输入一个芯片型号（由数字和字母组成），如 2N2222 等。输入芯片型号是整个流程的起点，系统将根据输入的芯片型号从知识库中提取相关信息，并进行后续的分类和参数查找工作。其次，系统从知识库中提取与该芯片型号相关的描述文字。这些描述文字通常包含关于芯片类型、特性、参数和应用的信息，是后续分类和参数查找的重要依据。知识库中的数据通常来自用户上传的技术文档，通过预处理和索引构建，使得检索过程能够高效且准确。在这



图1 综合智能推理链方法流程图

个过程中，RAG 框架发挥了关键作用，它结合了检索和生成两种能力，从海量文档中快速提取并生成与芯片相关的高质量文本。这一过程不仅提高了信息提取的速度和准确性，还为后续步骤提供了可靠的基础数据。为了准确识别芯片类型，系统依次检测描述文字中的特定关键词。如图2所示，Zero-shot CoT 在无示例情况下自主生成推理步骤，通过关键词匹配和推理链条构建来识别芯片类型，增强了模型在未知领域的适用性和推理能力。如果未检测到上述任何关键

字，系统输出“该芯片暂不在研究范围”，并退出整个流程。在检测到芯片类型后，系统在知识库中搜索相应的参数。Manual CoT 则利用专家预先设计的逻辑步骤，通过手工设定的推理链条，确保模型在处理特定任务时的精确性和一致性，特别是在参数查找过程中，通过预定义的规则和步骤保障查找的准确性和可靠性。系统根据判定的芯片类型，在知识库中搜索指定的该类型芯片参数。如果找到该参数，系统输出参数值；如果未找到，则输出“未查询到该参数”。



图2 Zero-shot CoT、Manual CoT、Few-shot CoT 机制示意图

算法 1 综合智能推理链算法

算法 1 IIRC	
需要:	若干技术文档 D 以及不同类型芯片预定义好的参数 P
确保:	提取并排序的参数 $p=[p_1, p_2, \dots, p_n]$ 适用于其对应的参数类别
1:	过程 IIRC (D, P)
2:	对于每个在文档集合 (D) 中的文档 (d) 执行
3:	使用 OCR 从文档 (d) 中提取文本段落
4:	使用关键词检测 (用户预定义的) 将文本段落分类
5:	对于 每一个类别 (c) 执行
6:	如果 (c) 是用户定义的元件类型 然后执行
7:	在 (d) 中搜索用户预先定义的特定参数
8:	提取参考值 (p)
9:	按照文档结构的相关性对参数 (p) 进行排序
10:	结束如果
11:	结束对于
12:	结束对于
13:	使用提取和排序的参数生成 PSPICE 模型代码
14:	返回 PSPICE 模型代码
15:	结束程序

最后，根据查找到的参数，系统将这些参数替换到预定义的输出模板中，生成相应的 PSPICE 模型代码。如图 2 所示，Few-shot CoT 通过提供少量示例引导模型理解任务要求，在生成 PSPICE 模型代码时，通过示例学习，使得生成的代码格式正确、内容完整。通过这种方式，系统能够生成高质量的模型代码，以满足工程设计和测试的需求。此外，IIRC 方法具有动态调整和自我调整的能力，以应对不同问题的复杂性。在解析过程中，模型根据输入文档的内容和结构，灵活调整推理链的长度和详细程度。这种动态调整机制使得系统能够更好地适应各种复杂文档的解析需求，提高解析的准确性和效率。通过结合 RAG 框架和 Zero-shot CoT、Manual CoT、Few-shot CoT，IIRC 方法能够有效处

理复杂的芯片技术文档，生成高质量的 PSPICE 模型代码，显著提升了文档解析的自动化水平和准确性。

3 实验和结果

在本次实验中，对 300 个芯片技术文档进行了模型生成实验，样本包括 100 个双极型晶体管 (Bipolar Junction Transistor, BJT)、100 个场效应管 (Field-Effect Transistor, FET) 和 100 个二极管 (Diode)。对每个样本进行了人工标注，生成标准的 PSPICE 模型代码，作为对比基准。在该实验中的部分思维链如图 3 所示。对于 IIRC、Zero-shot CoT、Manual CoT 和 Few-shot CoT 在准确性、召回率和处理时间等方面的表现如表 1 所示。

表 1 不同思维链方法的实验结果比较

方法	平均准确率 (%)	平均召回率 (%)	平均精确率 (%)	平均 F1 分数 (%)	平均处理时间 (s)
IIRC	92.5	93.2	91.7	92.4	12.5
Zero-shot	75.3	76.8	74	75.4	10.8
Manual	84.1	85	83.2	84.1	14.2
Few-shot	89	90.2	88.7	89.4	13

从实验结果来看，IIRC 方法在准确性、召回率、精确率和 F1 分数上均取得最佳结果，显著优于其他三种方法。在可解释性评估中，通过专家评审和用户反馈，IIRC 方法得到了较高的评价，图 4 为 IIRC 提取 PSPICE 代码的 LLM 对话示例，其推理链清晰明了，能够解释每一步推理过程的逻辑依据，图 5 为其生成的部分 PSPICE 模型代码。相较之下，Zero-shot CoT 的推理过程较难理解，Manual CoT 虽然逻辑明确但灵活性不足，Few-shot CoT 在提供示例后能够较好地进行推理。



图3 实验中的部分思维链

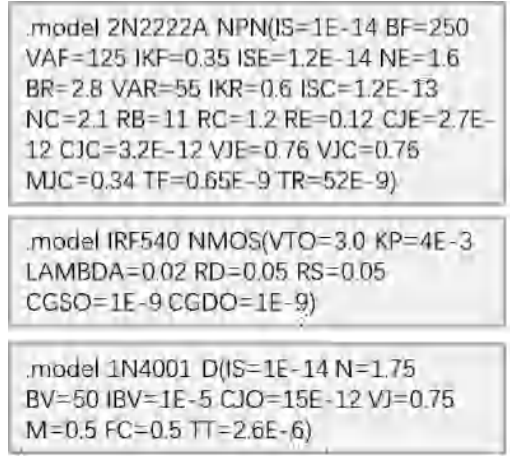


图5 IIRC 生成的部分 PSpice 模型代码

在处理标准格式文档时表现较好，但在不完整文档中表现欠佳，Few-shot CoT 在提供示例的情况下能够较好地适应不同文档格式。

因此，以上实验结果表明，综合智能推理链方法能够有效提升芯片技术文档解析和 PSpice 模型生成的自动化水平和准确性，为实际应用提供了可靠的解决方案。

4 结束语

随着科技的快速发展，现代电子器件的复杂度显著增加，芯片技术文档中的信息量和复杂性也随之提升，给人工解析带来了巨大的挑战。本文提出了一种基于综合智能推理链方法的解决方案，采用 RAG 架构，通过结合 Zero-shot CoT、Manual CoT 和 Few-shot CoT 三种思维链提示方式，实现了芯片参数提取和 PSpice 模型生成的自动化。

在本研究中，首先介绍了 IIRC 方法的基本概念和流程，详细阐述了其在芯片分类、参数查找和模型生成中的具体应用。接着，通过对 300 个芯片技术文档的实验，



图4 IIRC 提取 PSpice 代码的 LLM 对话示例图

IIRC 方法在面对不同类型和复杂度的文档时表现出较高的稳定性和一致性，能够处理各种格式的技术文档，包括噪声数据和不完整文档。Zero-shot CoT 在面对复杂文档时性能下降较为明显，Manual CoT

分别采用 IIRC、Zero-shot CoT、Manual CoT 和 Few-shot CoT 方法，进行了比较和评估。结果表明，IIRC 方法在准确性方面对比传统算法表现优异。同时，IIRC 方法在效率、可解释性和鲁棒性方面也展示了其独特的优势。

具体而言，IIRC 方法在准确性上达到了 92.5%，在召回率和精确率上分别达到了 93.2% 和 91.7%，其 F1 分数高达 92.4%。这些结果证明了 IIRC 方法在处理复杂芯片技术文档解析任务中的高效性和可靠性。此外，通过专家评审和用户反馈，IIRC 方法在可解释性和鲁棒性方面也得到了高度评价，表现出色。

本文的研究不仅展示了 IIRC 方法在实际应用中的潜力，还为未来的芯片文档解析和模型生成研究提供了新的思路和方法。综合智能推理链方法通过灵活应用不同类型的思维链提示，有效提升了文档解析的自动化水平和准确性，具有广泛的应用前景。

未来的研究可以进一步探索 IIRC 方法在其他类型技术文档中的应用，并优化其算法和流程，以应对更复杂的任务和数据集。同时，随着人工智能技术的不断进步，进一步提升系统的可解释性和鲁棒性，将有助于增强用户对自动化解析系统的信任和依赖。

总之，IIRC 方法在提升芯片技术文档解析和 PSPICE 模型生成效率和准确性方面，展示了其卓越的性能和广泛的应用潜力，为复杂技术文档的自动化解析提供了一个有效的解决方案。

参考文献

- 1 KUPIANSKYI H, HORSLEY S A R, PHILLIPS D B. High-dimensional spatial mode sorting and optical circuit design using multi-plane light conversion [J]. *APL Photonics*, 2023, 8 (2).
- 2 TORUN H M, SWAMINATHAN M. High-dimensional global optimization method for high-frequency electronic design [J]. *IEEE Transactions on Microwave Theory and Techniques*, 2019, 67 (6): 2128-2142. DOI: 10.1109/TMTT.2019.2915298.
- 3 KAFLE K, PRICE B, COHEN S, et al. Dvqa: Understanding data visualizations via question answering [C] // *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2018: 5648-5656.
- 4 BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners [C] // *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020. NeurIPS 2020*, 2020.
- 5 TOUVRON H, MARTIN L, STONE K, et al. Llama 2: Open Foundation and Fine-Tuned Chat Models [J]. *arXiv preprint arXiv: 2307.09288*, 2013.
- 6 LE SAO T, FAN A, AKIKI C, et al. Bloom: A 176b-parameter open-access multilingual language model [J]. *ArXiv preprint*, 2022.
- 7 CHOWDHERY A, NARANG S, DEVLIN J, et al. Palm: Scaling language modeling with pathways [J]. *ArXiv preprint*, 2022.
- 8 SCHAEFFER R, MIRANDA B, KOYEJO S. Are Emergent Abilities of Large Language Models a Mirage? [J]. *Advances in Neural Information Processing System*, 2024.
- 9 LYU Y, NIU S, XIONG F, et al. CRUD-RAG: A Comprehensive Chinese Benchmark for Retrieval-Augmented Generation of Large Language Models [J]. *arXiv preprint arXiv: 2401.17043*, 2024.
- 10 ROUZROKH P, FAGHANI S, GAMBLE C, et al. CONFLARE: CONFORMAL LARGE LANGUAGE MODEL RETRIEVAL [J]. *arXiv preprint arXiv: 2404.04287*, 2024.
- 11 WU Y, ZHU J, XU S, et al. RAGTruth: A Hallucination Corpus for Developing Trustworthy Retrieval-Augmented Language Models [J]. *arXiv preprint arXiv: 2401.00396*, 2003.

- 12 WANG Y, REN R, LI J, et al. REAR: A Relevance-Aware Retrieval-Augmented Framework for Open-Domain Question Answering [J]. arXiv preprint arXiv: 2402.17497, 2024.
- 13 WANG X, WEI J, SCHUURMANS D, et al. Self-consistency improves chain of thought reasoning in language models [C] //The Eleventh International Conference on Learning Representations. 2023.
- 14 WEI J, BOSMA M, ZHAO V Y, et al. Finetuned language models are zero-shot learners [C] // The Tenth International Conference on Learning Representations, ICLR 2022, Virtual Event. 2022.
- 15 ZHOU D, SCHÄRLI N, HOU L, et al. Least-to-most prompting enables complex reasoning in large language models [C] //The Eleventh International Conference on Learning Representations. 2023.
- 16 KOJIMA T, GU S, REID M, et al. Large language models are zero-shot reasoners [J]. Advances in Neural Information Processing Systems, 2023, 35: 22199–22213.
- 17 KOJIMA T, SHIXIANG S, GU G, et al. Large Language Models are Zero-Shot Reasoners [J]. Advances in neural information processing systems, 2022, 35: 22199–22213.
- 18 WAN X, SUN R, DAI H, et al. Better zero-shot reasoning with self-adaptive prompting [C] // Findings of the Association for Computational Linguistics. ACL 2023, Toronto, Canada: 3493–3514.
- 19 CRESWELL A, SHANAHAN M, HIGGINS I. Selection – inference: Exploiting large language models for interpretable logical reasoning [C] // The Eleventh International Conference on Learning Representations. 2023.
- 20 YORAN O, WOLFSON T, BOGIN B, et al. Answering questions by meta-reasoning over multiple chains of thought [J]. ArXiv preprint, 2023.

空战博弈场景下态势事件图谱构建及决策应用

郎彬¹ 雷达¹ 陈久红¹ 马瑞祥¹ 胡天祥¹

摘要 针对具体的空战博弈任务智能化的战术决策需求,通过大样本仿真技术构建态势-事件图谱,形成完整的作战知识库,将决策问题等效为态势-事件图谱中的路径查找问题,实现空战过程中基于当前态势实时输出任务决策方案。同时针对复杂不确定战场环境下基于当前空战态势预判最终胜利的可能性的实际需要,结合离散马尔可夫链模型,在机载环境下实时评估当前态势并预测最终胜率,为进一步提高飞行员任务认知与执行效率提供技术支撑。

关键词 态势事件图谱,图谱构建,态势分析,辅助决策

Construction and Decision Application of Situational Event Graph in Air Combat Game Scenario

LANG-Bin¹ LEI-Da¹ CHEN Jiu-Hong¹ MA Rui-Xiang¹ HU Tian-Xiang¹

Abstract In response to the intelligent tactical decision-making requirements of specific air combat game tasks, a Situational-Event Graph is constructed through large-sample simulation technology, forming a comprehensive combat knowledge base. The decision problem is equivalently transformed into a path-finding problem in the Situational-Event Graph, enabling real-time output of mission decision schemes based on the current combat situation during air combat. Moreover, to meet the practical need for predicting the likelihood of ultimate victory based on the current air combat situation in complex and uncertain battlefield environments, a discrete Markov chain model is integrated to enable real-time assessment of the current situation and prediction of the final win rate onboard. This provides technical support to enhance pilots' situational awareness and operational efficiency.

Key words situational event graph, construction of knowledge graph, situational analysis, decision support

0 引言

未来战争中,战场认知与决策速度将成为战争胜负的决定因素,谁能够更快地处理战场信息、理解态势、实施决策并执行打击,谁就能赢得主动^[1]。该特性在空

战博弈场景中尤为突出,面对空中来袭目标,飞行员急需在短时间内正确预判其来袭意图,并采取相应的攻击、防御或撤退措施。当前对空中来袭目标的意图判断,主要由飞行员根据数据融合提供的综合态势信息进行人为判断。在此过程中,飞行员要在时间紧急、信息复杂、高度不确定

1. 中国电子科技集团公司第五十二研究所

1. The 52nd Research Institute of China Electronics Technology Group Corporation

情况下,基于对作战环境的感知,建立对空战态势的理解,判断空战态势的发展趋势,选择目标攻击分配和排序方案,确定本机、编队协同的空战决策,并在执行决策的过程中根据实战态势变化适时调整。这一系列任务为飞行员带来了巨大的负担。

1 总体思路

知识图谱以结构化的形式描述客观世界中概念、实体及其关系,将信息表达成更接近人类认知世界的形式,提供了一种更好地组织、管理和理解海量信息的能力。事件图谱以事件为基础信息的新型结构化知识表示方式,图谱中的节点表示事件提及,节点之间的边表示事件提及之间的时间关系和指代关系。事理图谱是描述事件之间演化规律和模式的事理逻辑知识库,图谱中事件关系大多是不确定的,以一定的概率进行转移,更适合一些后续意图的识别或辅助性推理。借助知识图谱进行态势评估和辅助决策是一种可行的办法。态势评估是指对特定的时空环境中的要素感知,并基于要素理解预测态势在未来一段时间内的发展趋势^[2]。空战态势评估的方法主要有参量法和非参量法,参量法主要基于目标的特征概率分布,以我方平均概率风险最小或完成任务可能性最大等决策准则为指标,完成运算^[3];非参量法主要根据交战的态势信息进行定量判断。通常选取体现空战态势特征、对空战结果起决定作用的、便于定量分析的信息作为评估内容,如位置、速度、武器性能、雷达性能等。

基于知识图谱的辅助决策主要是利用知识图谱技术,将海量的战场信息和数据利用起来,辅助情报分析人员、作战指挥员进行战场态势的理解,为指挥决策提供更加准

确、高效、可靠的信息依据^[4]。韩晓^[5]通过在知识图谱中加入具有逻辑计算能力的认知节点,结合知识图谱强大的表示推理能力,设置触发条件激活认知节点,动态地应对图谱中的变化,并将影响通过认知类链条进行扩散,最终达到辅助决策的目的。薛冬梅^[6]利用深度学习技术对舰船指挥方面的多源异构数据进行态势要素抽取,利用知识推理技术对舰船指挥决策知识图谱扩展出更多有价值的舰船信息,辅助指挥决策。樊皓^[7]利用多粒度模糊贝叶斯网络对空中目标的战术意图进行估计,提高实际辅助决策过程中的可参考性。田鹏等^[8]研究建立了作战指挥规则图谱的图数据模型,设计实现了相应的辅助决策路径搜索生成算法,支撑基于规则的作战指挥。

本文针对具体的空战博弈任务,分析其战术决策需求,通过大样本仿真技术构建态势-事件图谱,形成完整的作战知识库,将决策问题等效为态势-事件图谱中的路径查找问题,实现空战过程中基于当前态势实时输出任务决策方案。同时针对复杂不确定战场环境下基于当前空战态势预判最终胜利的可能性的实际需要,结合离散马尔可夫链模型,在机载环境下实时评估当前态势并预测最终胜率,为进一步提高飞行员任务认知与执行效率提供技术支撑。总体设计思路如图1所示。

具体地,先利用空战仿真系统的仿真数据构造并不断完善态势-事件图谱,将构造完毕的态势-事件图谱应用于空战仿真系统,然后根据输入的态势信息来做行为决策。本文重点研究面向空战博弈场景下的事件抽取技术、战场态势聚合技术、转移概率计算技术,以得到具有代表性的态势节点和事件组合节点,构造态势-事件知识图谱,实现典型1v1空战场景下基于知识图谱的辅助决策生成。

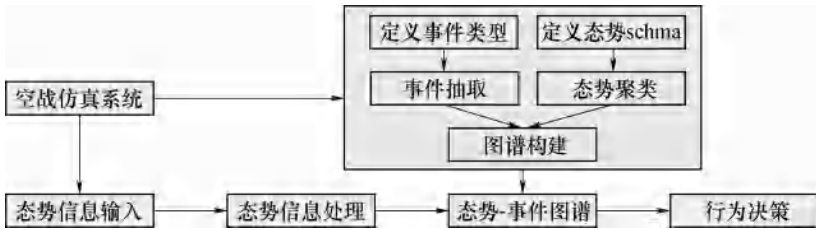


图1 基于态势-事件图谱辅助决策逻辑图

2 空战博弈场景下的态势-事件图谱构建

根据空战博弈下实际应用场景的特点,结合事件图谱和事理图谱的优点,本文拟构建一个空战博弈场景下的态势-事件图谱。该图谱是一个有向有环图,其中节点表示已聚合的态势,有向边表示引起态势改变的事件组合,两个态势节点间可由不同的事件组合进行连接,边上的转移概率表示当前态势下,可能触发的事件组合的概率。基于构建的态势-事件图谱,将决策问题等效为态势-事件图谱中的路径查找问题。此处的路径被定义为从当前态势节点到最终态势节点(红方或蓝方飞机被击落)的所有可能的路径。通过各态势节点之间的转移概率计算各路径出现的概率,指导当前时刻、当前态势下飞机需要执行的动作。

2.1 态势数据集构建

利用空战仿真平台进行1v1空战仿真模拟,红蓝双方的预配置参数如表1所示。

红蓝双方使用的智能体包括基于专家规则的智能体和基于强化学习的智能体,Random表示当前仿真场次下红蓝双方随机选择不同的智能体类型。包括利用强化学习算法PPO训练得到的智能体和基于交叉进攻策略、单边进攻策略、防守策略

等得到的智能体。

每场仿真生成的仿真数据包括每一个仿真步骤下所有态势信息,站在红方视角得到的红方飞机在时刻1的部分态势信息如表2所示。

表1 红蓝双方仿真前预配置参数

	红方	蓝方
飞机类型	J11B	SU-30MKI
挂载导弹类型	PL-15	AA-10
挂载导弹数量	6	6
初始位置	(0, 0, 12000)	(100000, 20000, 12000)
初始速度	278	278
智能体类型	Random	Random

2.2 态势聚合算法

在空战博弈过程中,飞机之间的相对特征尤为重要,它为飞行员提供最有价值的决策信息。在实际特征抽取过程中,要着重筛选相对特征。针对1v1场景,站在红方视角对红方飞机态势和蓝方飞机态势选择不同的属性,选取的飞机态势如表3所示。

2.3 事件抽取算法

在空战博弈过程中,飞机的每一个动作可看作当前时刻下发生的事件,故此处的抽取算法是根据紧邻2个时刻之间的态势变化确定飞机的动作,在利用态势-事件图谱进行辅助决策时,飞行员需要

表 2 红方视角下红方飞机 0 在时刻 1 的部分态势

字典	属性示例	飞机属性信息
idx	0	飞机 id
identification	J11B	飞机名称
type	fighter	飞机类别 (战斗机/预警机)
generation	3	飞机划代 (3 代机或 4 代机)
name	plane_0	名称
min_speed	180	最小速度
max_speed	544	最大速度
overload	24.34423108554597	当前过载
current_x	0	当前 x 坐标
current_y	0	当前 y 坐标
current_z	12000	当前 z 坐标
current_speed	278	当前速度
current_angle_hxj	2.48	当前航向角
current_angle_fyj	0	当前俯仰角
current_angle_qxj	0	当前滚转角
current_status	1	飞机当前状态
rcs	2.5	飞机截面积
current_fuel	9418	当前油量
disruptor_ammo	{ name: , current_number: , disruptor_ammo: , }	干扰弹相关信息
missile	{ name: , nums: , un_launch_nums: , missile: } }	导弹相关信息
ray_radar	{ rayRadarNum: , target_visible_status: , switch_status: , ... }	光雷相关信息
detect_radar	{ search_times: , detect_angle: , direction_noise: , ... }	探测雷达相关信息
jamming_pod	{ status: , transmitter_power: , transmitter_gain: , expected_jamming_power: . }	干扰吊舱相关信息

表 3 1v1 场景下选取的飞机态势

飞机阵营	态势变量名称	说明
Red	state_radar	飞机雷达状态, 开启: True, 关闭: False
	state_detect_plane	是否检测到敌机, 是: True, 否: False

续表

飞机阵营	态势变量名称	说 明
Red	state_lock_plane	是否锁定敌机，是：True，否：False
	state_beLocked	是否被敌机锁定，是：True，否：False
	state_ifHaveMissile	是否有可发射的导弹，是：True，否：False
	state_ifWorkingMissile	是否有已发射正在飞行的导弹，是：True，否：False
	state_ifHaveDisruptorAmmo	是否有未发射的干扰弹，是：True，否：False
	state_ifWorkingDisruptorAmmo	是否有干扰弹处于发射状态，是：True，否：False
	state_jamming_pod	干扰器状态，开启：True，关闭：False
	state_beTracked	是否正在被敌方导弹攻击，是：True，否：False
	state_beClose	是否距离敌方导弹很近，是：True，否：False
	state_relative_hxj	本机与敌机的相对航向角，按统计值划分为6个区间，分别用0~5来表示
	state_relative_distance	本机与敌机的相对距离，按统计值划分为6个区间，分别用0~5来表示
	state_relative_speed	本机与敌机的相对速度，按统计值划分为5个区间，分别用0~4来表示
	state_relative_height	本机与敌机的相对高度，按统计值划分为6个区间，分别用0~5表示
	state_live	飞机存活状态，1：生存，0：死亡
Blue	state_radar	飞机雷达状态，开启：True，关闭：False
	state_beClose	是否距离敌方导弹很近，是：True，否：False
	state_live	飞机存活状态，1：生存，0：死亡

执行的动作是两个态势节点之间的边所代表的事件组合。针对 1v1 场景，选取的飞机动作如表 4 所示：主要包括开启/关闭雷达、发射导弹、开启/关闭干扰器、发射干扰弹、飞机机动动作（左切/右切/拉升/降低/追击）等。

2.4 转移概率计算

在不同的智能体仿真得到的 1v1 空战数据的基础上，先统计所有不同的态势和事件，再统计各不同态势-事件-态势三元

组的数量，然后就可以对转移概率进行计算。

首先，统计所有不同的态势和事件，生成 id2event 和 id2state，其中 id2event 表示当前时刻发生的事件，id2state 表示当前时刻红蓝双方的状态，其部分示例及其说明如表 5、表 6 所示。

其次，依据仿真时序生成态势-事件-态势三元组，并统计各不同三元组的数量。部分态势-事件-态势三元组及其个数如表 7 所示。

表 4 1v1 场景下选取的飞机动作

动作变量名称	说 明
event_open_radar	open_radar: 开启雷达, close_radar: 关闭雷达
event_launch_missile	launch_missile: 发射导弹, planeA: 发射导弹飞机, planeB: 导弹攻击目标

续表

动作变量名称	说 明
event_open_jamming_pod	open_jamming_pod: 开启干扰器, close_jamming_pod: 关闭干扰器
event_launch_disruptor	launch_disruptor: 发射干扰弹
event_leftOffsetGuidance	JiDong_leftRight: 左切/右切
event_upDown	JiDong_upDown: 拉升/降高
event_chase	chase: 追击, planeA: 发生追击动作的飞机, planeB: 被追击的飞机
event_beShotDown	beShotDown: 飞机被击落

表 5 state-1 示例及其说明

态势名称	红方/蓝方态势	属性名称	示例	说明
state-0	red2red_state	plane_name	red_J11B	红方飞机名称
		radar_state	true	红方飞机雷达处于开启状态
		detect_plane	true	红方飞机检测到蓝方飞机
		lock_plane	true	红方飞机锁定了蓝方飞机
		beLocked	true	红方飞机被蓝方飞机锁定
		ifHaveMissile	true	红方飞机有可以发射的导弹
		ifWorkingMissile	false	红方飞机没有已发射在飞行中的导弹
		ifHaveDisruptorAmmo	true	红方飞机有可以发射的干扰弹
		ifWorkingDisruptorAmmo	false	红方飞机没有已发射在飞行中的干扰弹
		jamming_pod	false	红方飞机干扰器处于关闭状态
		beTracked	false	红方飞机没有被蓝方攻击
		beClose	false	红方飞机距离蓝方导弹较远
		relative_hxj	3	红方飞机和蓝方飞机的相对航向角
		relative_distance	4	红方飞机和蓝方飞机的相对距离
	relative_speed	0	红方飞机和蓝方飞机的相对速度	
	relative_height	1	红方飞机和蓝方飞机的相对高度	
	live	1	红方飞机处于存活状态	
	red2blue_state	plane_name	Blue-SU-30MKI	蓝方飞机名称
		radar_state	true	蓝方飞机雷达处于开启状态
		beClose	false	蓝方飞机距离红方导弹较远
live		1	蓝方飞机处于存活状态	

表 6 部分事件示例及其说明

事件名称	示 例	说 明
event-0	{ "event_name": "open_radar", "plane": "red_group1-plane_0-J11B" }	红方飞机开启雷达
	{ "event_name": "open_radar", "plane": "blue_group1-plane_1-SU-30MKI" }	蓝方飞机开启雷达
event-1	[]	空事件
event-2	{ "event_name": "chase", "planeA": "red_group1-plane_0-J11B", "planeB": "blue_group1-plane_1" }	红方飞机追击蓝方飞机
event-3	{ "event_name": "launch_missile", "planeA": "red_group1-plane_0-J11B", "planeB": "blue_group1-plane_1-SU-30MKI" }	红方飞机发射导弹攻击蓝方飞机
	{ "event_name": "chase", "planeA": "red_group1-plane_0-J11B", "planeB": "blue_group1-plane_1" }	红方飞机追击蓝方飞机

表 7 部分三元组及其个数

编号	三元组	个数
1	['state-103','event-1','state-104']	num = 4
2	['state-105','event-2','state-106']	num = 13
3	['state-114','event-3','state-116']	num = 10
4	['state-110','event-4','state-112']	num = 4
5	['state-113','event-5','state-112']	num = 22
6	['state-176','event-7','End-state']	num = 2

在上述结果的基础上即可进行转移概率的计算。具体地，统计所有头实体和尾实体相同的三元组，统计其个数和为 m ，当前三元组的个数记为 n ，则当前三元组上边的转移概率为 n/m 。

2.5 态势-事件图谱构建

本文选择 Neo4j 图数据库，利用 Cypher 语句创建节点和关系，以构建态势-事件图谱。

3 面向空战博弈场景的典型策略实现

在空战过程中，有两种典型对战场

景，分别对应进攻和防守任务。针对这两个任务，在上述知识构建的基础上，本文分别为其实现了相应的策略。

3.1 进攻策略

一个典型的攻击场景是红方飞机在自身安全的情况下攻击蓝方飞机。具体地，红方飞机已检测到并锁定蓝方飞机，蓝方飞机的雷达处于关闭状态；红方飞机未受到攻击，具有可发射的导弹，且距离蓝方飞机较近。在此场景下，红方飞机选择发射导弹攻击蓝方飞机，此时执行的动作类为 event-9，其态势-事件-态势三元组为 [state-145, event-9, state-146]，转移概率为 0.62；也可以在发射导弹的同时开展追击动作，此时执行的动作类为 event-3，其态势-事件-态势三元组为 [state-145, event-3, state-146]，转移概率为 0.38，具体的态势变化如表 8 所示。

表 8 典型攻击场景 1: [state-145, event, state-146]

state-145	event	state-146
"plane_name": "red_group1-plane_0-J11B"	event-9 转移概率为 0.62	"plane_name": "red_group1-plane_0-J11B"
"radar_state": true		"radar_state": true
"detect_plane": true		"detect_plane": true
"lock_plane": true		"lock_plane": true
"beLocked": null		"beLocked": false
"ifHaveMissile": true		"ifHaveMissile": true
"ifWorkingMissile": false		"ifWorkingMissile": true
"ifHaveDisruptorAmmo": true		"ifHaveDisruptorAmmo": true
"ifWorkingDisruptorAmmo": false		"ifWorkingDisruptorAmmo": false
"jamming_pod": true		"jamming_pod": true
"beTracked": false	event-3 转移概率为 0.38	"beTracked": false
"beClose": false		"beClose": false
"relative_hxj": 0		"relative_hxj": 0
"relative_distance": 1		"relative_distance": 1
"relative_speed": 4		"relative_speed": 4
"relative_height": 5		"relative_height": 5
"live": 1		"live": 1
"plane_name": "blue_group1-plane_1-SU-30MKI"		"plane_name": "blue_group1-plane_1-SU-30MKI"
"radar_state": false		"radar_state": true
"beClose": false		"beClose": false
"live": 1	"live": 1	

综上所述,在当前态势下,红方飞机一定会发射导弹攻击蓝方飞机,但是只有38%的概率会在发射导弹攻击的同时追击蓝方飞机。采用上述进攻策略最终获胜的概率最高。

3.2 防守策略

1v1空战博弈场景下的防守策略主要是通过开启干扰器、发射干扰弹、机动躲避等方式进行防守,一个典型的防守场景是红方飞机检测到并锁定蓝方飞机,且正在发射导弹攻击蓝方飞机,探测到自身被蓝方飞机锁定且处于被攻击状态,由于还

有可发射的干扰弹,所以在机动躲避的同时执行关闭雷达、开启干扰器、发射干扰弹等动作,期望躲过蓝方导弹的攻击,此时执行的动作类为event-30,其态势-事件-态势三元组为[state-420, event-30, state-421],转移概率为1.0,具体的态势变化如表9所示。

3.3 胜率计算

本文构建的态势-事件图谱满足马尔可夫特性,即一个状态只依赖于它前一个状态,而与过去所有状态无关。离散马尔可夫链主要由三个部分组成:状态集合、

表 9 典型防守场景 1: [state-420, event-30, state-421]

state-420	event	state-421
"plane_name": "red_group1-plane_0-J11B"	event-30 转移概率为 1.0	"plane_name": "red_group1-plane_0-J11B"
"radar_state": true		"radar_state": false
"detect_plane": true		"detect_plane": false
"lock_plane": true		"lock_plane": false
"beLocked": true		"beLocked": true
"ifHaveMissile": true		"ifHaveMissile": true
"ifWorkingMissile": true		"ifWorkingMissile": true
"ifHaveDisruptorAmmo": true		"ifHaveDisruptorAmmo": true
"ifWorkingDisruptorAmmo": false		"ifWorkingDisruptorAmmo": true
"jamming_pod": false		"jamming_pod": true
"beTracked": true		"beTracked": true
"beClose": false		"beClose": false
"relative_hxj": 3		"relative_hxj": 2
"relative_distance": 3		"relative_distance": 3
"relative_speed": 2		"relative_speed": 2
"relative_height": 0		"relative_height": 0
"live": 1		"live": 1
"plane_name": "blue_group1-plane_1-SU-30MKI"		"plane_name": "blue_group1-plane_1-SU-30MKI"
"radar_state": true		"radar_state": true
"beClose": false		"beClose": false
"live": 1	"live": 1	

转移概率矩阵和初始状态分布。态势-事件图谱的构建过程中利用大量的空战仿真数据通过态势聚合算法，得到当前场景下的所有状态集合，用 $S = \{s_1, s_2, \dots, s_n\}$ 表示。转移概率矩阵用 P 表示，它是一个 $n \times n$ 的矩阵， n 表示当前态势-事件图谱的状态节点个数， $P[i][j]$ 表示从状态 S_i 转移到状态 S_j 的概率，该值基于概率转移算法通过统计得到。该场景考虑的初始状态唯一，所以初始状态概率为 1。通过图谱查询找到初始状态节点和结束节点（红方飞机被击落或蓝方飞机被击落）所有路径，计算每条路径的转移概率，取最大值

得到当前状态下红方飞机取胜和失败的概率。

4 结束语

本文针对具体的空战博弈任务，分析其战术决策需求，通过大样本仿真技术构建态势-事件图谱，形成完整的空战博弈作战知识库，将决策问题等效为态势-事件图谱中的路径查找问题，在空战过程中基于当前态势实时输出任务决策方案。同时结合离散马尔可夫链模型，在机载环境下实时评估当前态势并预测最终胜率，为

进一步提高飞行员任务认知与执行效率提供技术支撑。

参考文献

- 1 MCCANN C, PIGEAU R. Clarifying the concepts of control and of command. In Proceedings of the Command and Control Research and Technology Symposium [C] // Washington, DC: US Department of Defense CCRP.
- 2 周思羽, 吴文海, 高丽, 等. 空战态势评估问题综述 [C] // 第13届中国系统仿真技术及其应用学术年会论文集. 2011: 5.
- 3 DAS S, GREY R, GONSALVES P. Situation Assessment via Bayesian Belief Networks [C] // ISIF. 2002: 664-671.
- 4 江志浩, 周卿, 石敏, 等. 作战目标知识图谱构建与应用 [J]. 海军航空工程学院学报, 2020: 35 (6).
- 5 韩晓. 面向筹划决策的动态知识图谱系统设计与实现 [D]. 大连: 大连理工大学, 2022.
- 6 薛冬梅. 面向舰船指挥决策的知识图谱构建方法研究 [D]. 哈尔滨: 哈尔滨工程大学, 2020.
- 7 樊皓. 面向机载态势感知系统的空中目标意图估计 [J]. 兵工自动化, 2022: 41 (4).
- 8 田鹏, 李定主, 陈勇, 等. 基于作战指挥规则图谱的辅助决策方法 [J]. 火力与指挥控制, 2022.

面向气象领域的大语言模型增量 预训练技术研究

雷 达¹ 马瑞祥^{1*} 瞿崇晓¹ 张永晋¹ 余华峰¹

摘要 为增强大语言模型领域专业性，提出军事气象领域增量预训练方法。文章使用低复杂度逻辑回归方法构建低质识别能力、SimHash 构建冗余去除能力，通过采样高质量数据，借助开源模型，使用零冗余优化模式在有限算力下进行增量预训练。实验表明：①通用大模型在气象领域存在专业知识缺乏问题；②增量预训练可以有效提升领域知识水平；③增量预训练后模型对通用知识存在遗忘。未来将持续扩充和优化数据，提升模型领域效果，缓解遗忘现象。

关键词 增量预训练，军事气象，大语言模型，预训练语言模型

Research on Continue Pre-training Techniques for Large Language Models in the Meteorological Domain

LEI Da¹ MA Rui-Xiang^{1*} QU Chong-Xiao¹ ZHANG Yong-Jin¹ YU Hua-Feng¹

Abstract To enhance professionalism in large language models for military meteorology, an incremental pre-training method is proposed. Utilizing low-complexity logistic regression for quality assessment and SimHash for redundancy removal, high-quality data is sampled. Incremental pre-training with zero-redundancy optimization on open-source models under limited computational resources is conducted. Results demonstrate: ①General models lack domain-specific knowledge in meteorology; ②Incremental pre-training effectively boosts domain expertise; ③Post-pre-training, general knowledge retention diminishes. Future efforts aim to expand and refine datasets, enhancing model performance and mitigating knowledge decay.

Key words continue pre-training, military meteorology, large language models, pre-trained language model

0 引言

军事气象是军事活动中一个至关重要的领域，它直接影响着作战计划的制订、

执行以及后勤保障工作。精准的军事气象场景服务能够有效获取、收集战场环境数据，为指挥官提供重要参考，制定更为科学、有效的战术策略。近年来，大语言模型（Large Language Models, LLMs）是人

* 通讯作者

1. 中国电子科技集团公司第五十二研究所

1. The 52nd Research Institute of China Electronics Technology Group Corporation

人工智能领域的一个重要突破, 通过在大规模语料库上进行预训练, 模型能够更精准地理解和生成自然语言文本。由于大语言模型的训练数据主要来源于通用领域, 对垂直领域的专业知识覆盖不够全面, 在领域应用中存在一定局限性。特别是在军事气象战场环境领域, 该领域要求模型具备极高的领域专业性, 能够对高度专业的气象知识和气象特点进行深入理解。

为了解决这一问题, 本文提出气象领域增量预训练 (Continue Pre-Training, CPT) 方法, 借助开源预训练语言模型, 使用战场环境气象领域数据进行增量预训练, 使得开源通用大模型能够获得领域专业知识, 增强其在军事场景领域的专业性, 提高其对复杂战场环境任务的理解能力。

1 问题的定义

军事指挥作业场景需要对战场气象环境相关知识进行处理和理解, 频繁查阅气象相关资料是一个非常需要解决的问题。为此期望引入大语言模型来高效获取气象领域的相关知识, 简化信息整合过程。本文的主要工作是将专业的战场环境气象领域知识注入大语言模型中, 完成军事气象领域大语言基础模型构建。

战场环境气象领域大模型构建, 需要使用大量无监督气象数据, 通过预训练的方式将战场环境相关知识注入模型, 该过程本质上是训练语言模型的问题。

假设输入的自然语言文本为 X , 其长度为 m , 模型需要生成的文本为 Y , 其长度为 n 。训练过程使用文本对 (X, Y) 进行自监督学习, 优化模型参数 θ , 模型的目标是最大化在给定输入 X 的条件下生成 Y 的概率 $P(Y|X; \theta)$ 。即:

$$X = (x_{start}, x_1, \dots, x_m, x_{end}) \quad (1)$$

$$Y = (y_1, y_2, \dots, y_n) \\ = (x_1, \dots, x_m, x_{end}) \quad (2)$$

$$P(Y|X; \theta) \\ = \prod_{i=1}^n P(y_i | y_1, y_2, \dots, y_{i-1}, X; \theta) \quad (3)$$

在预训练语言模型的构建过程中, 去除开始和停止特殊符号, 输入和输出的自然语言文本序列是相同的, 训练任务每次预测下一个词, 因此属于自监督训练。

2 相关工作

近些年, 预训练技术在自然语言处理 (NLP) 领域取得了显著进展, 通过在大规模无监督文本数据上进行训练, 模型能够获得通用性的语言表示, 捕获丰富的语法和语义信息。Transformer 架构的提出进一步推动了预训练模型的发展, 诸如 BERT、GPT 等模型在各种任务中均展现了优越的性能。学者们指出预训练模型的成功并不仅依赖于模型架构, 还与预训练数据的规模和质量密切相关, 先后对预训练模型结构、模型参数规模、预训练数据等方面做了诸多探索。

2020 年, Zhang 等^[1]研究了预训练数据量对基于 Transformer 架构的语言模型的影响, 发现约 1000 万到 1 亿词的预训练数据可以使模型掌握通用的语义和语法, 但要获得足够的常识需要更大规模的知识数据。同年, 文献 [2] 提出了域适应性预训练 (Domain-Adaptive Pretraining) 和任务适应性预训练 (Task-Adaptive Pretraining) 方法, 在四个领域、八个分类任务上展示了自适应预训练带来的效果提升; 文献 [3] 对多领域预训练效率进行研究, 指出权重伸缩加固 (Elastic Weight

Consolidation) 在减少灾难性遗忘方面表现最佳,同时提出了基于梯度和潜在聚类的数据选择技术。2021年,Gu等^[4]构建了生物医学领域预训练语言模型,指出从零预训练生物医学语言模型比继续预训练通用语言模型能带来更大收益。2022年,文献[5]提出为实现Transformer语言模型的最优训练,应将模型规模和训练数据量等比例扩大。Wei等^[6]指出扩大语言模型规模,模型具备小规模参数模型不具备的能力,即扩展参数规模模型将出现新能力。Meta公司^[7]开源了基于Transformers解码结构的预训练语言模型(OPT),指出OPT-175B与GPT-3的性能相当但能源消耗仅为GPT-3的1/7。2023年,Meta公司Touvron等^[8]开源Llama-2模型系列,详细介绍了Llama-2-Chat模型的微调和改进方法,指出该模型优于开源聊天模型,是闭源模型的有力替代品。同年,Valero-Lara等^[9]比较了Llama-2和GPT-3模型在生成高性能计算核方面的表现,指出Llama-2在准确性表现更出色。阿里巴巴千问团队Bai等^[10]介绍了Qwen模型系列,包括预训练语言模型和使用人类反馈强化学习训练的对话模型,展示了基础语言模型在下游任务中卓越的效果。百川智能公司Yang等^[11]开源了Baichuan系列多语言大规模语言模型,该模型在公开测试集上效果优于相似规模的开源模型,在医学和法律等垂直领域表现优异。Zhang等^[12]提出大型语言模型通过链式思维(CoT)推理技术可以显著提升复杂任务推理性能,该技术增强模型可解释性和可控性。

尽管预训练技术已经在诸多自然语言处理任务中取得较好效果,但是开源通用语言大模型在医疗、军事等垂直领域的专业性表现不足;同时,通用预训练模型需要大量算力和数据进行训练,训练成本巨

大。基于此,本文对军事战场环境气象领域预训练大模型进行相关研究,探索在有限算力的条件下构建领域预训练大模型。

3 军事气象领域增量预训练技术

增量预训练技术主要包括数据工程、预训练技术,技术架构图如图1所示。

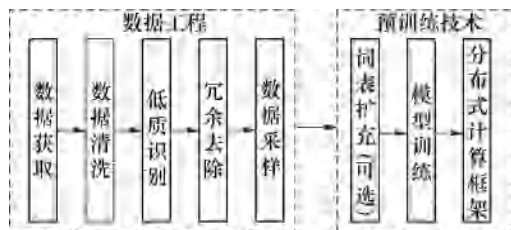


图1 增量预训练技术架构图

接下来将对军事气象领域增量预训练技术进行详述。

3.1 数据工程

3.1.1 数据获取

使用爬虫等工具,获取领域预训练数据集,数据来自业务积累、网页知识。共计获取气象领域、通用领域数据详细情况如表1所示。

表1 原始数据情况

数据	语言	Token 数/B	平均长度
气象数据汇总	中文	0.6	738
通用数据汇总	中文	34	1200

3.1.2 数据清洗

数据清洗是确保数据有效性和可用性的关键步骤,为数据驱动任务提供坚实的基础。通过数据清洗,可以对不同来源的数据进行统一,过滤掉数据格式错误。具体操作如下:

(1) 格式统一:解析来自网页、本地文件等类型数据,统一数据格式,本文使用JSON格式进行存储。

(2) 编码统一：统一不同数据源的编码格式，使用 UTF-8 编码进行存储。

(3) 无效符号去除：处理不同来源数据，去除无效符号，包括无效空格、无效字符、HTML 标签等。

(4) 无效数据去除：删除内容为空的数据和解析结果不完整的数据。

3.1.3 低质识别

低质数据通常指的是内容不准确、不可信、存在错误或欺骗性或者包含恶意意图的文本。这些数据可能包括语法错误、虚假信息、广告垃圾、滥用信息等。识别低质数据的目的是提升数据的可信度，确保文本信息的准确性和可靠性。低质数据识别问题本质上属于自然语言处理(NLP)中的文本分类研究范畴。整体技术架构图如图 2 所示，文本表示和文本分类器是低质数据识别中的核心单元。

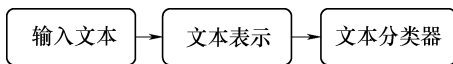


图 2 文本分类技术架构图

目前工业界主流的文本分类方法基于预训练语言模型——如双向编码预训练模型(BERT)——进行分类。由于在数据源获取阶段已经就内容质量做了严格控制，同时考虑后续扩展数据，数据量会较为庞大(如若待处理数据规模在百万级、模型响应速度 50ms/per 的情况下，低质识别需要处理 14h)，从整体性能角度出发，选择时间复杂度低的方法构建低质量数据识别技术能力。

本文选择词频特征进行文本表示，使用逻辑回归方法(Logistic Regression, LR)构建文本分类器，整体方案如图 3 所示。

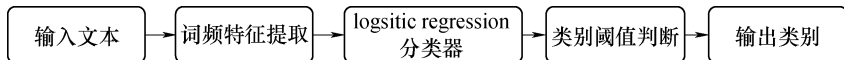


图 3 低质识别技术架构图

(1) 输入与词频特征提取：统计各个单词在一篇文档中出现的次数，通过词频和词序列对文本进行向量表示。

(2) 逻辑回归分类器：使用 sigmoid 函数转换线性回归的输出，输出离散类别下的概率值。LR 模型和其他分类模型相比，大大减少了时间复杂度。

(3) 类别阈值判断与类别输出：通常情况下输出概率大于 0.5 认为是高质量样本，小于 0.5 则认为是低质量样本。为严格控制高质量类别文本的输出，可提高评判基准线。本文设置阈值为 0.8，只有模型输出高质量类别下的概率值大于 0.8 才被认定为高质量样本。

3.1.4 冗余去除

数据冗余去除是指减少或消除数据中

存在的重复的信息，提升数据的丰富性，数据冗余识别本质上是文本相关性技术。

基于深度学习的文本相关性技术已经较为成熟，如基于语义理解的 ESIM^[13] 模型、基于孪生网络结构的 SBERT^[14] 模型、基于自监督对比学习的 ConSERT^[15] 模型。但深度学习文本匹配模型的时间复杂度较高，如在单次比较消耗 10ms 的情况下，在百万级规模的数据中完成一次匹配耗时达到约 170min，万级规模的数据不借助复杂的数据引擎技术基本无法完成数据冗余处理。

综合考虑系统的复杂性和处理性能问题，本文选取谷歌提出 SimHash 算法，该算法初衷是用于解决亿万级别的网页去重任务的算法。其主要思想是降维，将高维的特

征向量映射成低维的特征向量，通过向量距离来确定文章是否重复或者高度近似。

在存储阶段预先对海量样本进行处理，使用 64 位哈希值进行表示，同时将其拆分成四个部分，每个部分保存 16 位。分别使用 4 个 16 位二进制码查找对应位置上是否存在元素。如果对应位置没有元素，将哈希值直接追加到链表上；如果对应位置有元素，则将新的哈希值追加到链表尾部。

在相似判断阶段将待比较的 64 位 SimHash 签名同样拆分成 4 个 16 位的二进制码，分别与 SimHash 集合中对应位置元素进行相关性比较。该方法显著降低相似度比较的时间和次数。

3.1.5 数据采样

数据采样是一个重要的训练策略，可以减缓计算成本和计算时间的开销，定制数据以满足特定任务的需求。在领域数据量较小的情况下，也可以不进行采样，对高质量数据全部输出。数据采样通常包括随机采样 (Random Sampling)、分层采样 (Stratified Sample)、权重采样 (Weight Sampling)、过采样 (Over Sampling)、欠采样 (Under Sampling)。

本文对通用领域数据进行随机采样，对领域数据按照气候特征、降水预报气象科普、防灾减灾、气象服务等领域知识体系进行权重采样，通用数据与气象领域数据比约为 4:1。最终获取无监督训练样本情况如表 2 所示。

表 2 采样高质量数据情况

数据	语言	Token 数/B	平均长度
领域预训练数据	中文	0.03	1300

3.2 模型预训练

3.2.1 分布式计算框架

分布式计算框架是解决大规模深度学

习任务训练、推理的关键技术工具，通过将数据和计算任务在多台设备、多张 GPU 上进行处理，实现效率和性能的大幅提升。DeepSpeed 是微软研发的用于加速大规模模型训练的分布式框架，其核心优势在于减少资源消耗，保持模型的训练效果。它采用 MPI (Message Passing Interface) 技术实现节点间的通信和数据交换，支持在数千个 GPU 上进行大规模模型的训练。

DeepSpeed 的零冗余 (Zero Redundancy Optimizer, ZeRO) 技术是一种用于深度学习模型训练中的内存优化技术，它通过减少模型训练过程中的内存冗余来提高训练效率。ZeRO 技术提供三个级别的优化，每级都对显存占用和计算负载进行进一步减缓，包括：

(1) ZeRO-1: 只对优化器 (optimizer) 的状态进行分片，分散到不同的 GPU 上。在训练过程中，每个 GPU 只更新模型参数优化器一部分状态，减少单个设备的显存需求。

(2) ZeRO-2: 对优化器和梯度 (gradient) 进行分片。在 ZeRO-1 的基础上，ZeRO-2 进一步将梯度也进行分片处理，使得每个设备只需负责优化器参数和梯度参数的一部分。

(3) ZeRO-3: 对优化器、梯度和模型参数 (weight) 进行分片后分布式保存。ZeRO-3 是 ZeRO 技术的最高级别，它进一步将模型参数也进行分片处理，使得每个 GPU 只负责模型参数、梯度和优化器状态的一部分。ZeRO-3 能够最大限度地降低显存占用，在有限计算资源的情况下能够训练更大规模的模型。

ZeRO-offload 是 DeepSpeed 的优化深度学习模型训练方法，旨在将计算和数据从 GPU 卸载到 CPU 来优化大规模模型训练，核心思想是尽可能减少 GPU 和 CPU

之间的数据传输,降低计算开销,最大限度地节省 GPU 内存。具体来说,ZeRO-Offload 基于零冗余技术,通过三阶段的内存优化将梯度、优化器状态卸载到 CPU 内存中进行优化器状态更新,在 GPU 上进行参数更新。该过程利用 CUDA 流实现通信和计算的重叠,最大化训练效率。

本文训练机器显卡配置 8×A800,由于算力有限,无法采用通用大模型大规模算力集群训练的方案。本研究使用 ZeRO-2 零冗余优化技术,对梯度和优化器进行分片,实现有限资源条件下的增量预训练,配置信息如图 4 所示。

```
"zero_optimization": {  
  "stage": 2,  
  "allgather_partitions": true,  
  "allgather_bucket_size": 2e8,  
  "reduce_scatter": true,  
  "reduce_bucket_size": "auto",  
  "overlap_comm": true,  
  "contiguous_gradients": true  
}
```

图 4 训练配置 ZeRO-2 模式图

3.2.2 词表扩充

在领域增量预训练时是否进行词表扩充并非一概而论,主要取决于领域数据的特异性及其包含专业的词汇量。当领域数据存在显著差异性,包含大量未曾见过的专业术语时,词表扩充便成为提高模型适应性和表现的关键步骤。

词表扩充主要包括数据收集、分词器训练、分词器合并和分词器评估,通过收集大规模高质量的领域语料,训练领域文本分词模型,然后将该模型与原分词器进行合并,在领域测试数据上进行性能验证评估。词表扩充能够显著优化中文字符的编码效率,减少信息分割带来的损失,但急剧增加的词表规模也会增加模型的复杂度和计算需求。通常情况下,词表扩充后需进行预训练以使模型适应新词表。

本文使用开源基础模型的词表进行增量预训练,词表大小约 6.4 万,可覆盖常见的气象专业词汇。

3.2.3 模型训练

生成式预训练语言模型是自然语言处理领域的研究焦点。OpenAI 的 GPT 系列模型率先证明了大规模语言模型的强大潜力,激发了学术界与工业界的广泛兴趣。之后一系列模型如 Llama、GLM、Baichuan 等相继涌现,通过在海量数据上进行学习,显著提升了自然语言的理解和生成能力。

本研究基于 Baichuan 系列大语言模型进行气象领域增量预训练实验。Baichuan 是基于 Transformer 架构的生成式语言模型,引入了多项创新性改进,旨在提升训练的效率 and 模型的性能。具体而言,通过优化分词器并扩大词表规模,增强中文的处理效率和压缩比;采用更大规模高质量数据集进行训练,确保模型能够学到充分的知识和语言表示。在模型结构和训练策略上引入 SwiGLU 激活函数,通过增加隐藏层容量提升模型表达力,采用 RMSNorm 进行层归一化,使用 AdamW 优化器提升模型训练效率,输出嵌入层进行归一化确保模型的稳定性,使用 Max-z Loss 避免 softmax 概率分布受到异常值的影响。

本文选取 Baichuan-7B、Baichuan-13B-base、Baichuan-13B-chat 模型,使用 4W 高质量气象领域样本,上下文长度设置为 2048,进行增量预训练。

4 实验结果与分析

4.1 数据介绍

为全面评估基于增量预训练技术的军事气象领域预训练模型的效果,同时考察其保留通用知识的能力,本文构建了两套

测试集。

(1) 气象领域测试集：涵盖了军事气象领域知识，旨在评估模型对领域知识的掌握程度；示例数据如表 3 所示。

表 3 领域数据测试集示例

数据	选项	正确选项
日本气象厅的气象情报业务概念不包含以下哪项给定的选项	A. 天气预报	D
	B. 地震情报	
	C. 火山情报	
	D. 地形分析	
气象卫星大致可以分为哪两类?	A. 地球同步卫星和地球轨道卫星	B
	B. 地球同步卫星和极轨卫星	
	C. 地球轨道卫星和极轨卫星	
	D. 同步卫星和星座卫星	

(2) 通用知识测试集：侧重于非气象类通用知识，旨在评估模型吸收新领域知识的同时是否有效保留原有知识，如表 4 所示。

表 4 通用知识测试集示例

数据	选项	正确选项
下列山脉中，属于弧形山脉的是哪个?	A. 天山山脉	D
	B. 大兴安岭	
	C. 台湾山脉	
	D. 喜马拉雅山脉	
元朝政府曾经实行残酷的民族政策，把全国人民分为哪四个等级?	A. 色目人、蒙古人、汉人、南人	D
	B. 蒙古人、汉人、南人、色目人	
	C. 蒙古人、南人、色目人、汉人	
	D. 蒙古人、色目人、汉人、南人	

为量化评测过程，两套数据集均采用单选题形式，为模型的性能评估与改进提

供了坚实的数据基础。

4.2 评价指标

为准确衡量增量预训练技术对大模型在气象领域知识获取方面的影响，本实验选取可量化的方式对大模型进行评测——通过选择题评估模型对气象专业知识的掌握水平。每道选择题仅有一个正确答案，评测指标使用正确率 (Acc)。正确率的计算公式如下：

$$Acc = \frac{N_{correct}}{N} \quad (4)$$

式中， $N_{correct}$ 为模型在测试集中回答正确题目的数量； N 为总题数。

通过这一指标，直观地评估模型对气象知识的掌握程度。

4.3 实验结果

为验证领域增量预训练的效果，本实验使用相同的选择题数据集、相同的训练参数对不同基础模型下增量预训练模型进行全参微调，使得模型具备做选择题的能力。通过测试集上的表现，间接评估增量预训练模型的领域知识掌握程度。实验设置如下：

实验 1 (BASE [baichuan7B])：使用官方百川 7B 模型在气象领域测试集上进行评测。

实验 2 (CPT [baichuan7B])：基于官方百川 7B 模型，使用气象领域数据进行增量预训练得到的模型 QX-CPT-Baichuan-7B，通过有监督微调学习做选择题的能力，在气象领域选择题数据集下进行评测。

实验 3 (BASE [baichuan13B])：使用官方百川 13B 模型在气象领域测试集上进行评测。

实验 4 (CPT [baichuan13B])：基

于百川 13B 模型,使用气象领域数据进行增量预训练得到的模型 QX - CPT - Baichuan-13B,通过有监督微调学习做选择题的能力,在气象领域选择题数据集下进行评测。

实验 5 (BASE [baichuanChat13B]):使用官方 Baichuan-Chat-13B 模型,在气象领域选择题数据集下进行评测。

实验 6 (CPT [baichuanChat13B]):基于开源 Baichuan-Chat-13B 模型,使用气象领域数据进行增量预训练得到的模型 QX-CPT-Baichuan-Chat-13B,通过有监督微调学习做选择题的能力,在气象领域选择题数据集下进行评测。

实验结果如表 5 所示。

表 5 实验结果

实验	方法	是否增量预训练	正确率 (Acc)
1	BASE (baichuan7B)	否	0.20
2	CPT (baichuan7B)	是	0.32
3	BASE (baichuan13B)	否	0.22
4	CPT (baichuan13B)	是	0.54
5	BASE (baichuanChat13B)	否	0.26
6	CPT (baichuanChat13B)	是	0.56

通过对上述实验进行分析,可以得到如下结论:

(1) 通用大模型在军事气象领域存在知识欠缺的现象:实验 1、3、5 表明通用百川大模型在气象知识评测数据集上最优正确率是 0.26,说明存在领域知识不足的问题。7B 模型的领域知识欠缺问题最严重。

(2) 领域增量预训练可以提升大模型领域专业性:比较(实验 1,实验 2)、(实验 3,实验 4)、(实验 5,实验 6)可以得出,通过增量预训练技术,模型气象知识均有提升,在气象领域数据集上分

别相对提升 12%、32%、30%。

(3) 基于对话模型的增量预训练效果最优:比较实验 2、4、6 可以得出,基于对话模型进行增量预训练的 QX-CPT-Baichuan-Chat-13B 模型在气象测试集上正确率最高,达到 56%。

同时,本文选择领域效果最优的基于 QX-CPT-Baichuan-Chat-13B 微调的选择题任务模型,在通用数据集上进行评测,模型对于通用领域知识存在遗忘现象,正确率从 40% 下降至 30%。

5 结束语

本文致力于探索和构建战场环境气象领域预训练语言模型,有力验证了增量预训练技术在提升模型特定领域知识方面的显著成效。同时本研究仍然面临巨大的挑战,目前模型对于军事气象知识的表现仍有较大提升空间,增量预训练导致对通用知识的遗忘问题需要解决。

针对上述问题后续将聚焦于数据集的扩展与优化,通过收集更加丰富、全面的高质量数据,提升军事气象领域大模型的知识覆盖度,缓解模型遗忘问题。

参考文献

- 1 ZHANG Y, WARSTADT A, LI H S, et al. When do you need billions of words of pretraining data [J]. CoRR, 2020.
- 2 GURURANGAN S, MARASOVI A, SWAYAM-DIPTA S, et al. Don't stop pretraining: Adapt language models to domains and tasks [C] // ACL. 2020: 8342-8360.
- 3 ARUMAE K, SUN Q, BHATIA P. An empirical investigation towards efficient multi-domain language model pre-training [C] //EMNLP (1). 2020: 4854-4864.

- 4 GU Y, TINN R, CHENG H, et al. Domain-specific language model pretraining for biomedical natural language processing [J]. *ACM Transactions on Computing for Healthcare (HEALTH)*, 2021, 3 (1): 1-23.
- 5 HOFFMANN J, BORGEAUD S, MENSCH A, et al. Training compute - optimal large language models [J]. *CoRR*, 2022.
- 6 WEI J, TAY Y, BOMMASANI R, et al. Emergent abilities of large language models [J]. *CoRR*, 2022.
- 7 ZHANG S, ROLLER S, GOYAL N, et al. Opt: Open pre - trained transformer language models [J]. *CoRR*, 2022.
- 8 TOUVRON H, MARTIN L, STONE K, et al. Llama 2: Open foundation and fine - tuned chat models [J]. *CoRR*, 2023.
- 9 VALERO-LARA P, HUANTE A, LAIL M A, et al. Comparing Llama - 2 and GPT - 3 LLMs for HPC kernels generation [J]. *CoRR*, 2023.
- 10 BAI J, BAI S, CHU Y, et al. Qwen technical report [J]. *CoRR*, 2023.
- 11 YANG A, XIAO B, WANG B, et al. Baichuan 2: Open large - scale language models [J]. *CoRR*, 2023.
- 12 ZHANG Z, YAO Y, ZHANG A, et al. Igniting Language Intelligence: The Hitchhiker's Guide From Chain-of-Thought Reasoning to Language Agents [J]. *CoRR*, 2023.
- 13 CHEN Q, ZHU X, LING Z, et al. Enhanced LSTM for natural language inference [C] // *ACL*. 2017: 1657-1668.
- 14 REIMERS N, GUREVYCH I. Sentence - BERT: Sentence Embeddings using Siamese BERT - Networks [C] // *EMNLP/IJCNLP (1)*. 2019: 3980-3990.
- 15 YAN Y, LI R, WANG S, et al. ConSERT: A contrastive framework for self-supervised sentence representation transfer [C] // *ACL/IJCNLP (1)*. 2021: 5065-5075.

面向时变环境的大小模型协同决策方法研究**

韩云君¹ 王 玮² 张羽丰¹ 陶志坤^{1,3} 沈 震^{1*}

摘要 在时变军事、制造、服务环境中，大语言模型与小模型的协同决策模式具有强大的应用潜力。大模型负责长流程、宏观层面的规划计划，提供全面的态势感知和预测分析；小模型在微观层面执行具体任务，及时响应战场变化。这种协同方式提升了决策的准确性和灵活性，增强了对动态环境的适应能力。文章将探讨云侧大模型与端侧小模型协同进行长流程、时变决策的方法与内容，充分结合大模型的长链决策、涌现能力优势和小模型精细建模与快速求解优势，为时变环境下的军事指挥和智能生产服务等提供更加智能化和综合性的支持，提升效率与效能。

关键词 大模型，小模型，协同决策，战场任务规划

Research on Collaborative Decision-making Method of Large and Small Model under Time Varing Environment**

HAN Yun-Jun¹ WANG Wei² ZHANG Yu-Feng¹ TAO Zhi-Kun^{1,3} SHEN Zhen^{1*}

Abstract In the realm of military decision-making, the integration of large and small model collaboration exhibits significant potential. Large models are responsible for strategic formulation at the macro level, offering comprehensive situational awareness and predictive analysis. In contrast, small models execute specific tasks at the micro level, swiftly responding to battlefield dynamics. This collaborative approach enhances the accuracy and flexibility of decision-making, improving adaptability to dynamic combat environments. This paper explores the methodologies and strategies for command and control decisions through the collaboration of cloud-based large models and edge-based small models. By leveraging the long-chain decision-making and emergent capabilities of large models alongside the fine-grained modeling and rapid problem-solving strengths of small models, this study aims to provide more intelligent and integrated support for military command and operations, thereby enhancing combat effectiveness.

Key words big model, small model, collaborative decision making, battlefield mission planning

** 中国科技部政府间国际科技创新合作项目（2021YFE0116300）资助，科技部国家重点研发项目（2021YFB3301504）资助

** This work was supported in part by Intergovernmental International Scientific and Technological Innovation Cooperation Project of the Ministry of Science and Technology of China under Grant 2021YFE0116300; in part by the National Key Research and Development Program of China under Grant 2021YFB3301504

* 通讯作者

1. 中国科学院自动化研究所多模态人工智能系统国家重点实验室 2. 中国人民解放军 92942 部队 3. 中国科学院大学人工智能学院

1. MAIS, Institute of Automation, Chinese Academy of Sciences 2. Unit 92942 of the PLA 3. School of Artificial Intelligence, University of Chinese Academy of Sciences

0 引言

在军事领域，在提高装备能力的同时，加强并提高指挥控制“软”能力更为紧迫和有效。主要原因在于，敌我双方指挥机构都面临战场“迷雾”——作战决心、来袭兵器及打击目标等不确定不完备信息的严重影响^[1]；在工业领域，如面向长周期、复杂运用环境，智能起重机的全生命周期服务资源配置决策及运维管控等，也受到不确定因素影响。因此，采用人工智能、大数据及复杂系统优化等技术，降低时变环境“迷雾”影响，促进决策机制的完善，从而实现扁平化、自适应、快节奏与鲁棒决策，对提高决策效率具有重要价值。大模型凭借其强大的计算能力和广泛的适用性，能在长流程、复杂环境中提供宏观、准确的决策支持；小模型则以其快速响应和低计算成本，在资源受限的环境中表现出色^[2]。本文以作战指挥控制作为研究对象，探讨在长流程、时变环境下大小模型协同决策的方法，重点研究了相互调用机制、战场任务规划、大模型支持的小模型行动策略生成及模型的演化功能，以云侧大模型、端侧小模型的视角，研究其协同决策方法与内容。随着新一代大模型架构、智能体协同规划、合成内容可信验证等相关技术的推进，可以预见，大小模型协同决策将在军事决策领域发挥更大的使能作用。

1 战场背景下的大小模型相关概念

耗散结构理论^[3]指出，非线性反馈结构往往能形成涌现，实现量变到质变。战争巨系统具有非线性反馈结构特点，但是

传统的指挥控制全流程是战前筹划与战时控制的线性序贯决策：战场态势—指挥决策（制订作战计划）—计划实施（部队机动、侦察等预先行动）—交战控制（OODA）^[4]四个环节的战术指控过程，这导致长程的作战筹划与快节奏的交战控制缺少共振式的迭代与反馈。于是，通过构建战前作战筹划与战时指挥控制的一体化“大环”和交战阶段 OODA “小环”的大小环并行决策演化，如图 1 所示，取代传统的战前筹划与战时指挥控制线性序贯决策模式，将促使作战决策产生涌现性与动态适应性，具有颠覆性价值。

具有长链泛化决策与涌现能力的“大模型”，协同精细建模求解的“小模型”，实现作战筹划与作战控制的大小环反馈决策演进，具有优异广阔的潜力。大模型具有海量参数空间的长链与泛化决策、涌现能力优势。指挥控制的大环决策周期长、考虑要素众多且关联性复杂、以定性经验决策为主，适合采用大模型来进行指挥控制大环的宏观决策，生成作战决心，但是大模型处理特定领域时缺乏足够深入的专业知识，对复杂场景的理解不足，从而导致决策的不确定性和局限性；对应地，战时指挥控制的 OODA [观察（Observe）- Object（目标）- 瞄准（Direct）- 评估（Assessment）] 小环决策节奏快、定量决策多，一般采用小模型来求解策略，如数学模型等知识模型或者强化学习等数据模型，但是小模型缺乏宏观决策知识的引导，在特定任务上可能表现出误差或受限于其训练数据的范围，无法覆盖广泛的领域知识。大模型对算力要求高，部署在云侧，而小模型往往部署在端侧。于是，云侧大模型和端侧小模型（数学等知识模型或者小规模神经网络模型等）具有优势能力互补特点，探索两者协同的指挥控制策略生成方法，具有

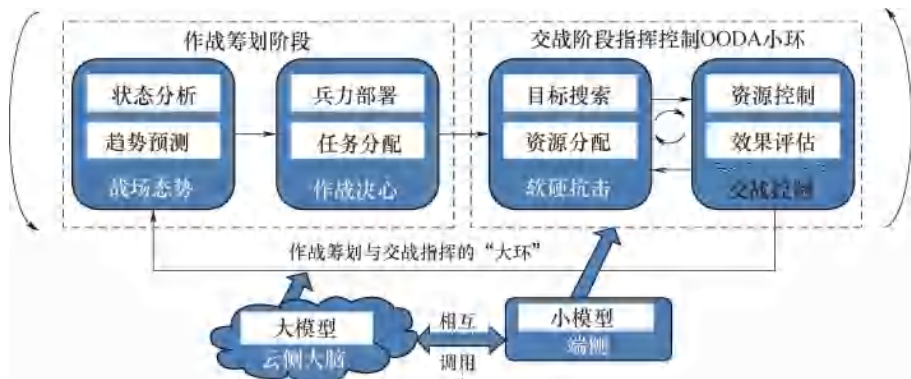


图1 面向战场指挥控制大小环的大小模型协同决策架构

广阔的应用前景。

因此,充分结合大模型的长链决策、涌现能力优势和小模型精细建模与快速求解优势,面向自动任务规划和自适应作战控制,研究云侧大模型与端侧小模型协同进行指挥控制决策的方法与内容,探索高动态作战场景下大小模型进行自适应演化的方法,以联合火力打击场景进行云侧大模型、端侧小模型协同演示验证成为战场决策模型的研究重点。该研究不仅能降低战场“迷雾”的影响,进行高动态不确定性条件下的体系作战指挥控制,还将为作战指挥机构的扁平化变革和分布式指挥协同机制完善提供强有力的技术支撑,示范引领与推动大模型在训练、装备建设等领域的应用。

2 大小模型协同调用方法研究

2.1 基于知识引导和任务评估的大模型调用小模型技术

虽然大模型在语言理解和意图识别上表现良好,但由于缺少专业任务理解和场景分析能力,其在特定场景下缺少有效的指导,整体流程可控性差,结果可信程度

低^[5]。因此,需要研究知识引导和场景反馈下的大模型技术,以进一步提高大模型处理复杂任务的能力,如图2所示。

思维链技术是一种有效的任务分解评估方法,也是当前增强模型性能的标准技术^[6]。通过引导模型“一步一步思考”,将困难的任务自动拆解为数个更简单、更具体的子任务,包括每个子任务将要调用的知识内容,使整个过程更便于管理,同时也更便于解释和追踪。在思维链的基础上,思维树技术(Tree of Thought)出现,即将思维链扩展为树状结构的形式,探索多种推理过程可能性。采用广度优先搜索和深度优先搜索的方式对每个分支进行搜索,从而得到最优的规划步骤。

为解决模型专业知识受限的问题,研究检索增强方法(RAG)^[7]优化大模型的结果生成具有很大成效。通过场景分析、智能搜索和结果增强等组件,驱动大模型从外部知识库中搜索有关当前提示文本中的精确信息,并结合大模型来优化模型结果生成的可靠性。通过知识协同作用,减少模型出现幻觉的问题,实现更精确、更智能的任务执行和控制,提高上游的指挥决策,调动下游小模型完成更为细致的任务。

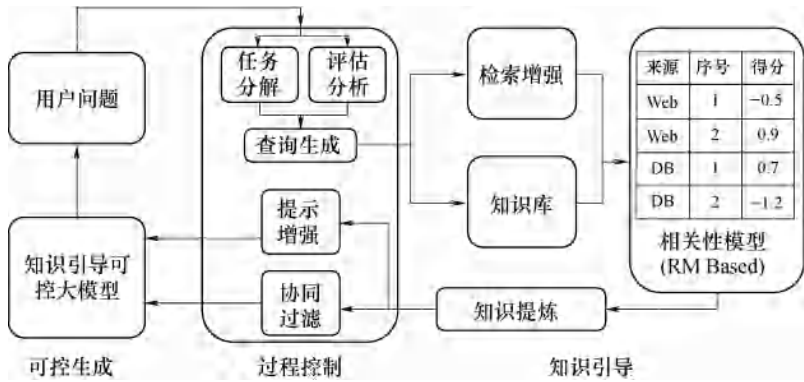


图 2 基于知识引导和任务评估的大小模型协同调用技术

2.2 小模型支持下的 大模型演化

目前大模型普遍存在对动态场景适应能力不足的问题，由于当前的大模型上下文长度都是十分有限的，历史的信息经常会出现遗忘的情况，模型难以对已有知识学习融会贯通^[8]。因此，需要研究具备记忆与自适应能力的小模型协同大模型演化技术，以解决大模型实际应用中的长上下文问题和遗忘问题，为大模型决策提供可成长能力。

记忆能力分为短时记忆和长时记忆：短时记忆又叫模型的工作记忆，它只能记录最近几轮的会话上下文，长度通常也是有限的；长时记忆则可称为持久化记忆，通过将上下文内容向量化（Embedding）表示并创建索引，存储在外部的向量数据库中，在需要时进行动态读取并载入短时记忆使用，实现知识的动态记忆。一般由于在向量数据库中的长时记忆存储量极大，需要采用高速的检索访问方法，如相似度计算或最大内积搜索等，提高相关知识的命中率。另外，通过使用检索增强的 DIT 方法对大模型和 Agent 检索器同时优化，最大限度地提高给定检索指令情况下正确答案的概率，并引导大模型即使在检索错误的情况下也能利用自身知识产生正确的回

答，实现模型的自适应性更新和优化。

在此基础上，使用预训练与微调、模块化设计、多级架构、知识蒸馏、协同训练等方法，使得小模型和大模型在实际应用中能够相互支持和互补，提高系统的整体性能和效率，实现大模型的持续演化。

2.3 基于图卷积网络的决心特征提取

传统的深度学习方法被应用在提取欧氏空间数据的特征方面取得了巨大的成功，但许多实际应用场景中的数据是从非欧式空间生成的，传统的深度学习方法在处理非欧式空间数据上的表现却仍难以使人满意^[9]。图的复杂性使得现有的深度学习算法在处理数据时面临着巨大的挑战。这是因为图是不规则的，每个图都有一个大小可变的无序节点，图中的每个节点都有不同数量的相邻节点，导致一些重要的操作（如卷积）在图像上很容易计算，但不再适合直接用于图。此外，现有深度学习算法的一个核心假设是数据样本之间彼此独立。然而，对于图来说，情况并非如此，图中的每个数据样本（节点）都会有边与图中其他实数据样本（节点）相关，这些信息可用于捕获实例之间的相互依赖关系。

图的特殊结构可以承载更多的节点信

息,因此,可以通过低维的向量信息来表征图的节点及拓扑结构,这种方法可以很好地处理非欧几里得空间上的数据,让网络模型容易学习到有效的特征信息。可以用图来建立场景本体的模型。

通过利用本体知识,融合边与节点结

合的信息,学习出一个为节点嵌入的低维度向量。为了进行预测,可以将低维度向量输入深度强化学习网络,并通过神经网络进行传递优化,见图3。例如,一个序列化的决策任务,利用RNN网络,该模型可以通过以往的访问信息进一步增强。

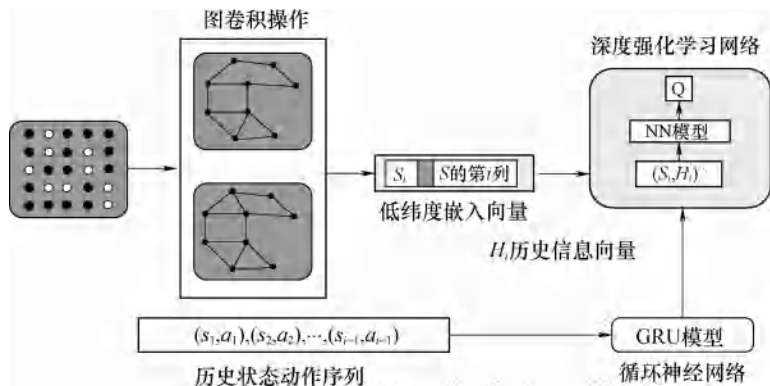


图3 本体知识图网络嵌入强化学习模型

3 自动任务规划的决心生成研究

3.1 大模型多模态指令微调

经过预训练,基础大模型会从大规模语料库中掌握相当广泛的语言知识(专业知识、回答逻辑、语义语法等),能够自然地生成符合人类语言习惯的回答,但是基础大模型并不具备专业场景中决策生成的能力^[10]。为了让大模型具有通过回答用户提问的方式完成专业场景决策生成的能力,需要使用多模态指令微调技术对基础预训练大模型进行微调。多模态指令微调是人工智能领域的一个重要研究方向,其目标是使计算机系统能够理解并执行人类提出的多模态指令,图文混合的指令。这种技术有着广泛的应用潜力,如智能家居控制、机器人导航、虚拟助手等。对于预训练好的基础大模型,其已经学得了大量

的基础知识,只需要使用极少量的指令数据对大模型进行微调即可在下游专业任务中获得显著的效果,使其的输出更加规范化并可以回答用户各种提问。

对于以往的单模态模型,指令数据通常由三部分组成,分别为指令文本、输入文本以及输出文本,其中指令文本为人提供给计算机的问题或命令,输入文本通常是对指令的进一步更详细的描述,输出文本为计算机对指令和输入做出的回答或响应,指令数据通常富含丰富的语义信息和人类意图,因此,预训练大模型和指令微调技术的结合可以广泛地应用于生产生活的方方面面,如可控文本生成、人类意图识别等。

对于多模态预训练大模型,研究者^[11-13]从信息流的角度出发,按照以下技术路线设计多模态大模型的指令微调路线:首先,模型需要先通过一系列预处理步骤理解输入的多模态信息;其次,利用相应的多模态指令对这些信息进行分析

处理；最后，生成相应的多模态响应。这一过程涉及多种复杂的技术，如自然语言处理（NLP）、计算机视觉（CV）、深度学习、强化学习等。需要指出的是，无论在NLP领域还是多模态领域，指令微调都是有监督训练，具体做法为将图像/文本输入转化为一个输入序列向量，然后采用自回归（auto-regressive）的方式预测下一个分词（token），最后使用交叉熵计算自回归的损失函数值。

如图4所示，使用大模型进行多模态指令数据集的构建。首先拥有少量的种子指令集，以及相应的输入和输出实例集，种子指令集和实例集由专家提供，其数量一般小于200个，与基于人类反馈和强化

学习来设计大量指令数据的方法相比，基于大模型构建指令数据集所需的人工设计指令的工作量极大地减少。大模型基于提示模板和种子指令集生成大量新的指令数据和相应的输入输出实例，进而使用生成的指令数据集对大模型进行下游任务的指令微调。与知识蒸馏相比，这种指令数据集的构建有两个显著的不同点：①知识蒸馏使用大模型的知识指导小模型的训练，本方法使用大模型本身来指导大模型在下游任务的微调；②知识蒸馏仅仅能提取到大模型学习到的领域内的知识，而本方法生成的指令数据以及相应的输入输出实例大部分位于预训练阶段数据分布之外。

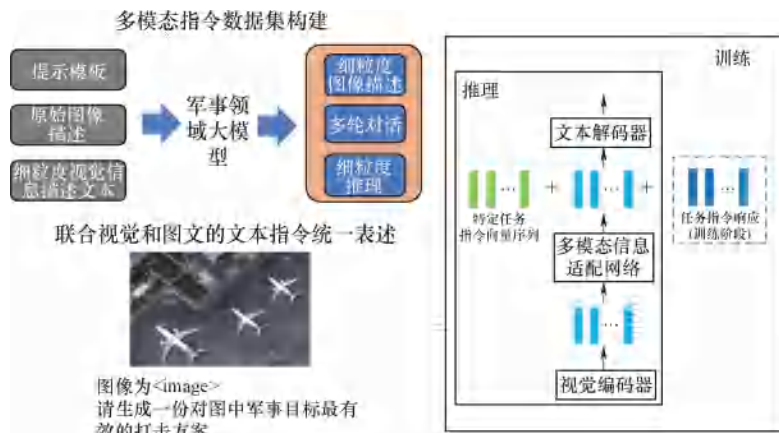


图4 基于多模态指令自构建的大模型微调技术

指令微调阶段，对一幅图像而言，有可能有多个指令，每个指令又有可能有多个响应（多轮对话，不同角度的细粒度图像描述等），因此，每次迭代前以等概率随机采样当前图像的一个指令，再从当前指令相应的输入-响应集合中以等概率随机采样一个输入-响应对，其中指令的输入有可能为空。将采样的指令文本、指令的输入文本、指令的响应文本以及多模态信息适配网络的输出序列拼接，共同作为

文本解码器的输入序列，根据指令文本的形式不同，多模态信息适配网络输出的拼接位置有可能不同。

下游任务推理阶段，模型的输入由指令文本、指令的输入文本以及多模态信息适配网络的输出序列三部分组成，与指令微调阶段相同，三部分输入共同作为模型的指令响应的提示信息。推理阶段预训练多模态大模型每次前向传播输出一个分词，直到达到指定的结束分词或者模型允

许的最大生成长度为止。

3.2 基于上下文提示与细粒度思维链的大模型自动任务规划生成

经过指令微调，大模型具有了生成专业任务决策的能力，但其生成的内容很多时候会出现逻辑有误、脱离人类意图期

望、语句无意义重复、产生误导性信息等不可控问题。因此，为了让大模型生成合乎逻辑、可行的决策安排，可控文本生成的重要性便显得尤为重要。从逻辑上约束大模型生成的决策计划，使生成的方案可行，同时可防止有矛盾的事项发生，如图5所示。

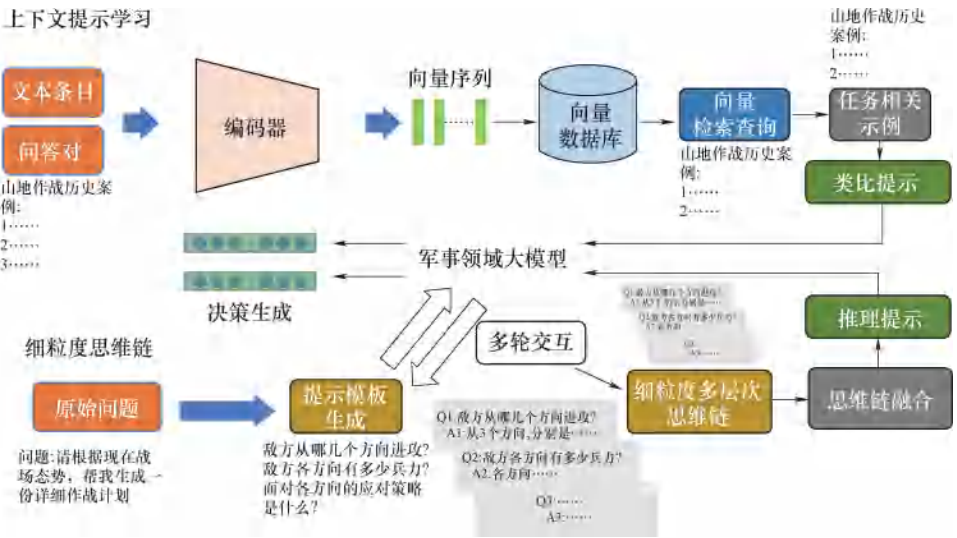


图5 基于上下文学习和细粒度思维链的任务决策生成

(1) 上下文提示学习技术。即设计基于任务和样本相似性的向量检索模块，面向多模态数据库中获取多个与当前输入和任务最相似的示例，使用编码器对多模态数据和任务在向量空间进行统一表示，保证具有相似任务和相似输入的数据会具有接近的嵌入，从而收集链接到对当前任务和输入最有帮助的示例，在构造合理示例的同时减少模型和计算量，同时针对已有的多模态数据构造向量数据库，保证查询检索效率，降低查询成本。

(2) 细粒度思维链技术。构造细粒度多层次的思维链作为大模型的推理路径，将视觉问答、图像描述等主流跨模态任务分解为多个中间推理步骤 (rationale)，构建一个两阶段的推理框架、细节描述和文

本生成，第一阶段对多模态信息进行细节描述，使用不同的提示模板引导大模型输出人物相关的细粒度信息，比如对于战机轮胎的一阶段推理，可以通过提示“敌方从哪几个方向进攻？”→“敌方各方向有多少兵力？”→“各方向的应对策略是什么？”等思维链来完善模型的细粒度和多个层次的细节描述。第二阶段是利用第一阶段的生成结果作为提示输出最后的结果。相比于之前的方式，更符合人类推理习惯，并且适用于复杂的可控文本生成任务，将复杂问题分步求解，提高文本生成的可控性。

在军事领域，任务规划是关键的重要组成部分，涉及从战略决策到战术执行的各个层面。基于上下文提示与细粒度思维链的

大模型自动任务规划生成技术,利用人工智能的强大计算能力和复杂数据解析能力,为军事任务规划提供了高效且精准的解决方案。

4 决策生成与模型演化

4.1 基于深度强化学习的小模型策略生成

通过图卷积网络进行特征提取,以屏蔽大模型生成的多样化决心对小模型神经网络架构的影响,同时有利于小模型的收敛;然后采用部分可观测马尔可夫决策方法来构建非完备信息下的“软”“硬”攻防模型,并采用多智能体强化学习进行策略求解;为了进一步增强模型的适应性,采用平行学习方法来研究小模型演化技术。

在单元实体较多,多智能体系统状态空间和动作空间的维度较大,单智能体强化学习算法无法学习到有效的策略^[14-15]。如果将多智能体系统中的每个单元看作一个智能体,并为每个智能体分配一个动作价值函数或策略函数,每个智能体的策略都会影响环境的变化,使环境维持一个非稳态状态,使得策略梯度中的方差被放大,这给智能体的学习造成了极大的困难,这也不符合传统强化学习的收敛条件。采用多智能体强化学习算法,成为解决多智能体博弈问题的有效方法之一。

首先,为加快收敛和提高求取的策略性能,可以采用数据和机理协同的方法来辅助训练多智能体网络。多智能体调度系统内置多智能体调度的约束关系模型和回报函数,内置规则引擎融合调度规则知识,解决动作转化、动作冲突、动作组合顺序调度等问题。

其次,在策略运用上,考虑融入决策

规则引擎,引入专家知识,根据实际情况联合决策调度方案。

再次,在数据训练上,将快速求解模型求取的方案(如通过数学模型求取的目标分配方案等)以及专家经验转化为多智能体网络可以使用的经验轨迹,输入训练网络以辅助学习,以期提高学习效率。

最后,将不确定性情况下实时调度算法的预测值与最优解进行比较,分析其与最优解的差距,对算法性能进行统计分析。

4.2 基于序列生成对抗模仿学习的小模型演化

环境是一个高动态、强实时、紧耦合的复杂系统,少量场景下的策略生成模型无法做到一次训练、终身使用的程度。需要结合场景进行计算实验和渐进式学习,实现模型演化,不断提高模型的适应性和求解的精度。

序列生成对抗模仿学习框架通过数据迭代和模型学习迭代,实现“小数据”到“大数据”的数据生成和模型演化^[16-17]。反馈数据包括采集战史上数据或者实战训练的专家方案,以及通过确定性模型的精确求解的最优方案,它们作为生成对抗强化学习模型的专家标本,以帮助生成模型改进性能。

多阶段决策场景涉及序列决策问题,需要考虑先前决策对后续决策影响。序列生成对抗模仿学习模型用于解决生成序列决策模型如何学习专家的序列决策方案。序列生成对抗模仿学习的基本原理是迭代训练生成模型 G 和判别模型 D。假设用 G 生成一个动作序列组成一个决策方案,由 D 来判别这个方案是训练集中的真实方案(True Data)还是模型生成的方案(Gen-

erate); 最终目标是用模型 G 生成以假乱真的方案, 让 D 无法分辨。其操作过程如图 6 所示, 详细描述如下:

左侧部分表示当前的状态, 右侧部分则详细描述了从当前状态出发, 通过一系列步骤和策略选择, 最终到达未来目标状态的过程。在这个过程中, 蒙特卡罗搜索用来评估和选择最佳路径, 基于每一步的奖励值和

策略确定度来进行决策。在单次操作中, 模型多次调用生成模型 G 和判别模型 D。右侧的每一个圈是生成一个决策的操作, 状态为已生成的动作与环境信息, 在生成下一个决策时, 先调用生成模型 G 生成多个备选项, 然后使用判别模型对各个选项评分, 根据评分选择最好的策略, 并调整策略梯度, 在不断的迭代过程中, 达到最优。

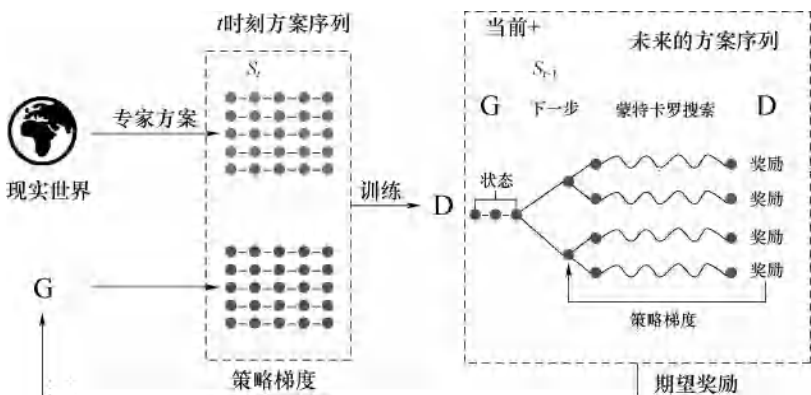


图6 序列生成对抗模仿学习框架

5 结束语

在当前环境下, 大小模型协同决策研究在军事领域展示了显著潜力。大小模型端云协同进化是生成式基座模型赋能多场景应用的重要技术, 涵盖基座大模型、大模型小型化、大小模型协同等关键研究方向, 具有端侧实时性、可扩展性、负载低、隐私安全强等优势, 是生成式人工智能未来发展的重要方向。通过整合大模型的广泛数据解析能力和小模型的快速响应特点, 可以实现更加精准和高效的军事决策。大模型能够处理复杂的战略分析和长远规划, 而小模型则适用于实时战术调整和局部优化。这种协同方式不仅提升了决策的准确性和灵活性, 还增强了对动态战场环境的适应能力。未来, 随着人工智能

技术的不断进步, 大小模型的协同将进一步深化, 为军事指挥和行动提供更加智能化和综合性的支持, 显著提升作战效能。

参考文献

- 1 陈德峻, 方子豪, 曾云秀, 等. 战场迷雾中的欺骗路径规划 (英文) [J]. 系统仿真学报, 2023, 35 (9): 1895-1908.
- 2 王永威, 沈弢, 张圣宇, 等. 大小模型端云协同进化技术进展 [J]. 中国图象图形学报, 2024, 29 (6): 1510-1534.
- 3 孙飞, 李青华. 耗散结构理论及其科学思想 [J]. 黑龙江大学自然科学学报, 2004, 21 (3): 76-79.
- 4 李强, 鞠卓亚, 阳东升, 等. 面向跨域联合作战的平行指挥控制与管理新范式 [J]. 指挥与控制学报, 2024, 10 (2): 137-145.
- 5 王寿彪, 李新明, 裴忠民, 等. 基于大数据的装备体系认知计算系统分析 [J]. 指挥与控制

- 学报, 2016, 2 (1): 54-59.
- 6 林博, 王尚文, 毛晓光. 基于思维链的软件漏洞自动修复技术研究 [J]. 软件学报, 2024: 1-23.
- 7 JEONG C. Generative AI service implementation using LLM application architecture: based on RAG model and LangChain framework [J]. Journal of Intelligence and Information Systems, 2023, 29 (4): 129-164.
- 8 李晓光, 魏思齐, 张昕, 等. LFKT: 学习与遗忘融合的深度知识追踪模型 [J]. 软件学报, 2021, 32 (3): 818-830.
- 9 WU Z, PAN S, CHEN F, et al. A comprehensive survey on graph neural networks [J]. IEEE transactions on neural networks and learning systems, 2020, 32 (1): 4-24.
- 10 罗俊仁, 张万鹏, 苏炯铭, 等. 面向智能博弈的决策 Transformer 方法综述 [J]. 指挥与控制学报, 2023, 9 (1): 9-22.
- 11 LI L, ZHANG Y, CHEN L. Prompt distillation for efficient llm-based recommendation [C] // Proceedings of the 32nd ACM International Conference on Information and Knowledge Management. 2023: 1348-1357.
- 12 LIU Z, HE X, TIAN Y, et al. Can we soft prompt LLMs for graph learning tasks? [C] // Companion Proceedings of the ACM on Web Conference 2024. 2024: 481-484.
- 13 MAHARJAN J, GARIKIPATI A, SINGH N P, et al. OpenMedLM: prompt engineering can out-perform fine-tuning in medical question-answering with open-source large language models [J]. Scientific Reports, 2024, 14 (1): 14156.
- 14 王龙, 黄锋. 多智能体博弈, 学习与控制 [J]. 自动化学报, 2023, 49 (3): 580-613.
- 15 PENG S, XIONG G, YANG J, et al. Multi-Agent Reinforcement Learning for Extended Flexible Job Shop Scheduling [J]. Machines, 2023, 12 (1): 8.
- 16 李渊, 刘运韬, 徐新海, 等. 面向博弈对抗的多智能体强化学习建模与迁移技术 [J]. 指挥与控制学报, 2024, 10 (2): 226-231.
- 17 刘小虎, 张恒巍, 张玉臣, 等. 欺骗谋略在网络空间防御行动中运用 [J]. 指挥与控制学报, 2024, 10 (1): 117-121.

面向用例生成与代码优化的 多智能体软件测试框架

杨 军¹ 何宇巍¹ 刘行健¹

摘要 随着软件系统的规模和复杂性的持续增长，尽管传统的自动化测试方法及基于大语言模型（LLMs）的测试策略在提高测试自动化效率方面取得了一定的成效，但这些方法在处理复杂的代码逻辑和深层语义理解方面仍存在不足，导致生成的测试用例无法全面覆盖或精确测试软件的关键功能。为此，文章提出了一种面向用例生成与代码优化的多智能体软件测试框架。该框架利用多智能体系统的协作能力与 LLMs 的高级语言理解能力，通过智能体间的信息交换和策略协调，显著提高了对软件系统代码理解及测试用例生成的质量。在本框架中，每个智能体专注于软件测试的一个特定环节，包括需求分析、测试用例生成和代码优化等，协同合作产生更为全面和深入的测试结果。通过在多个实际软件测试项目中的应用，文章验证了该框架在提升软件测试质量和效率方面的有效性。

关键词 软件测试，大语言模型，多智能体

Multi-Agent Framework for Test Case Generation and Code Optimization

YANG Jun¹ HE Yu-Wei¹ LIU Xing-Jian¹

Abstract With the continuous growth in the scale and complexity of software systems, traditional automated testing methods and strategies based on large language models (LLMs) have achieved some success in enhancing the efficiency of test automation. However, these methods still fall short in handling complex code logic and deep semantic understanding, resulting in test cases that cannot comprehensively cover or accurately test the key functionalities of software. To address this issue, this paper proposes a multi-agent framework for test case generation and code optimization. The framework leverages the collaborative capabilities of a multi-agent system and the advanced language understanding of LLMs. Through the exchange of information and coordination of strategies among agents, it significantly enhances the quality of software system code understanding and test case generation. In this framework, each agent focuses on a specific aspect of software testing, including requirement analysis, test case generation, and code optimization, working collaboratively to produce more comprehensive and in-depth testing outcomes. The application of this framework in multiple real software testing projects validates its effectiveness in improving the quality and efficiency of software testing.

Key words software testing, large language models, multi-agent

1. 中国电子科技集团公司第十五研究所

1. The 15nd Research Institute of China Electronics Technology Group Corporation

0 引言

软件测试是确保软件产品质量和可靠性的核心环节。随着软件系统的规模和复杂度的不断扩大,对高效自动化软件测试技术的需求变得更为迫切。通过实施全面细致的测试程序,企业能够显著减少关键软件故障,提升系统可用性,并防止可能导致财务损失或侵害用户信任的安全漏洞。此外,软件测试有助于在开发生命周期的早期阶段识别并解决问题,从而降低后期维护成本并避免未来出现更复杂的问题^[1]。

然而,当前自动化软件测试领域仍面临多项挑战。尽管现有的基于搜索^[2]、基于约束^[3]或基于随机的方法^[4]能够生成测试套件,但这些方法往往无法充分理解代码的语义信息,导致无法实现全面的测试覆盖。与此同时,大语言模型(LLMs)因其出色的文本语义理解能力,在代码生成和代码推荐等多种编程相关任务中已显示出巨大潜力。

尽管大语言模型(LLMs)在自动化软件测试领域展现出了潜力^[5],软件测试的核心挑战在于生成多样化的测试输入,以全面覆盖被测的软件,并验证代码在各种情况下的正确执行性,满足预定的功能和性能要求。这不仅要求对代码的运行逻辑有清晰的认识,还需深入理解软件的应用场景和用户需求。目前基于LLMs的方法主要关注代码的运行逻辑,尚不足以满足这些复杂要求。

针对这些挑战,提出了一种面向用例生成与代码优化的多智能体软件测试框架。该框架通过多智能体的协同合作,旨在提高软件测试的效率和质量。各智能体负责生成结构化输出,如高质量的需求分

析、方案设计和代码生成,且每个智能体都具备特定的角色和专长,严格遵循既定的标准。这种基于智能体的方法能够在运行时自动进行需求分析、代码生成、代码校验与修改,展示了增强软件测试能力的可行性。我们已在实际软件工程项目中测试了该框架,并取得了显著的执行覆盖率和错误修复率的提升,有效证明了该框架在实际软件测试应用中的高效性和实用性。

1 相关工作

1.1 软件测试及传统方法

软件测试是确保软件产品质量和可靠性的关键手段。传统的软件测试方法包括基于搜索的测试、基于约束的测试以及基于随机的测试^[2-4],在自动化生成测试用例方面取得了一定成就。然而,这些方法在覆盖范围和深度上仍存在局限。例如,在移动 GUI (Graphical User Interface) 测试领域,现有方法常常未能充分理解 GUI 界面的语义信息,从而导致测试覆盖不全面^[6]。

1.2 大语言模型在软件测试中的应用

随着如 OpenAI 的 GPT 系列等大语言模型(LLMs)在各行业的广泛应用^[7],这些模型在代码生成和结构分析方面展示了巨大潜力。研究如文献 [5] 已展示了利用LLMs进行自动化测试用例生成的方法,这表明了它们在软件测试领域的潜在应用价值。尽管如此,LLMs在生成多样化测试输入时面临挑战,主要由于这些模型在训练过程中往往缺乏对特定应用场景和用户需求的深入理解,可能导致实际测试中无法达到理想的测试覆盖率。

1.3 基于大语言模型的多智能体

近年来,基于大语言模型的多智能体系统在解决复杂问题方面显示出显著优势。例如,文献[8]中的 Stable-Alignment 项目通过智能体在沙盒环境中的互动,创造了基于共识的指导数据集,这对于模拟软件测试场景和理解需求至关重要。文献[9]中的 Generative Agents 项目则通过模拟智能体的社会互动,提供了一种深入理解用户行为和应用场景的新途径。多智能体系统通过整合不同智能体的专业知识和角色,提升智能应用的最终效果,而本研究搭建的多智能体软件测试框架利用这些优势,通过智能体的协作,有效提升了测试用例的生成质量和测试覆盖率。

2 多智能体软件测试框架

多智能体软件测试框架通过模拟软件测试全流程,整合各智能体的专长和功能,以提高测试质量和效率。每个智能体承担不同的角色,从需求分析到代码校验,通过精确的协同作业,提升了测试代码的生成效率和质量。这种协作不仅优化了软件测试流程,还增强了软件产品的可靠性和性能,确保软件系统能够在复杂多变的环境中稳定运行。

2.1 软件测试基本流程

首先,对软件测试的基本流程进行介绍,这有助于理解方法架构。具体流程如下:

(1) 需求分析:业务分析师负责收集和分析用户需求,确保需求的完整性和可测试性。产品经理定义产品的功能和市场定位,参与需求讨论,确保需求符合市场和业务目标。测试工程师,从

测试的角度理解需求,提出可能的问题和澄清点。

(2) 测试计划:测试经理负责制定整体测试策略和计划。测试工程师参与测试计划的制订,提供实施细节。

(3) 测试设计:测试工程师设计详细的测试用例和测试脚本。

(4) 测试环境的搭建:开发工程师提供必要的软件工具和版本。测试工程师确保测试环境符合测试需求。

(5) 测试执行:测试工程师执行测试用例,记录测试结果。

(6) 缺陷管理:测试工程师发现并记录缺陷。开发工程师负责缺陷的修复。测试经理监控缺陷的处理进度和质量。

(7) 测试报告:测试工程师编写详细的测试报告。测试经理审核测试报告,提供高层次的总结和评估。

(8) 回归测试:测试工程师执行回归测试,确保修改没有引入新的问题。

2.2 多智能体软件测试 workflow

在多智能体软件测试框架中,各个智能体都担当至关重要的角色,配合执行高度专业化的分工以产生结构化的输出。这些输出覆盖从需求分析、方案设计直至用例生成和代码校验的完整流程。通过将复杂任务细分为具体、可控的步骤,框架不仅加快了处理速度,还显著提高了输出结果的精确度和可靠性。

整个基于多智能体的软件测试流程 C 可以看作一个有限状态机,其中的状态对应软件测试流程的不同步骤。图1呈现了该状态机的转移流程,对于一个特定状态 S^i ,参与其中的智能体集合 \mathcal{P}^i 与环境 \mathcal{I} 发生交互,其中,环境会根据当前所处状态,通过提示词给每个智能体 \mathcal{A}^i 分配任

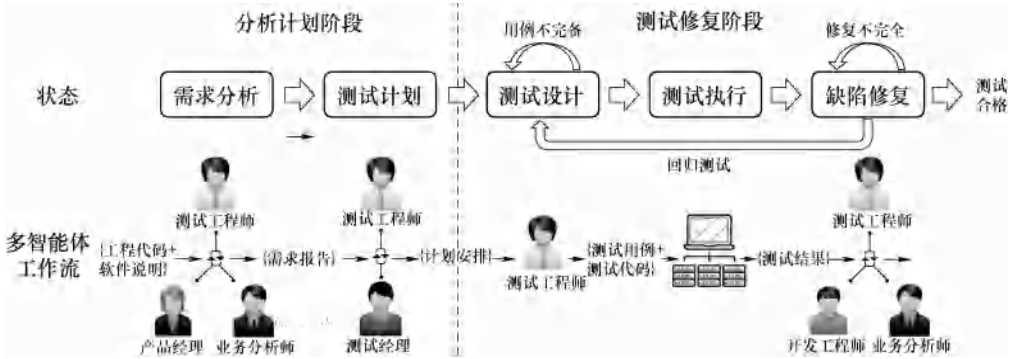


图 1 多智能体软件测试状态机

务，而智能体在输出结果并返回给环境后，环境会根据当前状态的评估标准进行判断，是继续进行对话还是进入下一状态。整个面向智能体工作流的有限状态机可以形式化地表示为：

$$C = \langle S^1, S^2, \dots, S^{|C|} \rangle$$

$$S^j = \tau(C(I, P^j)) \quad (1)$$

$$P^j = \langle A^1, A^2, \dots, A^{|P^j|} \rangle$$

$$C(I, P^j) = \langle I \rightarrow P^j, P^j \rightarrow I_c \rangle$$

测试流程在宏观上可以分成分析计划和测试修复两个阶段，第一阶段输出以分析文档为主，整个处理流程相对比较线性；第二阶段输出以测试代码、用例和修复后的软件代码为主。第二阶段的状态中加入了测试完备性和代码缺陷率的评估，因此，状态转移相对比较复杂， $C(I, P^j)$ 的轮次也会更多。

在具体实施中，多个智能体通过共享和协作机制，利用环境 I 的集中化信息池来交换关键信息。整个工作流框架如图 2 所示，每个智能体都依据自己独特的职责，从这个信息池中筛选出需要响应的信息。这个过程包括对事件的筛选和信息的提取，以明确当前阶段必须执行的操作和必需的上下文信息。通过精心设计的语言提示，确保了智能体间的信息交换既完整

又精确。例如，业务分析智能体从商业角度深入分析用户需求，确保需求的完整性和可测试性；产品经理智能体重点关注产品功能的市场定位，确保所提需求与业务战略保持一致；测试工程师智能体则依据这些需求设计出旨在全面覆盖所有功能和性能标准的测试代码。

智能体筛选并处理的任务和信息经过大语言模型的进一步处理后，结果会被反馈回信息池，为后续的测试用例生成和优化提供数据支持。这种基于智能体的协同工作流程不仅极大地优化了测试过程，而且显著提升了软件产品的测试质量和开发效率。这种高度集成的协作模式使得框架能够有效适应快速变化的软件开发需求，确保软件系统在多变的应用环境中保持健壮性和高性能。

2.3 单智能体工作流程

在多智能体软件测试框架中，单个智能体的工作流程详细而精确。以测试工程师智能体为例，对智能体的运行逻辑进行形式化的介绍。测试工程师的核心目标是生成具有高覆盖率的测试用例，确保软件测试的全面性和效率。为达到这一目标，构建了以下模型组件：状态空间 (S)：状态空间包括测试工程师智能体当前接收的

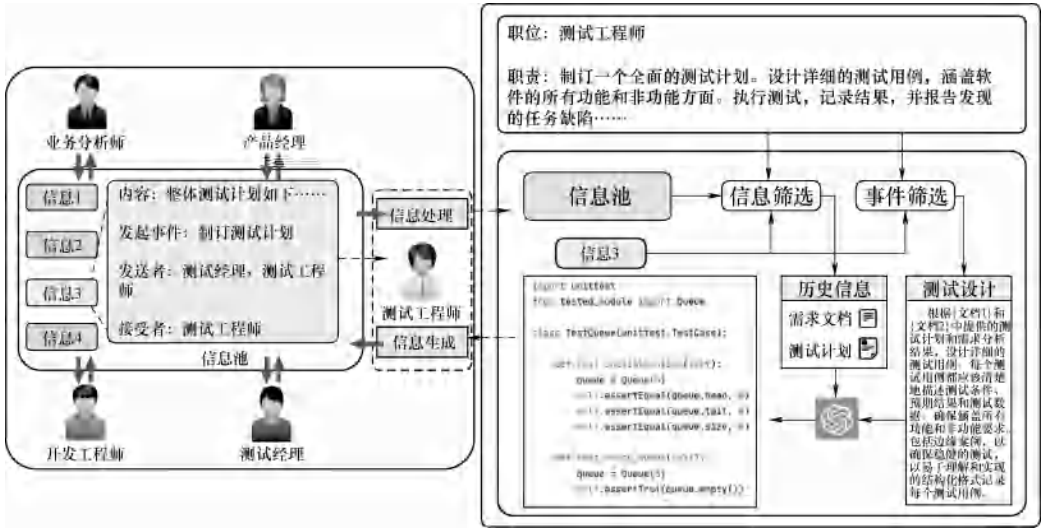


图2 多智能体软件测试工作流程框架

所有历史测试用例、测试结果和当前的测试需求。其中，任何一个状态 s 可以包含特定的软件信息、已执行的测试用例以及待测功能的详细描述。

动作空间 (A): 动作空间定义了测试工程师智能体可以执行的所有可能动作，这些动作包括选择测试用例模板、配置测试参数、生成特定的测试代码等。每一个动作 a 都是为了达到更好的测试覆盖率而精心设计的。

策略 (π): 策略 π 是一个决策规则，用于指导智能体在给定状态 s 下选择最优动作 a 。这基于历史数据，通过大语言模型从过去的经验中归纳得到。为了评估在特定策略下的长期表现，采用了价值函数 $V^\pi(s)$ ，该函数定义为期望的折现累积奖励，数学表达式为：

$$V^\pi(s) = \left[\sum_{k=0}^{\infty} \gamma^k R_{t+k+1} \mid s_t = s, \pi \right] \quad (2)$$

式中， γ^k 为折扣因子，用于平衡即时奖励和未来奖励的重要性。

通过评估这一价值函数，智能体可以

更有效地优化测试覆盖率，并在复杂的测试环境中做出更精确的决策。

状态转移概率 (P): 状态转移概率 $P(s_{t+1} \mid s_t, a_t)$ ，描述了在执行某个动作 a_t 后从当前状态 s_t 转移到新状态 s_{t+1} 的概率。这反映了测试动作对智能体的影响，是动态测试过程的核心部分。

奖励函数 (R): 奖励函数 $R(s_t, a_t, s_{t+1})$ 与覆盖率改变密切相关。

$$R(s_t, a_t, s_{t+1}) = C(s_{t+1}, a_t) - C(s_t, a_t) \quad (3)$$

式中， $C(s, a)$ 为动作 a 执行后的代码覆盖率：

$$C(s, a) = \frac{\text{被测试动作 } a \text{ 覆盖的功能点}}{\text{总功能点}} \quad (4)$$

则激励智能体选择那些能够显著提升覆盖率的测试动作。

测试工程师智能体的具体工作流程包括：

- (1) 事件识别与分析：智能体识别当前的测试需求，并分析环境状态 s 。这包括从状态空间中获取当前已执行的测试用

例和测试结果，以及待测功能的详细描述。

(2) 决策制定：根据当前状态 s_t ，智能体选择最佳的动作 a_t 。选择策略通过分析历史测试数据和大语言模型构建得到。

(3) 测试代码生成：执行选定的动作 a_t ，并通过测试代码生成模块生成高覆盖率的测试代码。

(4) 覆盖率评估：评估生成代码的覆盖率变化，即奖励函数 R ，用于衡量动作的有效性。

(5) 信息反馈与状态更新：将测试结果和代码覆盖率反馈到信息池，并更新智能体的状态空间，以此作为新的状态 s_{t+1} 。

(6) 长期性能评估：使用价值函数 $V^\pi(s)$ 来评估智能体在当前策略下的长期表现。通过迭代这一流程，智能体不断优化其策略，以提高测试质量和效率。

通过这种高度集成的策略和 workflows，测试工程师智能体能够有效应对复杂的软件测试需求，确保在多变的应用环境中保持软件系统的健壮性和高性能。这不仅优化了测试过程，还显著提升了软件产品的测试质量和开发效率。

3 实验

在本研究中，使用了 MetaGPT 工具^[10]进行多智能体软件测试框架的搭建。文本和代码的生成则采用了 GPT-3.5 模型。考虑到 GPT-3.5 模型的输入长度限制为 4096 词元，若一次对话输入超过此长度，将对需求分析等描述性语句进行精简。此外，对于测试代码生成和修复代码生成的部分，在每轮输出后，询问智能体是否已完成所有输出。若确认输出完毕，则标注“输出完成”，以确保输出内容的完整性和准确性。

3.1 软件代码分支覆盖

首先，进行软件代码分支覆盖的实验。从参考文献 [11] 提供的测试工程中随机选择了 50 个代码模块进行对比分析。表 1 中的实验结果显示，与传统的软件测试方法（Random 随机游走，MOSA，MIO，DynaMOSA）和直接使用大语言模型的测试策略（LLMs-based）相比，多智能体框架在分支覆盖率方面展现出了显著的优势。这一发现强调框架在提高分支覆盖效果方面的潜力。

表 1 软件代码分支覆盖实验结果

方法	覆盖率 (%)
Random	65.6
MOSA	70.5
MIO	70.3
DynaMOSA	70.7
LLMs-based	71.0
Ours	71.8

3.2 软件代码修复

同时，对代码修复功能进行了详细的测试。本实验使用了 BugsInPy 数据集，这是一个专门包含 Python 代码缺陷的集合，总计有 493 种不同类型的缺陷^[12]。为了进行这项实验，从中随机选取了 50 个不同的缺陷并进行缺陷修复的测试，其中，PyTER 是当前表现较为初色的传统软件代码修复方案，如表 2 所示。

表 2 软件代码修复实验结果

方法	覆盖率 (%)
PyTER	35.7
LLM-based	37.1
Ours	39.8

实验结果表明，多智能体软件测试框架在代码修复方面表现出色，证实了其在识别和修正代码缺陷中的有效性。

图3展示了代码缺陷在本框架中修复的具体过程。从图中可见，测试工程师智能体通过执行其生成的测试用例，成功地识别出了缺陷，并进行了详尽的分析。分析中发现，问题源于队列为空的判定函数。基于这一分析，测试工程师智能体随后进行了准确的缺陷修正。



图3 缺陷修复流程示例

3.3 测试用例生成质量对比

为了进一步展示多智能体框架在软件测试方面相较于单独使用大型模型的明显优势，在图4中对比了有无需求分析支持时，多智能体系统生成的测试用例。结果表明，在集成需求分析的环境中，测试工程师智能体能够生成更详尽、更具针对性的测试用例。此实验不仅证实了多智能体

自动测试流程的有效性，而且也突出了其在提升测试用例的质量和相关性方面的显著优势。

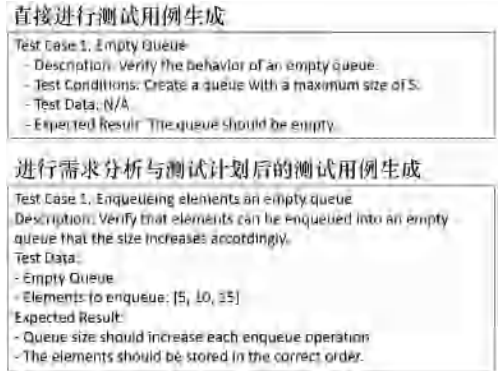


图4 测试用例生成质量对比

4 结束语

本研究提出了一种面向用例生成与代码优化的多智能体软件测试框架，旨在提升软件测试过程中的自动化水平及测试用例的质量。通过整合多智能体系统的协作能力和大语言模型（LLMs）的深度学习优势，本框架在多个实际软件项目中有效地展示了其对复杂代码逻辑的高效理解与高质量测试用例的生成能力。实验结果显示，相较于传统软件测试方法和单独使用大语言模型策略，本框架在代码分支覆盖和缺陷修复方面表现出明显优势，特别是在集成需求分析的环境中，能够生成更为详尽和精确的测试用例。

尽管展示了多项优点，本框架仍有一些不容忽视的局限性。首先，多智能体系统的实施和维护相比单一模型系统更为复杂，可能导致更高的时间成本。其次，由于技术限制，特别是在基于大语言模型的智能体使用时，处理长输入可能导致信息丢失，这可能影响测试的全面性。此外，部署和运维大语言模型需要显著的计算资

源,这可能带来较高的经济成本。

针对未来的研究,我们将致力于解决这些局限性,并进一步优化多智能体软件测试框架的性能和可用性。一方面,计划探索新的算法和技术以减少在处理大规模和复杂输入时多智能体之间的信息丢失。另一方面,研究将寻求更经济高效的模型部署策略,以降低大型模型的实施成本。同时,扩展多智能体框架以适应更多种类的软件测试环境和需求,将是未来工作的一个重点,以确保在各种实际应用场景中都能达到最优的测试效果。

参考文献

- 1 MYERS G J, SANDLER C, BADGETT T. The art of software testing [M]. John Wiley & Sons, 2011.
- 2 HARMAN M, MCMINN P. A theoretical and empirical study of search - based testing: Local, global, and hybrid search [J]. IEEE Transactions on Software Engineering, 2009, 36 (2): 226-247.
- 3 XIAO X, LI S, XIE T, et al. Characteristic studies of loop problems for structural test generation via symbolic execution [C] //2013 28th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE, 2013: 246-256.
- 4 PACHECO C, LAHIRI S K, ERNST M D, et al. Feedback-directed random test generation [C] // 29th International Conference on Software Engineering (ICSE'07). IEEE, 2007: 75-84.
- 5 YUAN Z, LOU Y, LIU M, et al. No more manual tests? evaluating and improving chatgpt for unit test generation [J]. arXiv preprint arXiv: 2305. 04207, 2023.
- 6 LIU Z, CHEN C, WANG J, et al. Makellm a testing expert: Bringing human-like interaction to mobile gui testing via functionality-aware decisions [C] //Proceedings of the IEEE/ACM 46th International Conference on Software Engineering. 2024: 1-13.
- 7 张洪广, 杨林, 杨雄军, 等. 大模型驱动的智能辅助决策原理与典型应用 [J/OL]. 指挥与控制学报, 1-8 [2024-06-30]. <http://kns.cnki.net/kcms/detail/14.1379.TP.20240318.1241.002.html>.
- 8 LIU R, YANG R, JIA C, et al. Training socially aligned language models in simulated human society [J]. arXiv preprint arXiv: 2305. 16960, 2023.
- 9 PARK J S, O' BRIEN J, CAI C J, et al. Generative agents: Interactive simulacra of human behavior [C] //Proceedings of the 36th annual acm symposium on user interface software and technology. 2023: 1-22.
- 10 HONG S, ZHENG X, CHEN J, et al. Metagpt: Meta programming for multi - agent collaborative framework [J]. arXiv preprint arXiv: 2308. 00352, 2023.
- 11 LUKASCZYK S, KROIB F, FRASER G. An empirical study of automated unit test generation for Python [J]. Empirical Software Engineering, 2023, 28 (2): 36.
- 12 WIDYASARI R, SIM S Q, LOK C, et al. Bugsinpy: a database of existing bugs in python programs to enable controlled testing and debugging studies [C] //Proceedings of the 28th ACM joint meeting on european software engineering conference and symposium on the foundations of software engineering. 2020: 1556-1560.

融合检索增强和思维链提示的大模型 关系抽取方法

刘琦¹ 张长亮² 杨雨婷¹ 方志^{1*} 郑一凡¹

摘要 关系抽取任务旨在从非结构化自然语言文本中识别并提取实体之间的关系，在军事领域，关系抽取是构建军事知识图谱的核心前置步骤和关键环节。然而，传统关系抽取模型由于参数量受限，缺少对复杂文本的上下文理解能力和知识泛化能力，导致抽取准确率难以满足现实要求。针对上述挑战，提出了一种基于大模型的军事领域关系抽取方法，首先通过思维链补全构建示例库，然后基于语义相似度检索召回相关示例并构造提示文本，利用大模型的少样本学习能力抽取句中实体及关系类型。实验证明，该方法取得了当前最优的表现，且在少样本条件下能实现关系的准确抽取，具有很强的泛化性。

关键词 信息抽取，关系抽取，军事领域，大模型，少样本学习

A Large Language Model for Relation Extraction Based on Retrieval Augmented Generation and Chain-of-Thought Prompting

LIU Qi¹ ZHANG Chang-Liang² YANG Yu-Ting¹ FANG Zhi^{1*} ZHENG Yi-Fan¹

Abstract The task of relation extraction aims to identify and extract relationships between entities from unstructured natural language text. In the military domain, relation extraction is a core preliminary step and a critical aspect of constructing a military knowledge graph. However, traditional relation extraction models are limited by the number of parameters, and they lack the ability to understand the context of complex texts and generalize knowledge, resulting in extraction accuracy that falls short of practical requirements. To address these challenges, we propose a relation extraction method based on large language models specifically for the military domain. This method first constructs an example library through chain-of-thought completion, then retrieves relevant examples based on semantic similarity and constructs prompt texts. By leveraging the few-shot learning capabilities of large language models, this method extracts entities and relationship types from sentences. Experiments demonstrate that this method achieves state-of-the-art performance and can accurately extract relationships under few-shot conditions, exhibiting strong generalization capabilities.

Key words information extraction, relation extraction, military domain, large language models, few-shot learning

* 通讯作者

1. 北京计算机技术及应用研究所 2. 中国人民解放军 93160 部队

1. Beijing Institute of Computer Technology and Application 2. Unit 93160 of the PLA

0 引言

关系抽取 (Relation Extraction, RE) 是信息抽取 (Information Extraction, IE) 领域的一项重要子任务, 它基于文本事实知识, 从非结构化的自然语言文本中抽取实体, 并识别实体之间关系类型。关系抽取对于理解文本内容、构建知识图谱以及支持如问答系统、推荐系统等各种智能应用具有重要意义。特别是在军事领域, 关系抽取能够从文本数据中自动识别实体及其相互关系, 为构建知识图谱提供数据支持, 从而帮助指挥员更准确地理解战场动态和敌方意图, 在军事情报分析中发挥着关键作用^[1]。

传统关系抽取算法多采用基于深度学习的方法, 通常包括两种研究思路: 有监督学习和远程监督学习。有监督学习方法依赖于大量标注数据, 通过为模型提供成对的输入和输出示例, 训练模型以识别和提取文本中的关系。例如, Zeng 等提出了基于卷积神经网络 (Convolutional Neural Network, CNN) 的关系分类模型, 通过提取文本的局部特征实现了对关系的准确识别^[2]。然而, 在军事领域, 获取大量标注数据往往是困难的, 标注成本高昂且时间耗费巨大。远程监督学习方法试图通过将未标注的数据自动标注来减少对人工标注的依赖。Mintz 等提出了利用知识库中的已知关系对未标注数据进行自动标注的方法, 这种方法通过关联已知的实体对来推断它们在文本中的关系^[3]。然而, 远程监督学习方法存在固有的噪声问题, 由于自动标注过程可能引入错误的标注, 导致模型的训练效果受到影响。尽管基于深度学习的方法是当下的主流算法, 但在军事领域中, 文本数据通常包含大量专业术语和领域知识, 对模型上下文理解能力有更高的要求。此外, 军事领域

的标注数据往往较为稀缺, 传统模型在少样本和零样本情况下表现不佳, 无法有效泛化到未见过的实例。

近年来, 大模型 (Large Language Models, LLMs) 技术的发展为关系抽取带来了新的机遇与挑战。大模型, 如 GPT^[4]、ChatGLM^[5]、Qwen^[6] 等, 以其强大的上下文理解和任务泛化能力, 为关系抽取任务提供了新的视角。相较于传统深度模型, 大模型主要优势在于其在预训练阶段通过海量数据学习得到的丰富文本知识。这种能力使得大模型在处理关系抽取任务时, 能够更加深入地理解文本中的语义和语法结构, 从而在分析长文本和复杂关系类型时也能展现出较好性能。大模型的另一个显著优势体现在任务泛化上, 由于模型在预训练阶段学习了足够的文本知识和任务形式, 使得大模型具备出色的上下文学习能力, 在提供少量示例或几乎不提供示例的条件下即可准确理解当前任务, 使得大模型在关系抽取任务中能够更好地利用不同案例之间的知识迁移, 提高模型的泛化性和适应性。

因此, 针对上述问题, 本文提出了一种基于大模型的军事领域关系抽取方法。方法整体采用检索增强框架, 首先利用公开搜集的军事语料构建示例样本库, 其次根据当前任务输入在所构建向量库中检索恰当的提示示例, 最后构造思维链提示完成关系抽取任务。实验结果表明, 本文方法取得了当下最优的效果, 且在少样本条件下依然取得了较好的性能, 验证了本方法的有效性。

1 相关工作

1.1 基于深度学习的关系抽取

基于深度学习的关系抽取模型通过自

动学习数据中的复杂特征，减少了对人工特征工程的依赖，从而在一定程度上避免了特征提取误差对关系抽取效果的负面影响。深度学习模型能够捕捉到更深层次的语义信息，为关系抽取任务提供了更为强大的表示能力。研究者们开发了两种主要的监督学习方法：有监督学习和远程监督学习。有监督学习策略通常依赖于精心设计的神经网络模型，如递归神经网络 (Recurrent Neural Network, RNN)、卷积神经网络 (Convolutional Neural Network, CNN)。RNN 因其能够处理任意长度的序列信息而受到青睐，Socher 等利用 RNN 解决了短语构成意义的捕捉问题^[7]。CNN 以其结构简洁和训练效率高的优势，被用于提取词和句子层次的特征，有效缓解了特征提取误差的传播问题。Zeng 等提出的 PCNN 模型进一步优化了 CNN 在关系抽取任务上的表现^[8]。远程监督学习通过利用公开的知识图谱和文本资源，自动生成大量的标注数据，其自动化程度较高，为大规模关系抽取提供了可能。然而这种方法容易受到噪声数据的影响，因此，Lin 等通过引入自注意力机制，增强了模型对错误标注的鲁棒性^[9]。

1.2 基于大模型的关系抽取

研究者们已经提出了多种方法来利用大模型进行关系抽取。一些方法通过在模型的预训练阶段引入领域特定的数据进行微调，以提高模型在特定关系抽取任务上的性能。其他方法则利用模型的零样本学习能力，通过精心设计的提示 (Prompts) 来指导模型完成关系抽取，无须额外的训练数据。为了解决大模型在关系抽取任务上的性能问题，研究者提出了 QA4RE 框架，通过将关系抽取任务与问答任务对齐来增强大模型的性能^[10]。GPT-RE 通过整

合任务感知表示并丰富演示中的推理逻辑，提高了实体与关系之间低关联度的识别能力^[11]。为了应对预定义关系类型众多且大模型缺乏控制的问题，Li 等提出将 LLM 与自然语言推理模块相结合以生成关系三元组，从而增强文档级关系抽取数据集的表现^[12]。最新研究进展表明，通过结合大模型的生成能力和结构化输出的约束，可以有效提高关系抽取的准确性和效率。例如，一些研究通过将关系抽取任务转化为问答任务，利用大模型在问答领域的强大能力来提升关系抽取的性能。此外，还有研究通过构建统一的信息抽取框架，使得大模型能够同时处理多个子任务，包括命名实体识别、关系分类和事件抽取等^[13-14]。

2 基于大模型的关系抽取方法

本文方法的整体框架采用检索增强 (Retrieval Augmented Generation, RAG) 技术实现，其架构如图 1 所示。

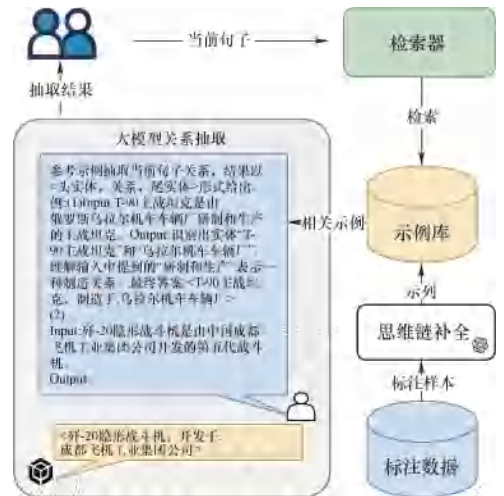


图 1 方法框架

本文方法共分三个主要步骤。首先，基于原有数据标注，利用大模型生成补全

推理路径,从而构建关系抽取示例库;其次,使用语义相似度检索召回与当前输入相关性最高的一组示例,加入提示模板;最后,结合选取示例构造思维链提示,利用大模型上下文学习能力抽取当前样本关系。

2.1 融合推理路径的示例库构建

本文所构造示例旨在为大模型完成关系抽取任务提供参考依据,示例质量对抽取效果有直接影响。因此,在构建示例库时,采用了思维链(Chain of Thought, CoT)的思想,通过在示例中加入分步推理的步骤结果及其对应的证据线索,以帮助大模型理解每个示例的推理逻辑,从而为大模型提供更优质的示例集。

在关系抽取任务中,句子中可能存在多种实体和多组关系,准确识别句子中的实体及其类型是正确判别其关系类型的基础。本文将关系抽取任务划分为两步,命名实体识别和关系标签预测。首先,从有标注数据中选定一个示例,给出其中包含的一组命名实体。随后,基于句子和实体生成一个查询。例如:“在‘2011年1月6日,中国海监15船正式入列中国海监船舶序列,并列入中国海监北海总队建制’,包含国家类实体为‘中国’,装备类实体为‘海监15’的推理依据是什么”,再使用大模型生成得到支持这一判断的事实依据和推理路径。例如:“在这句话中,‘中国海监’指的是中国的一个海事监督机构,‘15’是该机构下的一个具体船只的编号或名称。‘船’是装备类实体,而‘中国’是国家类实体。‘正式入列’表明这艘船已经成为该机构正式的一部分,而‘中国海监北海总队建制’进一步说明了这艘船所属的具体组织单位”,用以解释识别出的实体对。

随后的关系标签预测与第一步相类似。给定句子和实体对,生成一个查询提示,如“‘2011年1月6日,中国海监15船正式入列中国海监船舶序列,并列入中国海监北海总队建制’。句中,‘海监15’和‘中国’之间的关系为‘产国’的证据是什么”。基于此提示,使用大模型生成句子中实体对之间关系的推理证据,如“句子明确指出‘海监15’2011年1月6日‘列入中国海监北海总队建制’。这是一种直接描述,明确表明了该舰的产国是中国”,用以解释实体对之间的关系标签。

将以上两步产生的过程性推理线索统一整理,并与原始的句子和三元组一同作为关系实例,存储至示例库中。通过这种系统化的示例库构建方法,明确了实体对和关系类型,为模型提供清晰而详尽的推理路径,增强了其在执行关系抽取任务时的上下文理解能力和逻辑一致性。

2.2 基于语义相似度的示例检索

考虑到句子嵌入和关系抽取任务之间的差异,仅仅使用原始句子作为上下文可能不足以作为有用的检索索引。为了增强大模型对关系抽取任务中实体对的感知,在句子嵌入中增加了实体对的信息。即在句子上下文中显式地增加实体对的描述信息,如“‘海监15’和‘中国’之间的关系类型是‘产国’”。该方法在检索过程中既保留了句子的语义意义,也保留了以实体对为中心的信息。

使用了Sentence-BERT对目标句子和示例库中的句子进行语义建模。如图2所示,Sentence-BERT是一种基于BERT的句子嵌入模型,它能够将句子转化为固定长度的向量表示。这个向量表示捕捉了句子的语义信息,使得不同句子在向量空间

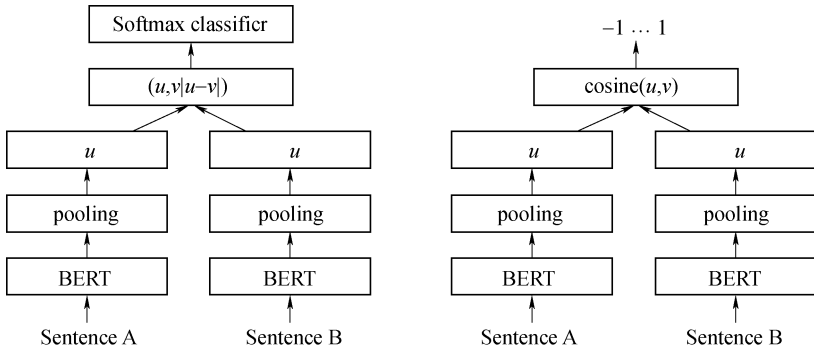


图2 Sentence-BERT 模型架构

中的位置反映了它们的语义相似性。通过这种方式，每个句子都被转化为一个高维向量。

使用最大边缘相关性 (Maximal Marginal Relevance, MMR) 作为演示示例选择的标准。MMR 是一种结合多种标准来优化句子的相似度计算方法。使用 MMR 的目的是平衡句子与查询的相似度并补充句子的多样性。其公式为：

$$\text{MMR}(D_i) = \lambda \times \text{Sim}_1(D_i, Q) - (1 - \lambda) \times \max_{D_j \in S} \text{Sim}_2(D_i, D_j) \quad (1)$$

式中， $\text{Sim}_1(D_i, Q)$ 为候选示例 D_i 和目标句子 Q 之间的相似度； $\text{Sim}_2(D_i, D_j)$ 为候选示例 D_i 与已选择集合 S 中句子 D_j 的相似度； λ 为平衡参数，用于调节相似度和多样性之间的权重。MMR 通过减少冗余，提高了所选句子的多样性和信息覆盖度。

计算目标句子与候选示例库中的所有句子的 MMR 得分，并从中选择得分最高的示例作为后一步提示构建中的演示示例。同时，在实验过程中采用 Langchain 中的示例选择器来执行示例的选择步骤，以及 FAISS 作为向量嵌入数据库以提升向量检索效率。

2.3 提示构造与关系抽取

为了提高大模型上下文学习的准确

性，将半格式化的结构约束纳入提示中，随后输入给大模型。这些结构约束通过明确关系类型、实体示例和上下文语境等信息，引导模型更准确地理解和生成所需的关系信息。每个提示都由以下组件组成：

Instruction I: 提供了关系抽取的任务描述和预定义关系类的简明概述。大模型应该明确地输出属于预定义关系类中的关系标签。

Demonstrations D: 利用前一小节中提到的最大边缘相关性算法来获取关系实例作为演示示例。

Task X: 使用与 Demonstration 类似的结构输入需要执行关系抽取的句子 x 。大模型应该输出其包含的关系类型 y 。

当给予大模型多个示例时，上下文学习意味着大模型需要从其中推断出一个共享的提示概念来进行预测。因此，上下文学习可以被看作大模型隐式地执行贝叶斯推理，如下式所述：

$$p(y) = \int_d p(y | d, p) p(d | p) d(d) \quad (2)$$

式中， $p(y)$ 为目标关系类型输出的概率分布； $p(y | d, p)$ 为在给定演示示例 d 和提示 p 下目标输出的条件概率； $p(d | p)$ 为在提示 p 下演示示例 d 的概率分布。Instruction I 和 Task X 共同组成了提示 p 。

给定提示 p 和多个示例，大模型通过“选择”示例来执行边缘化学习，并得到最终关系标签答案。

3 实验及分析

3.1 数据集与评价指标

为验证方法效果，本文通过互联网爬取公开军事装备语料和人工标注关系三元组的方式构建实验数据集。经筛选过滤，最终得到的数据集包含 1677 条样本，10 种关系类型，具体统计信息如表 1 所示。

表 1 数据集统计信息

关系类型	样本数量	样本平均长度
(装备, 产国, 国家)	180	57.71
(装备, 属于, 类型)	123	66.23
(装备, 研发时间, 时间)	197	57.21
(装备, 服役时间, 时间)	112	47.56
(装备, 退役时间, 时间)	164	67.12
(装备, 制造于, 地点)	144	43.50
(装备, 前型, 前型装备)	196	52.62
(装备, 口径, 武器口径)	228	62.19
(装备, 速度, 飞行速度)	171	48.72
(装备, 挂载, 武器)	162	49.17

本实验采用准确率 (Precision)、召回率 (Recall) 和 F1 值作为模型效果的评价指标，如果关系被正确抽取，则表示为 TP ，否则表示为 FN 。具体指标计算公式如下：

$$P = \frac{TP}{TP + FP} \quad (3)$$

$$R = \frac{TP}{TP + FN} \quad (4)$$

$$F1 = \frac{2 \cdot P \cdot R}{P + R} \quad (5)$$

3.2 实验参数设置

本实验在 Ubuntu 18.04 操作系统上进行，硬件配置包括 4 块 24G 显存的 NVIDIA 3090 显卡，软件环境采用 Python 3.8。实验框架结合 LangChain 库进行实现，为保证检索效率，向量检索部分采用 FAISS (Facebook AI Similarity Search) 库，基础大模型选用 Baichuan-7B，提示示例数量设置为 3 进行测试。

此外，选取了三个基线模型 SuRE、ReDMP、UIE 进行对比实验，以全面衡量所提方法的有效性。

3.3 实验结果与分析

3.3.1 主实验结果

本文方法与其他基线模型的效果对比可参见表 2，其中最优指标以黑体标注。

表 2 本文方法与基线模型对比

方法	Precision	Recall	F1
SuRE	90.77	89.52	89.89
ReDMP	87.67	83.81	84.60
UIE	90.89	90.18	90.54
Ours	92.81	90.62	91.63

从整体指标上来看，本文方法取得了最优的性能表现，相比于其他基线模型分别在 Precision、Recall 和 F1 指标上取得了 1.92% ~ 5.14%、0.44% ~ 6.81% 和 1.09% ~ 7.03% 的显著提升，验证了本文方法的有效性。进一步观察发现，基于小模型的 SuRE 和 ReDMP 性能指标相对弱于基于大模型的 UIE 和本文方法，表明大模型在处理军事领域关系抽取任务上具备一定优势，即便不经过训练，也能凭借其上下文理解能力和迁移泛化能力，理解当前的任务要求和输出格式，在数据高度敏感和标注数据稀缺的军事领域，类似 SuRE、

ReDMP 等有监督方法存在较大局限性, 无须训练即可达到预期性能指标的方法更具可用性。

3.3.2 分析少样本设置的影响

为了评估本文方法在零样本和少样本场景下的表现, 将示例数量分别设置为 0、1、3 进行测试。具体来说, 零样本测

试 (示例数量为 0) 用于检验模型在没有任何示例情况下的性能; 单样本测试 (示例数量为 1) 用于评估模型在只有单个示例时的表现, 少样本测试 (示例数量为 3) 用于评估模型在有极少量示例时的表现, 即为主实验设置。实验结果如图 3 所示。

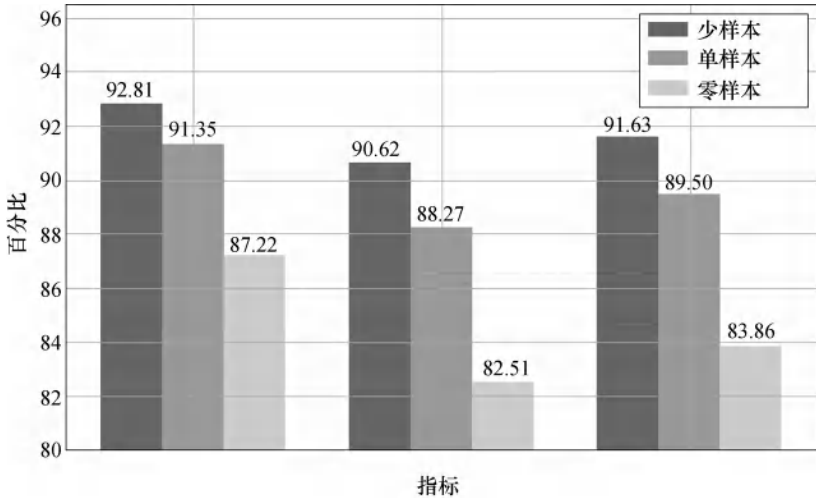


图 3 零样本和少样本场景下模型表现对比

观察图中结果, 本文方法在少样本设置 (Three-shot) 下表现最优, 单样本设置 (One-shot) 下次之, 零样本设置 (Zero-shot) 下表现最差。进一步分析指标差距, 少样本和单样本条件下方法所取得的指标较为接近, 基本上处于同一水平, 但在零样本设置下, 指标下滑明显。证明了在提示中加入示例的关键性, 大模型能够通过上下文学习从给定的示例中获取指导信息, 从而在抽取格式和内容上更好地遵循人类指令, 获取更高的抽取准确度。

3.3.3 分析思维链的影响

本文在构建示例时融入了思维链的思想, 即通过在示例中加入分步推理的步骤结果及其对应的证据线索, 帮助大模型理解每个示例的推理逻辑, 从而为大模型提

供更优质的示例集。为了进一步探究思维链设计的有效性, 本文消融了思维链部分, 并与主实验效果进行对比。实验结果如表 3 所示。

表 3 思维链消融实验

方法	Precision	Recall	F1
Ours	92.81	90.62	91.63
w/o CoT	90.37	87.64	88.79

从表 3 的实验结果可以明显看出, 思维链在提升模型性能方面起到了显著作用。去除思维链部分 (w/o CoT) 后, 模型在 Precision、Recall 和 F1 指标上分别下降了 2.44%、2.98% 和 2.84%。这种下降表明, 思维链不仅有助于提高模型的精确度和召回率, 而且对整体性能 (F1 分数) 的提升也同样重要。思维链在提高模型性

能方面的效果，主要体现在分步推理、增强理解和证据线索这几个方面。通过将复杂的推理过程分解为多个步骤，模型能够逐步接近最终答案，每一步都有明确的证据支持，从而减少了推理中的偏差和错误。思维链为模型提供了清晰的推理路径，使其不仅仅依赖于输入输出的映射关系，而是通过中间推理步骤更深刻地理解问题。这种方式提高了模型的鲁棒性和泛化能力。在每个推理步骤中引入相应的证据线索，使得模型的决策过程更加透明和可解释。这不仅有助于提高模型性能，还能为后续的模式优化和调整提供有力支持。

4 结束语

本文面向军事领域关系抽取需求，分析了现有方法的不足，提出了一种基于大模型的军事领域关系抽取算法。在相关语料上的实验结果表明，本文方法取得了当前最优的表现，且本文方法无须训练模型，在少样本条件下性能出色，具备高度的泛化性和适用性。未来，针对大模型推理效率问题，将尝试模型量化、模型蒸馏等轻量化算法，研究更低成本更高效率的抽取策略。

参考文献

- 1 商容轩, 张斌, 马海群, 等. 国外开源情报领域研究现状、研究热点及趋势分析 [J]. 现代情报, 2022, 42 (1): 5-13, 86.
- 2 ZENG D, LIU K, LAI S, et al. Relation classification via convolutional deep neural network [C] //Proceedings of COLING 2014, the 25th international conference on computational linguistics; technical papers. 2014: 2335-2344.
- 3 MINTZ M, BILLS S, SNOW R, et al. Distant supervision for relation extraction without labeled data [C] //Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP. 2009: 1003-1011.
- 4 OUYANG L, WU J, JIANG X, et al. Training language models to follow instructions with human feedback [J]. Advances in neural information processing systems, 2022, 35: 27730-27744.
- 5 DU Z, QIAN Y, LIU X, et al. GLM: General Language Model Pretraining with Autoregressive Blank Infilling [C] //Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 2022: 320-335.
- 6 BAI J, BAI S, CHU Y, et al. Qwen technical report [J]. arXiv preprint arXiv: 2309.16609, 2023.
- 7 SOCHER R, CHEN D, MANNING C D, et al. Reasoning with neural tensor networks for knowledge base completion [J]. Advances in neural information processing systems, 2013, 26.
- 8 ZENG D, LIU K, CHEN Y, et al. Distant supervision for relation extraction via piecewise convolutional neural networks [C] //Proceedings of the 2015 conference on empirical methods in natural language processing. 2015: 1753-1762.
- 9 LIN Y, LIU Z, SUN M, et al. Learning entity and relation embeddings for knowledge graph completion [C] //Proceedings of the AAAI conference on artificial intelligence. 2015, 29 (1).
- 10 ZHANG K, GUTIÉRREZ B J, SU Y. Aligning Instruction Tasks Unlocks Large Language Models as Zero-Shot Relation Extractors [C] //Findings of the Association for Computational Linguistics: ACL 2023. 2023: 794-812.
- 11 WAN Z, CHENG F, MAO Z, et al. GPT-RE: In-context Learning for Relation Extraction using Large Language Models [C] //Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing. 2023: 3534-3547.
- 12 LI J, JIA Z, ZHENG Z. Semi-automatic Data Enhancement for Document-Level Relation Extraction with Distant Supervision from Large Language

- Models [C] //Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing. 2023: 5495–5505.
- 13 LU Y, LIU Q, DAI D, et al. Unified Structure Generation for Universal Information Extraction [C] //Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 2022: 5755–5772.
- 14 PAOLINI G, ATHIWARATKUN B, KRONE J, et al. Structured prediction as translation between augmented natural languages [C] //ICLR 2021 9th International Conference on Learning Representations. International Conference on Learning Representations, ICLR, 2021: 1–26.

生成式任务网：基于大模型的任务规划与执行新范式

黄雪芹¹ 张 胜¹ 朱先强¹ 张千桢¹ 朱 承¹

摘要 在生成式人工智能的浪潮中，大语言模型（Large Language Model, LLM，简称大模型），以其卓越的通用智能特性，成为推动通用人工智能技术进步的关键力量。目前，以 GPT4、GLM4、Llama3 等为代表的一系列大模型已经在各个行业领域中发挥着重要作用，在帮助拓展人类或机器的能力边界、提升生产力等方面做出了巨大贡献。在此背景下，无人系统的智能任务规划技术也将迎来新的变革。

无人系统在现代军事和众多民用领域已经被广泛应用，但距离实现真正智能化和自动化的目标仍有不小差距。通常一个无人系统仅能处理某一个具体的领域任务，因为其智能任务规划模块在设计时为达到专业领域要求，做出了许多局限和假设，导致其规划的泛化性和可迁移性很弱。大模型的出现为无人系统的智能任务规划技术发展提供了新的方向和可能性。大模型具备强大的语言理解、逻辑推理、代码生成和知识整合能力，同时其涌现出的通用智能特性使它能处理广泛领域的复杂信息，可以针对复杂问题生成适宜的规划策略和解决方案。此外，大模型的多轮对话能力可以实现便捷的人机协同，为无人系统提供高效的信息共享和任务协调机制，增强无人系统的灵活性。

传统的智能任务规划模型主要有以运筹优化为主的数学解析模型、以领域知识设计任务分解方法为主的层次任务网模型、以因果概率关系分析为主的概率网络模型等。这些传统的规划模型有一个共性缺陷，即开发过程中需要专家耗费大量精力和时间参与，完成后的模型专用性强，适应性、可迁移性弱，一般不具备泛化性，当面临新的情况和任务时，又需要专家重新建模。其中层次任务网通过引入领域知识、模拟专家的思维方式，设计任务树并结合任务规范化模板实现了任务的树状层级分解，其运作流程模式与当前基于大模型的 AI Agent 流程十分契合。不过传统的层次任务网是受限于少量人类专家和工程师构建，只能根据既定规则进行任务生成，导致其自动化程度不高、迁移能力弱、泛化性不强。引入大模型后解决了专业知识限制问题，可以有效增强子任务生成能力、场景泛化性能和可迁移性。另外，传统的智能规划方法大多仅针对任务规划展开研究，对规划前的任务发现和规划后的任务执行是断开的过程，导致任务规划的时效性和可用性存疑，尤其是在针对时敏目标执行任务时，无法实现无人系统从任务自主发现到智能规划再到自动执行的全过程连通，将导致目标丢失、任务规划失效等问题。而将大模型接入无人系统的规划模块使其有潜力同时完成任务的自主发现、任务的智能规划并调度无人系统中的资源协同完成各项子任务，实现任务从自主发现到自动执行的快速闭环。

思维链（Chain of Thought, CoT）、思维树（Tree of Thought, ToT）等作为大模型提示工程的关键技术，揭示了大模型的问答能力可以通过更精确的问题描述来提升。因此，让大模型对复杂指令和情境数据进行逐步的理解和分析，通常能够产生更佳的结果。检索增强生成（Retrieval Augmented Generation, RAG）是利用外部知识来提升大模型问答性能并减少幻觉的有效方法，充分的外部数据和知识正是进行合理任务规划与任务执行的必要基础条件。

1. 国防科技大学信息系统工程全国重点实验室

1. National Key Laboratory of Information Systems Engineering, National University of Defense Technology

结合层次任务网思想和大模型的 CoT、ToT、RAG 等优势，本文提出了生成式任务网（Generative Task Network, GTN）方法及其技术框架。生成式任务网是一种基于大模型及其相关技术的新型智能任务规划与执行范式，对该范式的内涵和机理进行深入研究有助于推进无人系统的智能化和自动化发展，对于构建敏捷杀伤网等应用也具有重要参考意义。

关键词 无人系统，大模型，任务规划，任务执行，生成式任务网

Generative Task Network: A New Paradigm for Task Planning and Execution Based on Large Models

HUANG Xue-Qin¹ ZHANG Sheng¹ ZHU Xian-Qiang¹ ZHANG Qian-Zhen¹ ZHU Cheng¹

Abstract In the wave of generative artificial intelligence, large language models (LLMs), referred to as large models, have become a key force in advancing general artificial intelligence technology due to their exceptional general intelligence capabilities. Currently, a series of large models, represented by GPT-4, GLM4, Llama3, and others, are playing an important role across various industries. They have made significant contributions to extending the boundaries of human or machine capabilities and enhancing productivity. Against this backdrop, intelligent task planning technology for unmanned systems is also set to undergo new transformations.

Unmanned systems have been widely applied in modern military and numerous civilian fields, yet there is still a significant gap in achieving true intelligence and automation. Typically, an unmanned system can only handle tasks in a specific domain, as its intelligent task planning module is designed with many limitations and assumptions to meet professional field requirements, resulting in weak generalization and transferability of its planning. The emergence of large models provides new directions and possibilities for the development of intelligent task planning technology in unmanned systems. Large models possess strong language understanding, logical reasoning, code generation, and knowledge integration capabilities. Their emergent general intelligence characteristics enable them to handle complex information across a wide range of fields and generate appropriate planning strategies and solutions for complex problems. Furthermore, the multi-turn dialogue capability of large models facilitates convenient human-machine collaboration, providing efficient information sharing and task coordination mechanisms for unmanned systems, thereby enhancing their flexibility.

Traditional intelligent task planning models mainly include mathematical analytical models focusing on operations optimization, hierarchical task network models designed for task decomposition based on domain knowledge, and probabilistic network models centered on causal probability analysis. These traditional planning models share a common defect: they require experts to invest a significant amount of time and effort during development, and the resulting models are highly specialized, with weak adaptability and transferability, generally lacking generalization. When faced with new situations and tasks, experts need to rebuild the models. The hierarchical task network achieves tree-like hierarchical task decomposition by introducing domain knowledge and simulating expert thinking patterns, and its operational process aligns well with the AI Agent process based on large models. However, traditional hierarchical task networks are limited by being constructed by a small number of human experts and engineers, and can only generate tasks according to established rules, resulting in low automation, weak transferability, and poor generalization. The introduction of large models solves the limitation of professional knowledge, effectively enhancing subtask generation capabilities, scenario generalization performance, and transferability. Moreover, traditional intelligent planning methods mostly focus only on task planning, resulting in a disconnection

between task discovery before planning and task execution after planning, raising doubts about the timeliness and usability of task planning. This is especially problematic when executing tasks for time-sensitive targets, as it fails to achieve a complete process connection from autonomous task discovery to intelligent planning to automatic execution in unmanned systems, leading to target loss and task planning failure. Integrating large models into the planning module of unmanned systems holds the potential to simultaneously accomplish autonomous task discovery, intelligent task planning, and resource coordination within unmanned systems to complete various subtasks, achieving a rapid closed-loop from autonomous discovery to automatic execution.

Chain of Thought (CoT) and Tree of Thought (ToT), as key technologies in large model prompt engineering, demonstrate that the question-and-answer capability of large models can be improved through more precise problem descriptions. Therefore, allowing large models to gradually understand and analyze complex instructions and contextual data often yields better results. Retrieval Augmented Generation (RAG) is an effective method to enhance the question-and-answer performance of large models and reduce hallucinations by utilizing external knowledge. Sufficient external data and knowledge are necessary foundational conditions for reasonable task planning and execution.

Combining the advantages of hierarchical task network (HTN) concepts with CoT, ToT, and RAG technologies of large models, this paper proposes the Generative Task Network (GTN) method and its technical framework. The Generative Task Network is a new intelligent task planning and execution paradigm based on large models and related technologies. In-depth research into the connotations and mechanisms of this paradigm will help promote the intelligent and automated development of unmanned systems and provide important reference value for constructing agile killing networks and other applications.

Key words unmanned systems, large language model, task planning, task execution, generative task network

视觉语言大模型在目标分析领域的应用

张明新¹ 陈亚洲¹

摘要 在现代军事领域，目标分析作为核心技术，直接关系到任务成败。传统图像处理和计算机视觉技术在单一任务上表现良好，但在复杂环境和多样化目标下存在瓶颈。随着人工智能技术的发展，视觉语言大模型在处理复杂信息和多维数据方面展现出独特优势。这类模型能够同时接收文本和图像输入，结合自然语言处理和计算机视觉技术，实现跨模态的信息融合与深度理解。文章旨在探讨视觉语言大模型在军用目标分析中的应用与前景，首先概述了视觉语言大模型的发展历程及其技术原理，其次分析其在军用目标分析中的具体应用场景和赋能角度，再次讨论了这些模型在军事目标分析中的优势和挑战，最后展望了视觉语言大模型在未来军事领域中的应用前景。文章为视觉语言大模型在军用目标分析中的应用提供了全面的思考框架，并为未来的研究和实践提供了指导和启示。

关键词 视觉语言，大模型，目标分析，优势挑战，前景

The Application of Large Vision-Language Models in the Field of Target Analysis

ZHANG Ming-Xin¹ CHEN Ya-Zhou¹

Abstract In modern military domains, target analysis is a core technology that directly impacts mission success. Traditional image processing and computer vision technologies perform well on singular tasks but face limitations in complex environments and with diverse targets. With the rapid development of artificial intelligence, Large Vision-Language Models (LVLMs) have shown unique advantages in handling complex information and multidimensional data. LVLMs can simultaneously receive text and image inputs, integrating natural language processing and computer vision techniques to achieve cross-modal information fusion and deep understanding. This paper explores the application and prospects of LVLMs in military target analysis. It begins with an overview of the development and technical principles of LVLMs, then analyzes their specific application scenarios and empowerment angles in military target analysis. Additionally, the paper discusses the advantages and challenges of these models in broader applications and forecasts the future prospects of LVLMs in military fields. Through this discussion, the paper provides a comprehensive framework for the application of LVLMs in military target analysis and offers guidance and insights for future research and practice.

Key words vision-Language, large language models, target analysis, advantage and challenge, prospect

1. 国防大学政治学院

1. National Defense University, School of Political Work

0 引言

在现代军事领域中，目标分析作为一种核心技术，扮演着至关重要的角色^[1]。无论是在战场态势感知、智能监控，还是在无人系统的自主导航和决策支持中，精准、快速的目标识别与分析都将直接关系到任务成败。传统的目标分析方法主要依赖于图像处理和计算机视觉技术，这些技术在单一任务处理上表现优异，但在面对复杂环境和多样化目标时，往往会遇到瓶颈^[2]。具体而言，现有技术在处理高维数据、实现场景迁移、满足实时性要求以及提升识别准确度方面存在较大困难，导致其在应对动态战场信息和多源异构数据时显得力不从心。此外，传统方法还依赖于大量人工标注数据，成本高且易受人为因素影响，难以适应快速变化的战场环境。

随着人工智能（AI）技术的迅猛发展，视觉语言大模型（Large Vision-Language Models, LVLMs）逐渐展现出在处理复杂信息和多维数据方面的独特优势^[3-5]。这类模型能够同时接收文本和图像为输入，并输出高质量的文本响应，极大地拓展了智能分析技术的应用范围。与传统单模态模型不同，LVLMs 通过结合自然语言处理（NLP）和计算机视觉（CV）技术，能够实现跨模态的信息融合与深度理解。代表性的视觉语言大模型，如GPT-4V^[6]和Gemini-Pro^[7]，不仅具有强大的语言理解和生成能力，还能高效解析图像信息，从而在复杂场景中提供精准的目标识别与分析。例如，GPT-4V 通过其大规模的预训练和微调，可以在较短时间内处理大量战场图像，并结合上下文提供全面的态势报告；Gemini-Pro 则通过其先进的多模态融合机制，实现了对多源、多模态数据的统

一处理和智能决策支持。

本文旨在探讨视觉语言大模型在军用目标分析中的应用与前景。首先概述视觉语言大模型的发展历程及其技术原理。其次分析其在军用目标分析中的具体应用场景和赋能角度。此外，本文还将讨论这些模型在更广泛应用中的优势和挑战。最后，展望视觉语言大模型在未来军事领域中的应用前景，探讨其可能带来的技术突破和社会影响。通过本文讨论，希望为视觉语言大模型在军用目标分析中的应用提供一个全面的思考框架，并为未来的研究和实践提供指导和启示。

1 视觉语言大模型概述

视觉语言大模型是一类能够同时接收视觉和文本信息，并进行跨模态联合推理的生成式 AI 模型。得益于其庞大的参数量和训练数据量，这类模型能够以微调、少样本提示（few-shot）和零样本提示（zero-shot）等低成本方式完成如视觉描述、视觉问答、跨模态检索、目标检测、目标定位、指代表达理解与生成等多模态下游任务。视觉语言大模型的发展分为三个阶段。

1.1 基于外部专家的 LVLMs

阶段一（2019—2021年）的 LVLMs 通常以 Transformer 的编码器为主干架构^[8-9]。文本嵌入通常由 BERT 中训练好的嵌入层得到，图像嵌入则由目标检测专家模型输出的区域特征及其位置信息组成。两种模态的嵌入序列通过自注意力或交叉注意力机制进行交互融合。该阶段的训练数据通常由多种视觉语言下游任务的基准数据集组成。数据形式较为单一，通常为图像文本对。相反，这一阶段的预训练任务则种类繁多，代表性任

务包括 Masked Image Modeling (MIM)、Masked Language Modeling (MLM)、Image Text Matching (ITM)、Word Region Alignment (WRA) 等。其中, MIM 基于不同的自监督信号又可分为多个种类。由于目标检测模型的存在, 这一阶段的视觉语言大模型具有推理开销大的共性短板。此外, 将区域特征作为视觉嵌入可能导致图像信息的损失, 并导致模型表现受到目标检测模型的性能约束, 如图 1 所示。

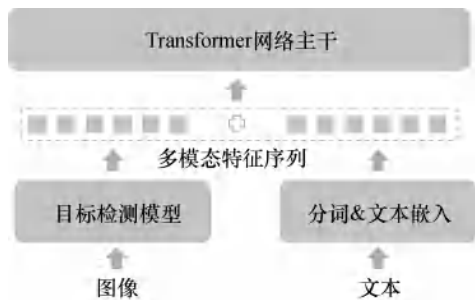


图 1 阶段一 LVLMs 架构图

1.2 端到端的 LVLMs

随着 Vision Transformer (ViT) 的问世, LVLMs 的发展进入了第二阶段 (2021—2022 年)^[10-11]。与阶段一相比, 此时的图像嵌入不再依赖于额外的目标检测模型,

而是对图像进行 patch 划分, 各 patch 经过一次线性映射后直接作为嵌入表征输入 Transformer 主干, 从而实现了端到端的设计。这一时期出现了一类以双编码器为架构的模型 (如 CLIP^[12] 和 ALIGN^[13]), 即一个编码器提取文本特征, 一个编码器提取图像特征, 虽然两个编码器在架构层面相互独立, 但通过对比学习能够将语义相近的图像和文本聚集在同一个表示空间的相近区域, 从而实现了跨模态高效检索以及零样本的开放域图像分类。这一阶段开始逐步出现具有互联网规模的弱标注训练数据集, 如样本量超过 4 亿的 WIT 数据集^[12] 和样本量超过 18 亿的 ALIGN 数据集^[13]。然而, 截至这一阶段, LVLMs 的建模目标仍属于表示学习, 其任务的执行方式也多以判别式为主。因此, 对于不同的下游任务, 需要为基础模型拼接不同的顶端层, 并在与任务相关的数据上做进一步微调训练。这种方式导致不同的任务需要保存不同的模型参数, 加重了存储负担。基于表示学习的模型通常不具备生成能力, 只能以分类的方式机械地完成如视觉问答和图像描述等开放式任务, 限制了其在实际环境中的应用价值, 如图 2 所示。

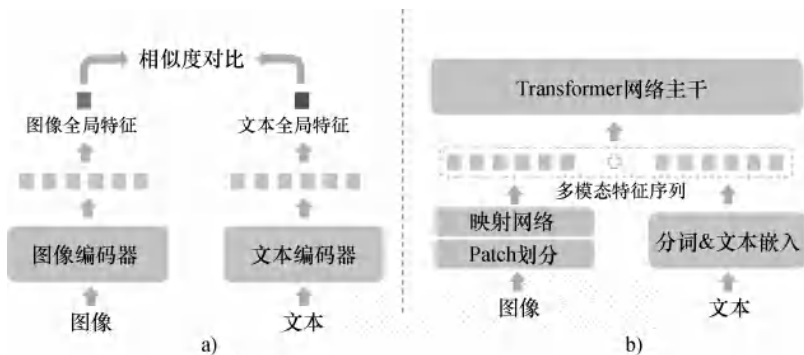


图 2 阶段二的两种 LVLMs 典型架构

a) 双编码器架构; b) 单编码器架构

1.3 基于 LLMs 的 LVLMs

从 2022 年开始，大语言模型（Large Language Models, LLMs）热度骤增，其所具备的涌现特性及强大的指令跟随能力，使其能够通过自然语言交互完成几乎所有类型的语言任务，而无须再对每一类下游任务进行微调。至此，LVLMs 的发展进入了第三阶段（2022 年至今），研究焦点全面转向如何让纯文本 LLMs 具备视觉模态的感知能力^[14-15]。

如图 3 所示，这一阶段的 LVLMs 通常由三部分组成：预训练视觉编码器、视觉语言适配器以及 LLM。视觉编码器用于从输入图像中提取关键的视觉特征；视觉语言适配器负责将这些视觉特征对齐到 LLM 的嵌入空间；最后，LLM 负责同时接收视觉特征和文本指令，通过多模态推理生成合理的文本响应。



图 3 阶段三的 LVLMs 架构图

在视觉编码器的选型上，大多数研究倾向于采用经过 CLIP（Contrastive Language-Image Pre-training，一种基于对比文本-图像对的预训练方法）预训练的 ViT 模型。一方面，ViT 模型生成的视觉特征本质上是序列化的，自然地适配了 LLM 对序列化输入格式的需求；另一方面，CLIP 采用的图像文本对比学习有助于确保视觉

特征的表示空间与 LLM 嵌入空间的一致性。

LLM 组件的选型则更为多样。早期工作偏好于使用 encoder-decoder 架构的 T5 模型^[16]，而近期研究则更倾向于使用 decoder-only 架构的 LLaMA 系列^[17]或经过指令微调的 LLaMA 变体，如 Vicuna 和 Alpaca。

视觉语言适配器的设计分为三类。第一类仅由一个线性层组成，其优势在于结构简单且参数量小，但非线性的缺席可能导致视觉特征和 LLM 嵌入空间的对齐不足。第二类则采用带有非线性激活函数的 MLP（Multilayer Perceptron Classifier，多层感知分类器）。这类 MLP 通常由两层组成，首先将视觉特征映射至低维空间，进行非线性激活后，其次将其映射到 LLM 的嵌入空间。相较于线性层，MLP 具有更强的对齐能力。第三类适配器采用融合了交叉注意力模块的 Transformer 编码器。其输入为固定数量的可学习查询向量，视觉特征通过交叉注意力模块与查询向量进行信息交互。这些查询向量在编码器中的最终表示将被视为对齐后的视觉特征传递给 LLM。这种设计具备两点优势：

(1) 可以通过设置可学习查询向量的个数来控制视觉特征的序列长度，从而减轻视觉特征对于 LLM 上下文窗口的占用，并提升模型的推理速度。

(2) 通过将文本指令在输入端和可学习向量一同输入编码器，可帮助其萃取出与当前任务更相关的视觉特征。

然而，这类适配器需要更多的参数和额外的预训练流程。由于这三种设计各有优劣，当前研究在适配器的选型上并未出现统一趋势。视觉特征注入 LLM 的方式也分为多种。在早期研究中，经对齐的视觉特征通常会通过 LLM 中集成的

交叉注意力模块进行整合。然而，这种方式在最近的工作中被逐渐抛弃，取而代之的是将视觉特征和文本嵌入拼接后同时在 LLM 的输入端注入。这种方式不仅可以减少模型的复杂度，更为模型处理不同类型的视觉信息提供了更强的灵活性。

现阶段 LVLMs 的训练方式均为文本生成，即最大化多模态训练数据中文本部分的对数似然。不同训练任务间的差异主要反映在训练数据的特定内容和呈现结构上。主流策略是将训练过程分为模态对齐和指令微调两个阶段。在模态对齐阶段，训练数据由大量的图像文本对组成，其中的文本部分通常是对图像内容的描述。通过将每个图像样本输入模型，并以最大化描述文本的似然值为目标来优化视觉语言适配器的参数，使得适配器学会如何将视觉特征有效对齐至 LLM 的嵌入空间。在指令微调阶段，训练数据式则由（图像，文本指令，文本响应）的三元组构成，目的是训练模型在多模态场景下的指令跟随能力。该阶段的训练数据按照指令类型不同，可分为传统视觉语言任务数据集和通用对话数据集。前者通常来自将传统视觉语言下游任务的数据集使用自然语言指令的格式进行范式统一，所涉及的任务种类包括视觉描述、视觉问答、视觉问题生成、目标检测、光学字符识别、指代表达理解和指代表达生成等。通用对话指令数据则通常由 GPT-4 等 AI 模型基于现有图像进行指令设计和响应生成，其指令类型更加丰富且响应风格更偏向自然交流。因此，这类数据能够进一步增强模型的指令理解能力，并将模型的响应和人类偏好相对齐。

2 视觉语言大模型在目标分析中的应用探讨

2.1 军用目标分析的任务分类

军用目标分析是现代军事行动中的重要组成部分，主要包括三个关键任务：目标检测、目标跟踪和目标识别。目标检测是从图像或视频中识别并定位出潜在目标的位置，无论是固定的地面目标还是移动的空中目标，检测技术能够在复杂背景下迅速发现潜在威胁。目标跟踪则是在视频序列中保持对目标的持续监控，应对目标在运动过程中可能发生的速度变化、遮挡和环境干扰，确保目标的持续可见性和位置更新。目标分析则是指对目标进行分析推断，比如区分目标的类型（如车辆、飞机或船只），或判断目标的具体型号和潜在威胁等级。通过这三类任务的相互配合，军用目标分析能够在战场环境中实现对目标的全面感知和精准分析，为军事行动提供有力支持。

视觉语言大模型在军用目标分析中的应用具有重要意义。这类模型通过结合视觉和语言信息，能够提升目标检测、目标跟踪和目标分析的精度和效率。例如，视觉语言大模型可以在复杂战场环境中更准确地识别和定位目标，提供连续且详尽的目标跟踪信息，以及生成详细的目标描述和分类。不仅增强了军队的态势感知能力，还提高了决策的准确性和反应速度，进而在战术和战略层面上提供显著优势。

2.1.1 军用目标检测

目标检测^[18]是指在复杂背景中自动识别并定位特定目标的过程。在军事领域，目标检测任务具有重要的战略和战术意义，常用于侦察、监视、威胁评估等方

面。现代军用目标检测系统通常融合多种传感器数据，如光学、红外和雷达，通过多源数据融合，可以在不同环境和条件下提高目标检测的鲁棒性和准确性。

军用目标检测在现代军事应用中起着至关重要的作用，其主要任务是在复杂的战场环境中，自动化地检测、识别和定位敌方目标。这些目标包括敌方的车辆、人员、无人机、导弹以及其他潜在威胁。军用目标检测系统需要在多变和苛刻的环境条件下，提供实时、精准和鲁棒的目标识别和定位能力。战场环境的复杂性主要体现在以下几个方面：背景复杂多变、目标种类多样、目标运动不规则、环境干扰因素多以及多目标同时出现等。

在实际战场中，目标检测的任务通常包括以下几个步骤：首先，通过传感器捕捉战场图像和视频数据；其次，利用先进的图像处理和分析技术，对捕捉到的数据进行处理，提取有用的特征信息；最后，利用检测算法识别并定位目标。这一过程中，系统需要处理大量的实时数据，且必须具备快速响应的能力，以应对战场上快速变化的情况。

现有的军用目标检测技术可以分为传统图像处理技术和现代深度学习技术两大类。传统图像处理技术依赖于手工设计的特征提取方法，如边缘检测、角点检测和颜色分析等。这些技术通常应用于低分辨率图像或特定环境下，具有计算量小和实现简单的优点，但其检测准确率和鲁棒性相对较低，难以应对复杂的战场环境。

传统的图像处理技术主要包括边缘检测、纹理分析和形状分析等方法。边缘检测通过检测图像中灰度变化显著的区域来识别目标边界，常用的方法有 Sobel 算子^[19]、Canny 算子^[20]等。纹理分析^[21]则通过分析图像中的纹理特征来检测目标，

常用的方法包括 Gabor 滤波器和局部二值模式 (LBP)。形状分析^[22]通过检测图像中的几何形状特征来识别目标，常用的方法有霍夫变换等。这些传统方法在简单场景中表现较好，但在复杂环境中容易受到背景干扰和目标变形的影响，导致检测精度下降。此外，这些方法对目标的特征提取依赖于手工设计，难以适应多变的战场环境和复杂的目标特征。

机器学习方法通过训练分类器（如支持向量机、决策树等）来识别目标。基于特征提取的机器学习方法在图像识别中取得了一定的成功，常用的特征包括尺度不变特征变换 (SIFT)、加速鲁棒特征 (SURF) 和直方图方向梯度 (HOG) 等。这些特征通过描述目标的局部特征，提高了目标检测的准确性。尽管机器学习方法比传统方法有所提升，但其仍然面临数据需求大、训练过程复杂等问题。机器学习模型需要大量的标注数据进行训练，且在应对复杂背景和多变环境时表现不够理想。此外，传统机器学习方法对特征提取的依赖较大，难以应对多样化的目标和复杂的环境变化。

深度学习技术的兴起大大提升了目标检测的准确性和鲁棒性。特别是卷积神经网络 (CNN) 的应用，使得目标检测在复杂环境中的表现大为改善。深度学习方法能够自动从数据中学习复杂的特征和模式，减少了对手工特征提取的依赖，提高了检测的鲁棒性和准确性。深度学习目标检测算法主要分为单阶段检测器和双阶段检测器两类。单阶段检测器如 YOLO^[23] (You Only Look Once) 和 SSD (Single Shot MultiBox Detector)^[24] 在单个神经网络中同时进行目标定位和分类，具有检测速度快的优势，适用于实时检测任务。然而，单阶段检测器在小目标检测和密集目标检测上表现欠佳。

双阶段检测器如 R-CNN (Region-based Convolutional Neural Networks)^[25] 系列, 首先生成候选区域, 然后对这些区域进行分类和回归。R-CNN 包括 Fast R-CNN、Faster R-CNN 和 Mask R-CNN 等变体, 尽管检测速度较慢, 但在检测精度上表现出色。特别是 Mask R-CNN, 不仅能够进行目标检测和分类, 还能实现目标的精确分割, 提供更加详细的目标信息。深度学习技术的应用大大提升了目标检测的准确性和鲁棒性, 但其也面临一些挑战。深度学习模型的训练过程需要大量的标注数据和计算资源, 且模型的复杂性增加了部署和运行的难度。此外, 深度学习模型对环境变化和多样性的适应性仍有待进一步提升。

现有的军用目标检测技术涵盖了从传统图像处理到现代深度学习的多种方法, 结合多源传感器数据、无人机和卫星遥感技术、边缘计算和人工智能辅助分析等手段, 为现代军事行动提供了强有力的技术支持。这些技术方案在复杂战场环境中能够有效地检测和识别目标, 提高了军事行动的效率 and 准确性, 确保了在复杂多变的战场环境中能够实现高效、精准的目标检测。

2.1.2 军用目标跟踪

目标跟踪在军事领域中具有至关重要的作用, 是指在连续帧图像中持续识别和定位同一目标的过程。这一任务在无人机侦察、导弹制导、战场监视等多种军事应用中都有广泛需求。军用目标跟踪作为一项关键的军事任务, 涉及在动态和复杂的战场环境中对移动目标进行实时跟踪。这些目标可以包括敌方车辆、人员、无人机、导弹等, 甚至是多目标的组合。跟踪任务不仅需要识别目标, 还需要准确预测其运动轨迹, 及时更新目标位置信息, 并

在干扰和遮挡情况下保持跟踪的稳定性。在复杂战场环境中, 目标跟踪的挑战主要包括复杂背景干扰、多目标同时跟踪、目标快速移动及目标遮挡等。

在战场环境中, 目标的运动方式多种多样, 可能会涉及突然加速、减速、转弯、停止等不规则运动。目标可能会进入和离开视野, 或者被其他物体遮挡。此外, 环境中的干扰因素, 如烟雾、灰尘、天气变化以及电子干扰等, 都会对跟踪系统的性能产生影响。因此, 军用目标跟踪系统需要具备高度的鲁棒性和适应性, 能够在各种复杂情况下保持稳定的跟踪性能。

现有的军用目标跟踪技术方案主要包括传统方法和基于深度学习的方法。传统方法如卡尔曼滤波和粒子滤波等, 依靠统计模型对目标运动进行预测和更新, 虽然计算效率较高, 但在处理非线性和非高斯分布的复杂目标运动时表现有限。均值漂移 (Mean Shift)^[26] 和光流法 (Optical Flow)^[27] 等技术通过图像特征匹配进行目标跟踪, 但在目标变形和遮挡情况下表现欠佳。

卡尔曼滤波是一种基于线性高斯模型的递推估计方法, 适用于平稳或缓慢变化的目标运动。它通过估计目标的状态 (如位置、速度) 及其不确定性, 来实现对目标的预测和更新。卡尔曼滤波的优点在于计算效率高, 适合实时处理, 但在面对快速变化和非线性运动时, 其表现较差。粒子滤波是一种基于蒙特卡罗方法的非线性和非高斯状态估计技术, 通过大量粒子 (假设) 的权重更新来近似目标状态分布。粒子滤波在处理复杂目标运动时表现优异, 但计算量较大, 不适合实时应用。均值漂移是一种基于目标颜色和纹理特征的非参数统计方法, 通过迭代计算质心位置来实现目标跟踪, 适合处理缓慢变化的

目标，但对快速运动和遮挡敏感。光流法通过分析图像序列中像素的运动来估计目标的运动轨迹，适用于细微运动检测，但在大范围运动和遮挡情况下表现不佳。传统方法虽然在某些简单场景中表现良好，但面对复杂战场环境时，其鲁棒性和精确性有限。

深度学习方法的出现，大大提升了目标跟踪的准确性和鲁棒性。卷积神经网络（CNN）和循环神经网络（RNN）等深度学习模型，能够从大数据中学习复杂的特征和运动模式，实现了更加稳定和精准的目标跟踪。基于深度学习的目标跟踪算法可以分为以下几类：

基于检测的跟踪：这种方法首先检测目标的位置，然后在后续帧中进行跟踪。典型的算法包括 YOLO 和 SSD 等，利用深度学习模型对每帧图像进行目标检测，然后通过关联算法实现目标跟踪。优点是检测精度高，但计算量大，适合离线处理。

端到端跟踪：如 Siamese 网络^[28]（孪生网络）结构，通过比较目标模板和当前帧图像的相似性来实现目标跟踪。这种方法训练简单，能够实现实时跟踪，适用于快速变化的目标。

强化学习跟踪：利用强化学习算法，通过不断学习和适应环境变化，优化跟踪策略，实现更加鲁棒的目标跟踪。典型算法如基于深度强化学习的 DRL-T 方法，通过与环境的交互，不断调整跟踪策略，提高跟踪性能。

在实际应用中，多传感器数据融合技术显得尤为重要。通过融合光学、红外、雷达等多源数据，可以在不同环境条件下提供稳定的跟踪能力。例如，红外传感器在夜间和低能见度条件下表现优异，而雷达可以为穿透烟雾和障碍物，提供可靠的目标信息。多传感器数据融合不仅提高了

目标检测和跟踪的准确性，还增强了系统的鲁棒性和适应性。

光学传感器：光学传感器可以提供高分辨率的可见光图像，适用于白天和良好照明条件下的目标跟踪。光学图像的细节丰富，有助于提高目标识别的精度，但在夜间或恶劣天气条件下表现不佳。

红外传感器：红外传感器通过检测物体的热辐射，实现夜间或低能见度条件下的目标跟踪。红外图像能够穿透烟雾和薄雾，在复杂环境中提供稳定的目标信息，但分辨率相对较低，易受背景温度变化影响。

雷达传感器：雷达传感器通过发射和接收电磁波，实现目标的检测和跟踪。雷达能够穿透障碍物，如烟雾、灰尘等，在全天候条件下提供可靠的目标信息。雷达信号具有较强的抗干扰能力，适用于复杂战场环境，但分辨率和细节较低。

多传感器融合：通过融合光学、红外和雷达数据，可以在不同环境条件下提供更加稳定和可靠的目标跟踪。例如，在白天可以利用光学传感器提供高分辨率图像，夜间和低能见度条件下利用红外传感器提供目标信息，而在复杂环境中则利用雷达传感器提供可靠的检测数据。多传感器融合技术不仅提高了目标检测和跟踪的准确性，还增强了系统的鲁棒性和适应性。

无人机和卫星遥感技术在军用目标跟踪中具有重要应用。无人机可以提供高分辨率的实时图像和视频数据，广泛应用于战场监控和目标跟踪。无人机具有灵活机动的特点，能够快速到达目标区域，提供大范围的监控和跟踪能力。卫星遥感技术通过对地球表面的持续观测，提供高分辨率的图像和数据，适用于大范围目标的检测和跟踪。

无人机技术：无人机搭载高分辨率摄

像机和传感器，能够实时获取战场环境中的目标信息。无人机具有灵活机动的特点，可以在复杂地形和危险区域执行任务，通过实时传输数据，实现远程监控和目标跟踪。无人机的应用大大提升了军用目标跟踪的广域性和精确性。

卫星遥感技术：卫星遥感技术通过对地球表面的持续观测，提供高分辨率的图像和数据，适用于大范围目标的检测和跟踪。卫星遥感能够覆盖广阔的区域，提供全天候的目标监控能力，在战场环境中发挥重要作用。

随着计算能力的提升，边缘计算在军用目标跟踪中的应用越来越广泛。通过将部分计算任务下放到前端设备，如无人机、前线车辆，可以降低数据传输延迟，提高检测速度和实时性。边缘计算能够在靠近数据源的位置进行计算和处理，减少了数据传输的瓶颈，提高了系统的响应速度和实时性。

边缘计算：边缘计算通过在靠近数据源的位置进行计算和处理，减少了数据传输的瓶颈，提高了系统的响应速度和实时性。在军用目标跟踪中，边缘计算可以在无人机和前线车辆上实时处理数据，实现快速检测和跟踪。边缘计算的应用提高了系统的灵活性和鲁棒性，能够在复杂战场环境中提供稳定的目标跟踪能力。

分布式系统：分布式系统通过多个节点的协同工作，实现大规模数据的处理和分析。在军用目标跟踪中，分布式系统能够通过多个传感器和设备的协同工作，提高检测和跟踪的精度和可靠性。分布式系统的应用增强了系统的鲁棒性和适应性，能够在复杂战场环境中提供稳定的目标跟踪能力。

现有的军用目标跟踪技术涵盖了从传统图像处理到现代深度学习的多种方法，

结合多源传感器数据、无人机和卫星遥感技术、边缘计算和人工智能辅助分析等手段，为现代军事行动提供了强有力的技术支持。这些技术方案在复杂战场环境中能够有效地检测和识别目标，提高了军事行动的效率 and 准确性，确保了在复杂多变的战场环境中能够实现高效、精准的目标跟踪。

2.1.3 军用目标分析

军用目标分析在现代军事行动中占据着重要地位，旨在通过对敌方目标的深度分析和评估，为指挥官提供决策支持。目标分析任务包括识别和分类目标、评估其威胁程度、预测目标行为和动向，以及制定相应的作战策略。这些任务通常在复杂多变的战场环境中进行，需要处理大量实时数据，且必须具备高度的准确性和鲁棒性。目标分析的复杂性主要体现在以下几个方面：目标种类多样，包括地面车辆、人员、无人机、导弹等；目标行为多变，可能涉及快速移动、躲避和反击等；战场环境复杂，背景干扰、恶劣天气、电子干扰等因素都会影响目标分析的准确性。

现有的军用目标分析技术涵盖了从传统统计分析到现代深度学习的多种方法。传统统计分析方法依赖于规则和模型，对已知目标特征进行分析和分类。这些方法包括基于贝叶斯推理的威胁评估、马尔可夫链的行为预测等。虽然传统方法在特定条件下表现良好，但其对复杂和多变环境的适应性较差，难以应对动态变化的战场情况。现代深度学习技术的引入，大大提升了目标分析的精度和鲁棒性。卷积神经网络（CNN）、循环神经网络（RNN）和深度强化学习（DRL）^[29]等方法能够从大量数据中自动提取特征和模式，实现了对目标的精确识别和行为预测。例如，CNN可以有效识别目标的图像特征，RNN适用

于处理时间序列数据，预测目标的动态行为，而 DRL 通过与环境的持续交互，优化目标分析策略。

为了应对复杂的战场环境，多传感器数据融合技术在军用目标分析中发挥了重要作用。通过融合来自光学、红外、雷达等多种传感器的数据，可以获得更加全面和可靠的目标信息，提高分析的准确性和鲁棒性。例如，光学传感器提供高分辨率的图像数据，有助于目标识别和分类；红外传感器在夜间和低可见度条件下表现出色，可以检测目标的热辐射信号；雷达传感器具有穿透障碍物的能力，能够在复杂天气条件下提供稳定的目标信息。通过多传感器数据的融合，可以在不同环境和条件下，全面掌握目标的动态信息，增强目标分析的精度和可靠性。

智能化处理技术在军用目标分析中也有着广泛应用。边缘计算和云计算的结合，通过在前线设备上实时处理数据，减少数据传输延迟，提高分析速度和实时性。例如，前线无人机和车辆上的边缘计算设备，可以实时分析和处理捕获的目标数据，快速提供目标位置、类型和行为等关键信息。而云计算平台则通过强大的计算能力和海量数据处理能力，进行深度学习模型的训练和复杂数据的分析，为前线提供智能决策支持。此外，人工智能技术的引入，特别是深度学习模型的应用，使得目标分析系统能够自动从数据中提取关键信息，识别潜在威胁，预测目标行为，辅助指挥官进行决策。深度学习模型如 YOLO、SSD 等在目标识别中表现出色，能够快速准确地识别目标；RNN 和 LSTM^[30] 等时间序列模型，能够分析和预测目标的动态行为，为制定作战策略提供依据；深度强化学习模型通过不断学习和适应环境变化，优化目标分析策略，提高了系统的

鲁棒性和适应性。

现有的军用目标分析技术结合了传统统计分析和现代深度学习方法，利用多传感器数据融合和智能化处理技术，为军事决策提供了强有力的支持。传统统计分析方法通过对已知目标特征的分析 and 分类，为初步目标识别和威胁评估提供了基础。然而，面对复杂和多变的战场环境，其适应性和鲁棒性相对较低。现代深度学习技术的引入，通过自动特征提取和模式识别，大大提升了目标分析的准确性和鲁棒性。多传感器数据融合技术通过综合利用不同传感器的优点，在不同环境和条件下提供全面和可靠的目标信息。智能化处理技术通过边缘计算和云计算的结合，实时分析和处理大量数据，提高了目标分析的速度和实时性。人工智能技术，特别是深度学习模型的应用，使得目标分析系统能够自动识别和预测目标行为，辅助指挥官进行决策。综上所述，现有的军用目标分析技术在复杂战场环境中能够有效地识别和分析目标，为军事行动提供精准的情报支持，确保了作战决策的科学性和有效性。

2.2 现有方法的不足

现有的军用目标检测、跟踪和分析技术虽然在许多方面取得了显著进展，但在实际应用中仍然存在一些不足。传统图像处理技术依赖于手工设计的特征提取方法，如边缘检测、角点检测和颜色分析等。这些方法在低分辨率图像或特定环境下表现良好，但在复杂的战场环境中，其鲁棒性和准确性较低，难以适应多变的环境。特征提取过程中的主观性和局限性，使得这些方法在应对背景复杂、目标多变的战场情况时，效果不佳。此外，传统方法在处理高维数据和复杂模式识别时表现不足，无法充分利用现代传感器提供的丰

富信息。

机器学习方法通过训练分类器来识别目标，虽然比传统方法有所提升，但也面临一些挑战。首先，这些方法需要大量标注数据进行训练，数据标注成本高且耗时。其次，机器学习模型在处理复杂背景和多变环境时，表现仍然不够理想。特征提取和分类器设计的局限性，使得这些方法在面对非线性和非高斯分布的复杂目标运动时，鲁棒性和精确性不足。此外，机器学习方法对特征的选择和组合高度依赖于人工经验，缺乏自动化和适应性。

深度学习技术虽然大大提升了目标检测的准确性和鲁棒性，但也存在一些不足。深度学习模型的训练过程需要大量的标注数据和计算资源，训练成本高且时间长。模型的复杂性增加了部署和运行的难度，特别是在资源受限的前线设备上。此外，深度学习模型对环境变化和多样性的适应性仍有待进一步提升。深度学习算法在处理实时数据时，计算量大，响应速度较慢，难以满足实时性要求。此外，深度学习模型的“黑箱”特性使得其决策过程难以解释和调试，影响了在实际应用中的信任度和可控性。

在目标跟踪方面，传统方法如卡尔曼滤波和粒子滤波，依赖于统计模型进行目标运动的预测和更新，尽管计算效率较高，但在处理非线性和非高斯分布的复杂目标运动时表现有限。特别是当目标出现快速变化、非线性运动或被遮挡时，传统方法的鲁棒性和准确性明显下降。此外，这些方法对环境变化的适应性较差，难以应对战场上多变的情况。深度学习方法在目标跟踪中取得了一定进展，但其对快速变化和复杂背景的适应性仍有待提高，特别是在目标被遮挡和环境光照变化较大的情况下，跟踪效果不佳。

在目标分析方面，传统统计分析方法依赖于规则和模型，对已知目标特征进行分析和分类，这些方法在特定条件下表现良好，但其对复杂和多变环境的适应性较差。现代深度学习技术尽管提升了目标分析的精度和鲁棒性，但也面临一些挑战。深度学习模型的训练过程需要大量的标注数据和计算资源，训练成本高且时间长。模型的复杂性增加了部署和运行的难度，特别是在资源受限的前线设备上。此外，深度学习模型对环境变化和多样性的适应性仍有待进一步提升。在实时数据处理方面，深度学习算法计算量大，响应速度较慢，难以满足实时性要求。深度学习模型的“黑箱”特性使得其决策过程难以解释和调试，影响了在实际应用中的信任度和可控性。

在上述背景下，现代大规模视觉语言模型（Large Vision-Language Models, LVLMs）应运而生，提供了一种全新的解决方案。LVLMs 通过结合视觉和语言信息，能够更全面地理解和分析目标，提升检测、跟踪和分析的准确性和鲁棒性。它们可以利用大规模数据进行预训练，自动学习复杂的特征和模式，减少对手工特征设计的依赖，并且能够在多样化的环境中表现出色。通过引入 LVLMs，军用目标检测、跟踪和分析系统可以实现更高效的自动化处理和智能化决策，从而在复杂的战场环境中提供更强有力的支持。

2.3 各类任务中应用视觉语言大模型的可行性和潜力

随着 LVLMs 的快速发展，其在军事领域中的应用潜力日益显著。为了充分挖掘这些模型在目标检测、目标跟踪和目标识别等任务中的潜力，深入探讨其数据输入与处理机制，以及模型的适用性和有效性

显得尤为重要。本节将详细分析 LVLMs 在这些任务中的应用可行性和潜力，重点关注数据输入和处理的关键环节，以及模型的适用性分析。

2.3.1 数据输入和处理

在军事任务中，数据的多样性和复杂性对视觉语言大模型的应用提出了巨大的挑战。高质量的数据输入和高效的数据处理是确保 LVLMs 在各类任务中表现出色的基础。为了应对这些挑战，LVLMs 需要具备处理多模态数据的能力，包括图像、视频和文本等多种数据源。这些数据源不仅格式各异，而且在实际应用中往往具有较高的实时性和准确性要求。

1. 数据源的多样性与融合

在军事领域，常见的数据源包括卫星影像、无人机拍摄的视频、地面传感器捕捉的图像以及各类文本情报报告。每种数据源都有其独特的优势和局限性，如何有效地将这些数据进行融合，是 LVLMs 在实际应用中的关键所在。卫星影像提供了广域覆盖和高分辨率的地面图像，能够捕捉到大范围的战场态势。无人机视频则提供了高灵活性和实时性的数据，能够对目标进行持续跟踪和监控。地面传感器数据则可以提供更加细致的局部信息，如目标的具体特征和行为模式。而文本情报报告则包含了丰富的语义信息，能够提供背景知识和上下文信息。

LVLMs 通过多模态学习方法，能够将这些不同类型的数据进行有效融合，形成更为全面和精确的目标描述。例如，CLIP 模型通过在大规模图像-文本对上进行预训练，实现了图像和文本的紧密对齐。这种多模态融合能力使得 LVLMs 在处理复杂战场环境和多源信息时，能够提供更加精准的情报分析。

2. 高效的特征提取与表达

视觉语言大模型在数据处理方面表现出色，主要得益于其强大的特征提取和表达能力。通过在大规模数据集上进行预训练，LVLMs 能够学习到丰富且具有判别力的视觉特征和语义特征。这些特征不仅能够提升模型的识别和检测精度，还能增强模型在面对复杂环境和多变背景时的鲁棒性。在最新的 LVLMs 中，ViT 通常被用于图像或视频数据的特征提取。ViT 模型通过引入 Transformer 架构，实现了图像特征的全局建模能力。与传统的卷积神经网络 (CNN) 相比，ViT 能够更好地捕捉图像中的长距离依赖关系，从而提升特征提取的效果，为 LLM 组件提供更为准确的视觉信息。

在实际应用中，视觉语言大模型可以通过迁移学习和微调技术，快速适应不同的任务需求和环境变化。通过在特定任务数据集上的微调，LVLMs 可以被用于检测和识别特定类型的军事目标，如装甲车辆、战机、舰艇等。这种灵活性和适应性使得 LVLMs 在实际应用中具有广泛潜力。

3. 数据预处理与增强

高效的数据预处理和增强技术是提升 LVLMs 性能的重要环节。在军事任务中，数据预处理通常包括数据清洗、归一化、数据增强等步骤。通过数据清洗，可以去除噪声和无关信息，提升数据质量。归一化处理则可以确保数据的尺度一致性，提升模型的训练效果。数据增强技术在提升训练数据的多样性和鲁棒性方面具有重要作用。常见的视觉数据增强方法包括旋转、翻转、裁剪、颜色变换等。这些方法可以生成更多的训练样本，增加模型的泛化能力，从而提升其鲁棒性。此外，数据生成技术也在军事领域中得到了广泛应用。通过生成高逼真度的训练数据，可以

模拟各种复杂的战场环境和目标特征，进一步提升模型的鲁棒性和适应性。

在目标检测任务中，可以利用数据生成技术创建包含不同视角、光照条件和背景环境的目标图像。结合实际的标注数据，这些合成数据可以显著提升模型在复杂环境中的检测精度和鲁棒性。在目标跟踪任务中，数据生成技术可以帮助生成更多的连续帧图像，提升模型对目标的持续跟踪能力。

4. 计算资源与实时处理

在军事任务中，数据处理通常需要面对大规模、高分辨率的数据，这对计算资源和实时处理能力提出了较高要求。为应对这些挑战，LVLMs 可以采用模型优化技术，如模型剪枝、量化和分布式计算等，以提高模型的运行效率和实时性。模型剪枝技术通过移除冗余的神经元和连接^[31]，可以显著减少模型的计算量和存储需求，从而提升运行效率。量化技术^[32]则通过将模型参数从浮点数表示转换为低精度表示，进一步减少计算和存储开销。分布式计算技术通过将计算任务分散到多个节点上进行并行处理，可以显著提升数据处理的速度和实时性。在实际应用中，通过结合这些优化技术，LVLMs 可以在有限的计算资源下，实现高效的数据处理和实时目标检测。在无人机侦察任务中，视觉语言大模型可以通过边缘计算技术，在无人机上实时处理视频数据，对目标进行检测和跟踪，从而提供及时的情报支持。

5. 跨模态数据的联合建模

视觉语言大模型在处理跨模态数据方面的能力，使其在军事任务中具有独特的优势。通过联合建模图像和文本数据，LVLMs 能够在多源信息中提取更加丰富和有意义的特征。

ALIGN 模型通过在大规模图像和文本

数据上进行联合训练，实现了跨模态特征的高效对齐。这种联合建模能力使得模型能够更好地理解和描述目标特征，在复杂的战场环境中提供更为精准的目标识别和分类。联合建模的优势在于能够将图像和文本信息进行互补和强化。在卫星影像分析中，视觉语言大模型可以结合图像数据和文本报告，对目标进行精确定位和描述，提升情报分析的准确性和全面性。在战场监控任务中，LVLMs 通过结合视频流和指挥中心的文本指令，可以实现对目标的实时监控和跟踪，提供更为灵活和高效的情报支持。

2.3.2 模型的适用性分析

在军事任务中，视觉语言大模型以其卓越的性能和多样化的应用场景展现出巨大的适用性。然而，为了充分发挥这些模型在目标检测、目标跟踪和目标识别等任务中的潜力，需要深入分析其适用性，探讨其在不同任务中的具体表现和潜力。

1. 目标检测中的适用性

在目标检测任务中，LVLMs 凭借其多模态融合和强大的特征提取能力表现出色。传统的目标检测模型主要依赖于单一的视觉信息，容易受到背景复杂度和环境变化的影响。而视觉语言大模型通过将视觉和语言信息相结合，能够提供更加全面和精确的目标定位和识别。例如，在战场侦察中，LVLMs 可以结合无人机视频和地面侦察报告，实现对目标的精准检测和定位，从而提高情报的准确性和及时性，如图 4 所示。

此外，LVLMs 在处理多源异构数据方面表现优异。它们可以将不同类型的数据源，如卫星影像、无人机视频、地面传感器数据和文本情报，进行有效融合，从而提升目标检测的鲁棒性和精度。现代的 LVLMs 通过在大规模图像-文本对

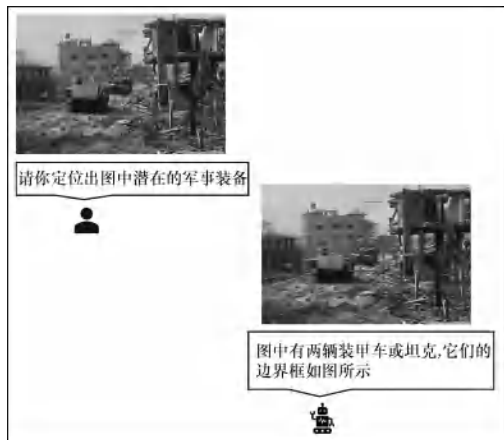


图 4 LVLMs 进行军用目标检测

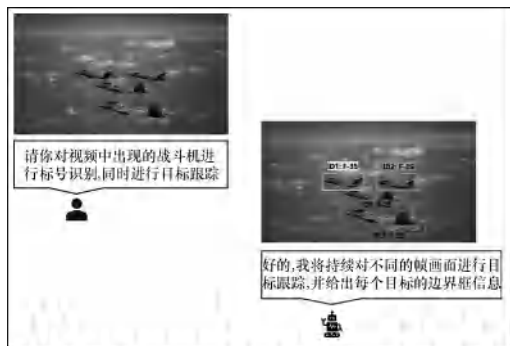


图 5 LVLMs 进行军用目标跟踪

上进行预训练，实现了图像和文本特征的紧密结合，具备了优秀的跨模态特征学习能力。

2. 目标跟踪中的适用性

在目标跟踪任务中，视觉语言大模型通过其强大的跨帧特征提取和建模能力，能够在连续帧图像中保持对目标的持续跟踪。这对于军事任务中的无人机侦察、战场监控等应用尤为重要。传统的目标跟踪算法往往在处理目标遮挡、光照变化和背景复杂度等问题时表现欠佳，而 LVLMs 通过结合世界知识，能够更好地适应这些变化，提供更加稳定和精确的目标跟踪。例如，在无人机侦察任务中，LVLMs 可以通过实时分析无人机拍摄的视频流，对目标进行持续跟踪和定位，确保目标不会在复杂环境中丢失。通过结合地面指挥中心的文本指令，LVLMs 可以实现更加灵活和动态的目标跟踪，提升战场态势感知和决策支持能力，如图 5 所示。

3. 目标识别中的适用性

现代大规模视觉语言模型（LVLMs）在军用目标分析中具有显著的适用性。它们通过结合视觉和语言信息，能够从多源数据中自动学习复杂特征和模式，实现更

加准确和全面的目标检测、跟踪和分析。LVLMs 的预训练能力允许其在多样化环境中保持高鲁棒性和适应性，减少了对手工特征设计的依赖，并提高了实时处理能力。此外，LVLMs 的多模态理解和分析能力，使其能够更好地应对战场环境中的动态变化和复杂背景。通过利用这些模型，军用目标分析系统可以实现更高效的自动化处理和智能化决策支持，从而为指挥官提供更加精准和实时的情报，有助于制定更有效的作战策略和应对方案。LVLMs 不仅提升了系统的整体性能，还增强了在复杂战场环境中的应用广度和深度，为现代军事行动提供了强有力的技术支持，如图 6 所示。



图 6 LVLMs 进行军用目标分析

4. 模型的灵活性与适应性

视觉语言大模型在不同军事任务中的适用性还体现为其高度的灵活性和适应性。通过迁移学习和微调技术, LVLMS 可以快速适应不同的任务需求和环境变化。例如, 通过在特定任务数据集上的微调, LVLMS 可以被用于检测和识别特定类型的军事目标, 如装甲车辆、战机、舰艇等。这种灵活性使得 LVLMS 在实际应用中具有广泛的适用性, 能够满足各种复杂和多变的战场需求。此外, LVLMS 在处理多模态数据方面的优势, 使其在跨任务应用中表现出色。无论是目标检测、目标跟踪还是目标识别, LVLMS 都能够通过其强大的跨模态特征学习能力, 实现高效的数据融合和处理, 提升各类任务的执行效果和准确性。

未来, 随着视觉语言大模型技术的不断进步和应用经验的积累, 这些模型将在军事任务中发挥更加重要的作用。通过进一步优化模型的适用性和鲁棒性, 提升数据处理和融合能力, LVLMS 将为军事情报分析和决策提供更为强大的技术支持, 显著提升战场态势感知和指挥决策的精准度和及时性。

总的来说, 视觉语言大模型在目标检测、目标跟踪和目标识别等任务中的适用性分析显示了其巨大的潜力和广泛的应用前景。通过多模态数据融合、强大的特征提取与表示能力, 以及高效的计算资源优化, LVLMS 为各类军事任务提供了坚实的技术支撑。随着技术的不断发展, 这些模型将在未来的军事应用中发挥更加重要的作用, 推动战场情报分析和决策支持能力的不断提升。

2.3.3 视觉语言大模型的实际应用

视觉编码器是 LVLMS 的重要组成部分, 当前最常用的编码器是基于预训练的

ViT 模型, 该模型在拥有充足的训练数据时, 其性能可以超越传统的卷积神经网络 (CNN)。ViT 的核心思想是将输入的图像分割成多个固定大小的小块 (patches), 这些小块类似于自然语言处理中的单词。这些图像块首先被展平, 随后通过线性变换层转换为固定维度的嵌入向量。为保持图像块的空间关系, ViT 为每个图像块引入了位置嵌入 (position embeddings), 此方法与 Transformer 在 NLP 中的处理方式类似。这些嵌入向量被送入多个 Transformer 层, 每层都包含多头自注意力机制和前馈神经网络, 使模型能在处理每个图像块时综合其他所有图像块的信息, 从而捕捉图像丰富的全局上下文信息。

CLIP 是由 OpenAI 开发的一种先进的多模态学习模型, 其主要通过对比学习方法在大规模异构数据集上同时训练图像和文本编码器。该模型主要由两个组件组成: 一是基于 Vision Transformer (ViT) 的视觉编码器, 用于从输入图像中提取特征; 二是基于 Transformer 架构的文本编码器, 负责处理输入的文本描述并将其转化为嵌入向量。CLIP 的核心训练机制是利用对比学习, 在每个训练批次中区分正确的图像-文本对 (正样本) 与错误的图像-文本组合 (负样本)。通过这种机制, 模型被训练以将图像特征和对应的文本描述映射到同一个高维空间中, 并在该空间内最大化正样本对的相似性, 同时最小化与负样本对的相似性。ViT 作为视觉编码器在 CLIP 中的应用展示了其多样性和适应性, 具体变体包括常用于 CLIP 模型的 ViT-L, 以及在不同版本的 CLIP 实现中使用的其他架构, 如 OpenCLIP 中的 ViT-L^[33] 架构和 EVA-CLIP^[34] 使用的 ViT-g 版本。这些变体展示了 ViT 架构在处理复杂多模态数据时的强大能力和灵活性。

视觉语言大模型在目标跟踪任务中具备诸多优势。首先,这些模型能够有效处理和融合多模态数据,如将图像、视频和文本信息相结合,从而在复杂的战场环境中提供更准确和全面的跟踪信息。通过将视觉和语言信息融合,LVLMs可以更好地理解 and 描述目标特征,提升跟踪的稳定性和精度。LVLMs通过融合多模态数据,提供更加全面和精确的目标分析。军用任务中,通常需要结合多种数据源,如卫星影像、地面传感器数据、情报报告等。视觉语言大模型能够将这些不同类型的数据进行有效融合,形成综合的情报分析。将视觉输入有效地投影到文本嵌入空间的最直接方法之一是使用线性映射。这种方法通过单个线性层将视觉特征转换为与文本特征相同维度的表示,从而实现模态之间的对齐。例如,LLaMA-Adapter^[35]和FROMAGe^[36]均采用了这种简单的线性层来作为视觉语言适配器。进一步地,多层感知机(MLP)提供了一个更复杂的替代方案,它通过增加非线性处理层来增强模型的表达能力。例如,LLaVa-1.5^[37]和MouSi^[38]均采用了包含两层MLP的结构,这种方法显示出了在处理多模态输入时的改进能力。其他模型如Lynx^[39]和LION^[40]也采用了相似的双层MLP构架作为其视觉语言适配器。在无人机跟踪任务中,大模型可以结合实时视频流和指挥中心的文本指令,对目标进行精确定位和持续跟踪,确保目标不会在复杂环境中丢失。

其次,视觉语言大模型具备强大的特征提取和表达能力。这些模型能够从大规模数据中学习 to 丰富且具有判别力的视觉特征,使其在面对多种干扰因素(如目标遮挡、姿态变化、光照变化)时,仍能保持高效跟踪。现代LVLMs是基于Transformer架构的模型,能够捕捉到目标

的细微变化和长时依赖特征,显著提升跟踪的鲁棒性和准确性。此外,通过迁移学习和微调技术,这些模型可以快速适应不同的任务需求和环境变化,提升在实际应用中的灵活性和适应性。

在实际应用中,视觉语言大模型已经在多个军用目标跟踪任务中得到了验证。例如,在无人机战场监视任务中,LVLMs被用于实时处理无人机拍摄的连续视频流,对敌方目标进行持续跟踪和定位,从而提供及时的战场态势信息。在导弹制导系统中,视觉语言大模型通过融合多模态数据,实现对移动目标的精确跟踪,提高导弹命中率和打击效果。此外,在边境监控系统中,LVLMs通过对监控视频的实时分析和目标跟踪,有效识别和追踪非法入侵者,增强边境安全。视觉语言大模型在军用目标跟踪中的应用也面临一些挑战。军用目标跟踪任务通常需要处理大规模和高分辨率的视频数据,这对计算资源和实时处理能力提出了高要求。为应对这一挑战,可以采用模型剪枝、量化和分布式计算等技术,提高模型的运行效率和实时性。同时,目标跟踪任务往往处于复杂和动态的战场环境中,模型需要具备较强的鲁棒性和适应能力。通过多模态数据融合和自监督学习技术,可以提升模型在复杂环境中的稳定性和适应性。

视觉语言大模型通过将视觉信息与自然语言结合,实现了对图像和视频内容的语义理解和描述。相比传统的图像处理技术,LVLMs可以通过自然语言与用户进行交互,提供更直观和易于理解的分析结果。例如,指挥官可以通过简单的自然语言指令,查询特定目标的详细信息,如目标的类型、位置、状态以及相关的战术建议。这种自然语言交互能力使得操作人员可以更方便地获取所需的情报,提高了分

析效率和准确性。在实际应用中，视觉语言大模型可以对已检测到的军用目标进行实时分析和描述。例如，在无人机侦察任务中，LVLMs 可以自动生成目标的文本描述，包括目标的外观特征、行为模式以及可能的威胁等级。这些描述可以直接呈现在指挥中心的情报界面上，帮助指挥官快速了解目标的具体情况，做出相应的决策。

军事场景下，LVLMs 可以结合卫星影像和地面传感器数据，对某一目标区域进行全面扫描和分析，识别出所有潜在威胁并生成详细的报告。这种多模态数据融合能力不仅提高了分析的准确性，还能提供更为全面的战场态势感知。通过对多模态数据的融合分析，LVLMs 能够生成更加详尽和有意义的情报报告。例如，在战场监控中，LVLMs 可以分析实时视频流和历史情报数据，预测敌方部队的行动路线和可能的攻击目标。通过将这些分析结果转换为自然语言描述，指挥官可以更直观地理解战场态势，并做出更有效的战略决策。

视觉语言大模型的引入使得目标分析过程更加智能化和自动化。传统的目标分析依赖于人工操作和判断，效率较低且容易出错。而 LVLMs 通过自动化的图像和文本处理能力，可以实现对目标的实时分析和持续监控。例如，在导弹制导系统中，LVLMs 可以自动识别和跟踪目标，并提供实时的目标状态和位置更新。这种智能化的分析过程不仅提高了任务的执行效率，还减少了人工操作的负担，降低了出错的风险。此外，LVLMs 还可以通过学习和适应，不断优化其分析能力。通过对历史数据和实时数据的持续学习，LVLMs 可以不断提升其对目标特征和行为模式的理解，提供更加精准的分析结果。LVLMs 可以通过不断更新和优化模型，适应不同的任务需求和环境变化，提高目标分析的适用性

和鲁棒性。

视觉语言大模型的自然语言交互能力显著提升了人机交互体验。操作人员可以通过自然语言直接与模型进行对话，查询目标信息和获取分析结果。例如，指挥官可以询问：“这一区域内有哪些潜在威胁？” LVLMs 会自动分析相关数据并生成详细的回答。这种直观的交互方式不仅简化了操作流程，还使得复杂的情报分析变得更加易于理解和利用。在军事训练和演习中，LVLMs 的自然语言交互能力也发挥了重要作用，训练人员可以通过自然语言指令，模拟不同的战场场景和目标情况，进行实战演练和战术推演。LVLMs 通过生成详细的情报报告和战术建议，帮助训练人员提高应对复杂战场环境的能力。

3 视觉语言大模型的优势与挑战

随着军事技术的快速发展，军事目标分析领域对信息处理技术的需求日益增加。视觉语言大模型作为人工智能领域的重要分支，其多模态输入的处理能力、复杂场景的识别和分析能力以及高效的任务执行能力为军事目标分析带来了新的可能性。然而，视觉语言大模型在军事目标分析领域的应用也面临着诸多挑战，如模型训练和优化的难度、数据隐私和安全性问题以及实时性和计算资源要求等。本章将从优势与挑战两个方面，结合军事目标分析领域，对视觉语言大模型进行探讨。

3.1 视觉语言大模型的优势

3.1.1 多模态输入的处理能力

传统的大模型仅针对文本数据进行训练和应用，如 GPT 系列和 LLaMA 系列等，它们在文本理解和生成等任务上表现出色，但在理解其他数据类型方面存在局限

性。虽然这些文本模型在情报分析与侦察、作战决策、网络及认知战方面已取得广泛应用，但视觉感知能力的缺失极大地限制了其在目标分析领域的赋能应用。

视觉语言大模型的一个显著优势在于其能够处理多模态输入，即同时处理文本、图像和视频等多模态数据。这种能力使得模型能够更全面地理解世界，提高信息处理的准确性和效率。在军事目标分析领域，信息的来源多种多样，包括图像、视频、文本等。视觉语言大模型能够同时处理这些多模态输入，将不同来源的信息进行有效融合。例如，在军事侦察中，通过无人机拍摄的图像和视频可以获取目标的外观、位置等信息，而文本情报则可能包含目标的类型、用途等关键信息。视觉语言大模型能够将这些信息进行融合，生成更全面的目標分析报告，为军事决策提供更有力的支持。

3.1.2 复杂场景的识别和分析能力

视觉语言大模型在复杂场景的识别和分析方面表现出色。通过深度学习技术的训练，模型能够学习到大量图像和文本的特征，从而实现对复杂场景的准确识别和分析。视觉语言大模型能突破人眼在速度、不可见光范围的极限，提高武器装备信息获取能力的自动化程度，是提高装备智能与自动化水平的关键^[41]。

军事目标分析通常需要在复杂的场景中进行，如战场环境、城市街道等。这些场景中的目标数量巨大、种类繁多，且往往存在遮挡、变形等问题。在军事目标分析中，视觉语言大模型可以自动识别出目标类型、数量、位置等信息，并对目标的运动轨迹、速度等动态信息进行跟踪和分析。这对于及时发现敌方目标、评估战场态势具有重要意义。

3.1.3 高效的任務執行能力

军事目标分析任务通常需要在短时间内完成，以便为军事决策提供及时支持。人工智能技术能够对采集到的海量图像进行准确、快速的分析，使人工资源与物质资源的消耗得到减少，且随着国防水平的不断提高与科技能力的不断增强，即处理器运算速度的提升与识别算法的不断优化，对于目标的识别速度与准确率也远远高于人的肉眼。新形势下，迎合信息化联合作战与智能化武器装备，会在未来无人战争的发展中，对掌握战场态势、获取最终胜利起到至关重要的作用^[42]。

视觉语言大模型具有高效的任務執行能力，可以快速处理和分析大量信息，生成准确的目标分析报告。在军事目标分析中，视觉语言大模型可以实时接收来自各种传感器的数据，如雷达图像、红外成像等，对这些数据进行快速处理和分析，并生成目标分析报告。这种高效的任務執行能力使得军事目标分析更加及时、准确和有效。

3.2 视觉语言大模型面临的挑战

3.2.1 模型训练和优化的难度

视觉语言大模型的训练和优化是一个巨大的挑战。由于模型需要处理多模态输入和复杂场景，因此，需要大量的标注数据用于训练。然而，在实际应用中，标注数据的获取和标注成本往往非常高昂。此外，由于模型结构复杂、参数众多，因此，在训练过程中容易出现过拟合、优化震荡等问题。为了解决这些问题，研究人员需要采用各种优化算法和技巧，如正则化、批量归一化、梯度裁剪等，以提高模型的泛化能力和训练稳定性。

在军事目标分析领域，由于目标种类繁多、场景复杂多变，因此，模型的训练

和优化难度更大,且模型的调整和优化也需要大量的时间和计算资源。目前,军事领域用于训练的有效数据占比不高,文本和图像的匹配数据稀缺,容易导致输出模型在执行多模态任务时出错或出现结果偏差^[43]。因此,如何在有限的资源和时间内训练和优化出性能良好的视觉语言大模型是一个亟待解决的问题。通过梳理大模型训练调优全过程对军事领域数据特征的需求,可以为二次预训练、领域数据微调学习、模型调优三个阶段建设垂直领域高质量数据集。针对现有相关数据资源,使用统计学方法进行分析,如评估数据样本的分布、类别、主题和复杂性等,并采取清洗、扩增、泛化、标注、治理等手段确保数据集的均衡性和质量,提升不同应用场景下垂域微调数据集的准确性和有效性。

3.2.2 数据隐私和安全性问题

视觉语言大模型面临着数据隐私和安全性问题。由于模型需要处理军事图像、情报文本等敏感信息,因此,必须确保这些数据的安全性和隐私性。然而,在实际应用中,由于模型通常部署在云端或第三方服务器上,因此,可能存在数据泄露的风险^[44]。研究人员需要采用各种加密技术、访问控制策略等手段,确保训练和推理数据在传输、存储和处理过程中的安全性。在军事目标分析领域,由于视觉语言大模型需要处理大量的军事敏感信息,如目标位置、类型等,数据的隐私和安全性问题尤为重要。因此,需要加强对模型使用过程的监管和审计工作,防止数据泄露和滥用事件的发生。

3.2.3 实时性和计算资源要求

视觉语言大模型在实时性和计算资源要求方面也存在挑战。在实际应用中,由于硬件设备和计算资源的限制,往往难以满足这种要求。为解决该问题,研究人员

需要采用各种优化算法和技巧,如模型压缩、剪枝、量化等,以降低模型对计算和存储资源的消耗。同时,还需要探索新的硬件设备和计算架构,如专用芯片、分布式计算等,以提高模型的实时性和计算性能。

军事目标分析任务对实时性和计算资源提出了更高的要求。在战场环境下,信息的实时性对于军事决策至关重要。一方面,为了针对动态环境提高模型效能,需要快速高效地对大量的图像和视频进行有效处理,实时地掌握军事目标的动态信息,因此,要求视觉语言大模型必须具有较快的计算速度,否则会导致系统的时滞,难以实时掌握动态信息。另一方面,视觉语言大模型应具有很强的抗干扰能力,即在战场环境中存在一系列干扰源的情况下,也能保证快速对图像进行准确处理,使得图像处理的结果准确和不失真,并将结果反馈给指挥系统^[45]。然而,视觉语言大模型的参数量大、计算复杂度高,需要大量计算资源以满足实时性的要求。除此之外,视觉语言大模型普遍存在幻觉现象,在目标分析时容易被相似物体所迷惑^[46]。

为了解决这个问题,研究人员需要采用各种优化算法和技巧,如模型压缩、剪枝、量化等,以降低模型的计算复杂度和资源消耗。同时,还需要探索新的硬件设备和计算架构,如专用芯片、分布式计算等,以提高模型的实时性和计算性能。模型压缩与剪枝通过剪枝、量化等手段减少模型参数和计算量,提高模型推理速度。边缘计算将视觉语言大模型部署到边缘设备上,减少数据传输延迟,提高实时性。分布式计算利用分布式计算架构,将计算任务分配到多个计算节点上并行处理,提高整体计算效率。结合模型压缩、边缘计

算和分布式计算技术等，可以帮助构建高效、低延迟的军事目标分析系统。

4 视觉语言大模型在军用目标分析中的前景

4.1 潜在的技术突破

随着视觉语言大模型的发展，其已在军用目标分析领域展现出了强大前景。但由于视觉语言大模型本身所存在的局限性，如幻觉现象，需要更加优异的算法以及模型架构以提高其在目标分析任务中的准确性。

4.1.1 自适应算法

自适应算法主要包括自适应权重调整以及在线学习和持续学习^[47]。其中自适应权重调整是指能够动态调整权重的自适应学习算法^[48]，以帮助模型在处理不同类型的视觉以及语言数据时能够更加灵活，提高其在不同环境和任务中的具体表现；在线学习和持续学习主要是指实现模型的在线学习能力，使其能够在部署后持续学习和优化，对于模型应对在战场环境中的快速变化和新目标的出现尤为重要。

4.1.2 多模态融合技术

增强模型的跨模态注意力机制^[49]，使其能够更好地捕捉图像和文本之间的复杂关系。例如，开发更精细的自注意力机制（self-attention）来处理图像中的细节和文本描述之间的对应关系；研究新的表示学习方法，统一表示学习。将图像和文本统一编码到同一个高维空间中，减少模态之间的差距，提高模型的理解和生成能力。

4.1.3 模型压缩

通过剪枝（pruning）和量化（quantization）技术^[50]，减少模型参数和计算量，

使得视觉语言大模型能够在资源受限的设备上高效运行。这对于前线的移动设备和无人系统尤为重要。此外，也可以利用知识蒸馏技术，将复杂模型所学习的知识转移到参数更少、效率更高的模型上，做到保留性能的同时减少计算资源的需求。

4.2 增强现实（AR）和虚拟现实（VR）技术的结合

增强现实（AR）可用于增强战场态势感知。通过实时信息叠加将视觉语言大模型生成的情报信息，如目标位置、威胁等级和行动建议等，投射到士兵的AR眼睛或者头盔显示器上，进一步提高士兵在战场上的态势感知和决策能力。同时利用AR技术进行战场模拟和训练，能够将真实环境和虚拟敌人相结合，从而提高训练的真实感和效果。

VR沉浸式目标分析主要包括两部分：目标分析环境和战术规划及演练。目标分析环境方面是指通过构建虚拟现实情报分析室，分析人员可以在虚拟环境下查看和分析来自不同传感器和数据源的目标情报，进而通过自然交互方式（如手势、语音）对所得数据进行操作和分析；战术规划演练方面，即利用VR技术进行战术规划和演练，指挥官可以通过在虚拟环境中测试和优化战术方案，从而进一步评估不同策略的效果，用以提高实际执行的准备度。

未来可以考虑将增强现实（AR）和虚拟现实（VR）技术进一步结合，发展混合现实（MR）协同作战技术：开发混合现实界面（多模态协调），结合AR和VR技术，完成士兵、无人系统和指挥中心之间的三位一体，完成三者之间的多模态协同。士兵可以在AR界面中看到指挥中心的实时指示和无人系统的反馈，而指

挥中心可以在 VR 环境中监控和协调全局。同时通过混合现实技术, 远程专家也可以实时指导前线士兵, 进而为军队和士兵提供技术支持和战术建议。专家通过 VR 设备查看前线士兵的 AR 视角, 为作战提供更准确和更及时的支援。

4.3 可能的应用场景

视觉语言大模型在军用目标分析中具有广阔的前景。可以显著提高自动目标识别和分类的效率以及准确性。通过结合视觉以及语言信息, 视觉语言大模型能够在复杂的作战环境中精确识别分类各种目标, 如车辆、武器、人员和建筑物等。

视觉语言大模型在目标跟踪与监控方面也展现出强大的应用潜力。它们可以实时跟踪和监控目标, 提供精确的位置信息和动态变化情况, 同时, AR 和 VR 技术可以用来增强监控系统的实时性和分析能力。通过 AR 眼镜, 安全人员可以实时接收来自监控摄像头的警报和可视化信息, 快速定位和响应潜在威胁。VR 技术则可以用于回放和分析监控视频, 重建犯罪现场或战场情况, 进行详细的事后分析。同时, 利用 AR 技术实现可视化情报展示, 将监控系统收集到的情报数据以可视化的形式叠加在现实世界中, 帮助安全人员更直观地理解复杂的情报信息。结合视觉语言大模型与 AR 和 VR 技术^[51], 监控系统可以在接收到图像和视频数据后, 自动识别和标注潜在威胁。通过 AR 眼镜, 安全人员可以实时接收警报和情报数据的可视化信息, 如目标身份、位置和活动描述。利用 VR 技术进行监控视频的回放和分析, LVLMS 可以提供详细的事件描述和推理, 重建犯罪现场或战场情况。

情报收集方面, 视觉语言大模型能够处理无人机、卫星等获取的大量图片信

息, 从中提取有价值的情报。操作人员可以通过大模型实现远程控制和监控^[52], 通过 VR 设备和 LVLMS, 操作人员可以在沉浸式环境中控制无人机或无人地面车辆, 实时获取多模态信息(图像和文本)。LVLMS 可以分析环境数据, 提供自然语言描述, 帮助操作人员做出更精确的决策, 并远离危险区域; 在环境感知和决策方面, AR 技术结合 LVLMS, 能够有效增强无人系统的环境感知能力。传感器数据和导航信息可以实时转换为视觉和语言描述, 叠加在操作人员的视野中。无人系统可以自主进行语义理解和决策, 通过自然语言与操作人员互动, 解释其决策过程和环境变化。

同时, 视觉语言大模型也可用于辅助指挥官决策, 结合 AR 和 VR 技术与 LVLMS, 可以构建沉浸式的战场态势感知系统。指挥官可以通过 AR 眼镜查看实时战场地图、部队位置和敌情动态, 并通过 LVLMS 生成的自然语言描述进行态势解释和建议。利用 VR 设备进行战术推演和决策模拟, LVLMS 可以分析不同战术方案, 提供语义反馈和优化建议。同时, 在协同作战和任务规划方面, 利用 VR 技术和 LVLMS 进行任务规划和演练, 可以模拟不同战术方案, 并生成详细的语义描述和评估报告。LVLMS 可以整合多源数据, 提供全面的态势分析和协同作战建议, 帮助指挥官优化任务规划, 提高协同作战能力。

4.4 道德和社会影响

4.4.1 数据隐私保护

结合 LVLMS 的 AR 和 VR 技术在军事和监控系统中的应用会产生大量的视觉和语言数据, 这些数据将涉及敏感的军事及私人信息。确保数据的安全存储和传输, 防止泄露和滥用, 是一个关键挑战。需要

开发先进的加密和访问控制技术,保护数据隐私。同时,也需要在透明度和监管方面进一步加强,需要建立透明的数据,使用政策和有效的监管机制,确保在使用AR和VR技术结合LVLMs收集和数据处理数据时,遵守相关法律法规,保护个人隐私权。制定明确的使用和管理准则有助于确保数据被合理和合法地使用。

4.4.2 自动化战争的伦理问题

目前,自动化战争的伦理问题主要在于两个方面,其一在于人类控制和对应的责任,随着LVLMs在自主无人系统中的应用,战争中的决策将越来越自动化。确保这些系统在关键决策中保留人类控制^[53],并明确责任划分,是一个亟待解决的伦理问题。需要制定明确的伦理准则和操作规范,确保人类对自动化系统的最终控制权;其二在于战争本身的成本问题以及战争带来的影响,自动化战争无疑会降低战争的直接成本,进而会增加使用武力的可能性,从而影响全球和平和安全。对于此,国际社会需要制定和遵守相关伦理准则,防止技术滥用和战争升级^[54]。需要进行广泛的社会讨论和国际合作,建立全球范围内的技术监管和伦理框架。

5 结束语

本文探讨了视觉语言大模型在目标分析中的应用与前景。通过综合自然语言处理和计算机视觉,视觉语言大模型具备了多模态信息融合能力,使其能够在复杂多变的战场环境中,实现高效、精准的目标识别与分析。例如,通过实时处理战场图像并结合文本信息,视觉语言大模型可以为指挥官提供更为全面和精确的战场态势报告,辅助决策的制定。然而,尽管这类模型具备诸多优势,其在实际应用中仍面

临若干挑战。比如,模型的训练和优化过程复杂,依赖于大规模的高质量训练数据和计算资源。此外,数据隐私和安全性问题也是不容忽视的关键因素。在军事应用中,如何确保数据和模型的安全和隐私保护,避免潜在的安全风险,是需要重点解决的问题。实时性要求和计算资源的制约,也对模型的部署和应用提出了更高的要求。总体而言,视觉语言大模型在军用目标分析中的应用前景令人期待。未来研究应聚焦于模型的优化与改进,探索更为高效的训练策略和模型架构,并提升模型面对攻击时的鲁棒性。同时,还需关注技术带来的伦理和社会问题,确保其在军事领域的应用符合相关法规和道德规范。通过持续的技术创新和实践应用,视觉语言大模型有望成为推动军事智能化发展的重要力量,为实现更加智能、高效的目标分析和决策支持贡献力量。

参考文献

- 1 江志浩,王雅芬,郑义成,等.战场目标特性数据应用分析[J].数字海洋与水下攻防,2021,4(3):160-166.
- 2 袁艺.目标分析:找准对手的“阿喀琉斯之踵”[N].解放军报,2014-02-18(5).
- 3 LIU H, LI C, WU Q, et al. Visual instruction tuning [J]. *Advances in neural information processing systems*, 2024, 36.
- 4 LIU H, LI C, LI Y, et al. Improved baselines with visual instruction tuning [C] // *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2024: 26296-26306.
- 5 ZHU D, CHEN J, SHEN X, et al. Minigt-4: Enhancing vision-language understanding with advanced large language models [J]. *arXiv preprint arXiv: 2304.10592*, 2023.
- 6 ACHIAM J, ADLER S, AGARWAL S, et al. Gpt-4 technical report [J]. *arXiv preprint arXiv:*

2303. 08774, 2023.
- 7 TEAM G, ANIL R, BORGEAUD S, et al. Gemini: a family of highly capable multimodal models [J]. arXiv preprint arXiv: 2312. 11805, 2023.
- 8 TAN H, BANSAL M. Lxmert: Learning cross-modality encoder representations from transformers [J]. arXiv preprint arXiv: 1908. 07490, 2019.
- 9 CHEN Y C, LI L, YU L, et al. Uniter: Universal image-text representation learning [C] //European conference on computer vision. Cham: Springer International Publishing, 2020: 104-120.
- 10 KIM W, SON B, KIM I. Vilt: Vision-and-language transformer without convolution or region supervision [C] //International conference on machine learning. PMLR, 2021: 5583-5594.
- 11 WANG Z, YU J, YU A W, et al. Simvlm: Simple visual language model pretraining with weak supervision [J]. arXiv preprint arXiv: 2108. 10904, 2021.
- 12 RADFORD A, KIM J W, HALLACY C, et al. Learning transferable visual models from natural language supervision [C] //International conference on machine learning. PMLR, 2021: 8748-8763.
- 13 JIA C, YANG Y, XIA Y, et al. Scaling up visual and vision-language representation learning with noisy text supervision [C] //International conference on machine learning. PMLR, 2021: 4904-4916.
- 14 BAI J, BAI S, YANG S, et al. Qwen-vl: A frontier large vision-language model with versatile abilities [J]. arXiv preprint arXiv: 2308. 12966, 2023.
- 15 WANG W, LV Q, YU W, et al. Cogvlm: Visual expert for pretrained language models [J]. arXiv preprint arXiv: 2311. 03079, 2023.
- 16 LONGPRE S, HOU L, VU T, et al. The flan collection: Designing data and methods for effective instruction tuning [C] //International Conference on Machine Learning. PMLR, 2023: 22631-22648.
- 17 TOUVRON H, LAVRIL T, IZACARD G, et al. Llama: Open and efficient foundation language models [J]. arXiv preprint arXiv: 2302. 13971, 2023.
- 18 方路平, 何杭江, 周国民. 目标检测算法研究综述 [J]. 计算机工程与应用, 2018, 54 (13): 11-18.
- 19 陆宗骥, 梁诚. 用 Sobel 算子细化边缘 [J]. 中国图象图形学报, 2000, 5 (6): 516-520.
- 20 林卉, 赵长胜, 舒宁. 基于 Canny 算子的边缘检测及评价 [J]. 黑龙江工程学院学报, 2003, 17 (2): 3-6.
- 21 刘丽, 匡纲要. 图像纹理特征提取方法综述 [J]. 中国图象图形学报, 2009, 14 (4): 622-635.
- 22 尤鸿霞. 形状分析方法综述 [J]. 电脑知识与技术, 2009 (11X): 9047-9049.
- 23 REDMON J, DIVVALA S, GIRSHICK R, et al. You only look once: Unified, real-time object detection [C] //Proceedings of the IEEE conference on computer vision and pattern recognition. 2016: 779-788.
- 24 LIU W, ANGUELOV D, ERHAN D, et al. Ssd: Single shot multibox detector [C] //Computer Vision-ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part I 14. Springer International Publishing, 2016: 21-37.
- 25 GIRSHICK R, DONAHUE J, DARRELL T, et al. Region-based convolutional networks for accurate object detection and segmentation [J]. IEEE transactions on pattern analysis and machine intelligence, 2015, 38 (1): 142-158.
- 26 COMANICIU D, MEER P. Mean shift analysis and applications [C] //Proceedings of the seventh IEEE international conference on computer vision. IEEE, 1999, 2: 1197-1203.
- 27 BEAUCHEMIN S S, BARRON J L. The computation of optical flow [J]. ACM computing surveys (CSUR), 1995, 27 (3): 433-466.
- 28 CHICCO D. Siamese neural networks: An overview [J]. Artificial neural networks, 2021: 73-94.
- 29 LI Y, HU X, ZHUANG Y, et al. Deep reinforcement learning (DRL): Another perspective for unsupervised wireless localization [J]. IEEE internet of things journal, 2019, 7 (7): 6279-6287.
- 30 YU Y, SI X, HU C, et al. A review of recurrent

- neural networks; LSTM cells and network architectures [J]. *Neural computation*, 2019, 31 (7): 1235–1270.
- 31 AN Y, ZHAO X, YU T, et al. Fluctuation-based adaptive structured pruning for large language models [C] // *Proceedings of the AAAI Conference on Artificial Intelligence*. 2024; 10865–10873.
- 32 LEE C, JIN J, KIM T, et al. Owq: Outlier-aware weight quantization for efficient fine-tuning and inference of large language models [C] // *Proceedings of the AAAI Conference on Artificial Intelligence*. 2024; 13355–13364.
- 33 DOSOVITSKIY A, BEYER L, KOLESNIKOV A, et al. An image is worth 16×16 words; Transformers for image recognition at scale [J]. *arXiv preprint arXiv*: 2010. 11929, 2020.
- 34 SUN Q, FANG Y, WU L, et al. Eva-clip: Improved training techniques for clip at scale [J]. *arXiv preprint arXiv*: 2303. 15389, 2023.
- 35 ZHANG R, HAN J, LIU C, et al. LLaMA-adapter: Efficient fine-tuning of large language models with zero-initialized attention [C] // *The Twelfth International Conference on Learning Representations*. 2024.
- 36 MA C, JIANG Y, WU J, et al. Groma: Localized Visual Tokenization for Grounding Multimodal Large Language Models [J]. *arXiv preprint arXiv*: 2404. 13013, 2024.
- 37 LIU H, LI C, LI Y, et al. Improved baselines with visual instruction tuning [C] // *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2024; 26296–26306.
- 38 FAN X, JI T, JIANG C, et al. MouSi: Poly-Visual-Expert Vision-Language Models [J]. *arXiv preprint arXiv*: 2401. 17221, 2024.
- 39 ZENG Y, ZHANG H, ZHENG J, et al. What matters in training a gpt4-style language model with multimodal inputs? [C] // *Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers)*. 2024; 7930–7957.
- 40 CHEN G, SHEN L, SHAO R, et al. LION: Empowering multimodal large language model with dual-level visual knowledge [C] // *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2024; 26540–26550.
- 41 黄少罗, 张建新, 卜昭锋. 机器视觉技术军事应用文献综述 [J]. *兵工自动化*, 2019, 38 (2): 16–21. DOI: 10. 7690/bgzdh. 2019. 02. 004.
- 42 宋晓茹, 刘康, 高嵩, 等. 基于深度学习的军事目标识别算法综述 [J]. *科学技术与工程*, 2022, 22 (22): 9466–9475. DOI: 10. 3969/j. issn. 1671-1815. 2022. 22. 003.
- 43 蔡磊, 孟宪波, 韩冬梅, 等. 大模型在军事垂直领域的应用 [J]. *舰船科学技术*, 2024, 46 (5): 171–175. DOI: 10. 3404/j. issn. 1672-7649. 2024. 05. 032.
- 44 周中元, 刘小毅, 李清伟, 等. ChatGPT 技术及其对军事安全影响 [J]. *指挥信息系统与技术*, 2023, 14 (2): 7–16. DOI: 10. 15908/j. cnki. cist. 2023. 02. 002.
- 45 陈静, 宫黎明. 机器视觉在军事领域的应用现状及发展趋势 [J]. *遥测遥控*, 2022, 43 (6): 124–135. DOI: 10. 12347/j. ycyk. 20211115001.
- 46 BAI Z, WANG P, XIAO T, et al. Hallucination of Multimodal Large Language Models: A Survey [J]. *ArXiv*, abs/2404. 18930.
- 47 WU Z, YAN H. Adaptive dynamic networks for object detection in aerial images [J]. *Pattern Recognition Letters*, 2023, 166: 8–15.
- 48 PADULANO R, LAMA G F C, RIANNA G, et al. Future rainfall scenarios for the assessment of water availability in Italy [C] // *2020 IEEE International Workshop on Metrology for Agriculture and Forestry (MetroAgriFor)*. Trento, Italy, 2020; 241–246.
- 49 ZONG Y, MAC A O, HOSPEDALES T. Self-supervised multimodal learning: A survey [J]. *arxiv preprint arxiv*: 2304. 01008, 2023.
- 50 LIANG T, GLOSSNER J, WANG L, et al. Pruning and quantization for deep neural network acceleration: A survey [J]. *Neurocomputing*, 2021, 461: 370–403.
- 51 ZHU F, ZHU Y, CHANG X, et al. Vision-language navigation with self-supervised auxiliary reasoning tasks [C] // *Proceedings of the IEEE/CVF conference on computer vision and pattern*

- recognition. 2020: 10012–10022.
- 52 RANE N. Transformers in Intelligent Architecture, Engineering, and Construction (AEC) Industry: Applications, Challenges, and Future Scope [C] //Engineering, and Construction (AEC) Industry: Applications, Challenges, and Future Scope (October 24, 2023). 2023.
- 53 AMOROSO D, TAMBURRINI G. Autonomous weapons systems and meaningful human control: ethical and legal issues [J]. Current Robotics Reports, 2020, 1: 187–194.
- 54 ANDERSON K, WAXMAN M C. Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can [J]. Ssrn Electronic Journal, 2013.

视觉语言大模型在网络舆情分析领域的应用：潜力与挑战

刘晓亮¹ 马 壮¹

摘要 文章提出了视觉语言大模型（LVLMs）在网络舆情分析中的应用，强调其在跨模态分析、行为意图识别和决策支持方面的优势。分析了 LVLMs 在实际应用中的技术挑战，包括隐私保护、模型偏见、技术限制和伦理法律问题，并提出相应解决方案。文章展望了 LVLMs 在提升舆情分析精度、响应速度和自适应学习能力方面的未来发展，指出其在智能监控和预警系统中的潜在作用，为网络舆情分析提供了新的视角和解决方案。

关键词 视觉语言大模型，网络舆情分析，多模态数据，跨模态分析，行为识别，决策支持系统，数据隐私，伦理问题

The Application of Visual Language Large Models in the Field of Network Sentiment Analysis: Potential and Challenges

LIU Xiao-Liang¹ MA Zhuang¹

Abstract The application of Large Vision-Language Models (LVLMs) in network sentiment analysis has been proposed, highlighting their advantages in cross-modal analysis, behavior and intent recognition, and decision support. The technical challenges of LVLMs in practical applications have been analyzed, including privacy protection, model bias, technological limitations, and ethical and legal issues, with corresponding solutions offered. The research prospects for the future development of LVLMs in improving the accuracy, response speed, and adaptive learning capabilities of sentiment analysis have been outlined, pointing to their potential role in intelligent monitoring and early warning systems, providing new perspectives and solutions for network sentiment analysis.

Key words large vision language models, network sentiment analysis, multimodal data, cross-modal analysis, behavior recognition, decision support systems, data privacy, ethical issues

0 引言

近年来，随着人工智能技术的迅猛发

展，视觉语言大模型（Large Vision-Language Models, LVLMs）逐渐崭露头角，并在各个领域展示出广泛的应用潜力。这种大模型相比于传统的语言模型，增加了图像

1. 国防大学政治学院

1. Political College of National Defence University PLA China

处理与图文对齐的能力，能够对多模态数据进行信息提取和理解，从而在计算机视觉、自然语言处理等领域取得了显著的成果。例如，OpenAI 的 GPT-4V^[1] 和 DeepMind 的 Gemini^[2] 模型能够处理包括文本和图像在内的多种输入形式，极大地扩展了人工智能的应用范围。

而在网络舆情分析领域，信息的多样性和复杂性对舆情分析工具提出了更高的要求。传统的网络舆情分析方法主要依赖于文本数据的处理，然而随着信息来源的多样化，图像、视频等非文本数据的比例不断增加。如何高效地处理和分析这些多模态数据，成为当前网络舆情分析领域亟待解决的问题。在这种背景下，LVLMs 的引入，为网络舆情分析提供了一种新的解决方案，具有重要的研究意义和应用前景。

本文旨在探讨 LVLMs 在网络舆情分析中的应用潜力，以及在实际应用中可能遇到的挑战。通过对现有 LVLMs 的技术原理和应用案例进行分析，揭示 LVLMs 在网络舆情分析中的优势和不足，并提出相应的解决方案和未来的发展方向。

本文将首先介绍 LVLMs 在网络舆情分析中的潜力，探讨其在跨模态分析、行为和意图识别以及决策支持等方面的优势；其次，通过具体的应用场景分析，展示 LVLMs 在战场监控、数据筛选和事件预测中的实际应用效果；再次，本文将深入探讨 LVLMs 在网络舆情分析中面临的技术挑战和实践难题，并提出相应的解决方案；最后，对 LVLMs 在网络舆情分析领域的未来发展进行展望，探讨其可能的发展趋势和研究方向。通过上述内容的探讨，本文希望为 LVLMs 在网络舆情分析领域的应用研究提供有益的参考和启示。

1 视觉语言大模型概述

1.1 定义和原理

视觉语言大模型巧妙地结合了计算机视觉和自然语言处理领域的技术，使其成为能够同时处理和理解视觉（图像、视频）和语言（文本）数据的人工智能模型。这种模型通过整合视觉和语言信息，能够在多模态数据中进行信息提取、理解和生成。其核心原理在于利用深度学习技术，尤其是卷积神经网络（CNN）和 Transformer 架构，对图像和文本进行特征提取，并在多模态空间中进行融合和推理。

如图 1 所示，LVLMs 通常由三个核心部件组成：预训练的视觉编码器、视觉语言适配器以及预训练的大语言模型。视觉编码器首先从输入图像中提取视觉特征，这些视觉特征经过视觉语言适配器的转换后被对齐到大语言模型的嵌入空间，最终大语言模型负责融合视觉与文本信息，并利用其强大的世界知识和推理能力完成多模态信息理解并生成精准的文本响应。通过这种方式，LVLMs 能够实现对复杂多模态信息的高效处理和理解。

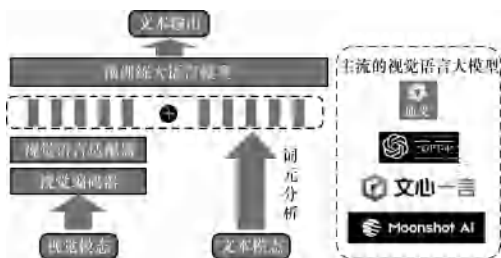


图 1 视觉语言大模型概览图

1.2 主要模型介绍

自 2022 年谷歌研究出的 Flamingo^[3] 大

模型问世以来，LVLMs 领域便迎来了前所未有的快速发展。目前，业界已经开发出了多种具有代表性的 LVLMs，例如：

GPT-4V^[1]：是 OpenAI 推出的 GPT-4 模型的视觉扩展版本，是当前最火热的视觉语言大模型之一。该模型能够处理包括图像和文本在内的多种输入形式。在文本生成的基础上，GPT-4V 引入了图像处理能力，使其能够在多模态数据中进行信息提取和理解。GPT-4V 通过对图像和文本的联合训练，实现了多模态数据的无缝融合和推理，广泛应用于图像描述生成、视觉问答等任务中。

通义千问^[4]：是由阿里巴巴集团旗下的云端运算服务的科技公司阿里云开发的视觉语言大模型，能够与人交互、回答问题及协作创作，主要应用于中文和英文的自然语言处理任务。该模型具有超大规模的参数量，最新版本通义千问 2.0 在多个权威测评中显示出超越 GPT-3.5 的性能，接近 GPT-4 的水平。

文心一言：是由百度开发的一款大规模视觉语言大模型，主要用于多模态生成和自然语言处理任务。该模型的开发基于百度的 ERNIE 系列知识增强大模型和大规模开放域对话模型 PLATO，结合了多项核心技术，包括有监督精调、人类反馈强化学习（RLHF）、提示构建、知识增强、检索增强和对话增强技术。

KIMI：是由中国初创公司 Moonshot AI 开发的一款大型语言模型聊天机器人，旨在处理和生成类人文本响应。作为一款先进的视觉语言模型（LVLMs），KIMI 能够通过结合视觉和语言信息来执行多种任务，包括文本生成和视觉数据处理。其最大特点在于拥有超过 200 万字的上下文窗口，从容应对长文本内容的挑战。

这些代表性模型的问世，不仅展现了

LVLMs 在多模态数据处理中的强大能力，也为进一步的研究和应用奠定了坚实的基础。

2 视觉语言大模型在网络舆情分析中的潜力

在现代战争和军事策略制定中，LVLMs 结合决策支持系统（DSS）为网络舆情分析提供了革命性的改进。这种技术集成不仅极大提高了舆情分析的准确性、及时性和相关性，而且通过深度整合多模态数据，赋予军事指挥官前所未有的洞察力和决策能力^[5]。LVLMs 从战场监控到战术决策制定，从行为和意图识别到长期趋势分析，都显示出其前所未有的潜力。随着技术的进一步发展和优化，可以预见，LVLMs 将在未来的舆情分析和网络安全领域中发挥更加关键的作用，不仅提高军事操作的效率和响应速度，也为战略规划和国家安全提供坚实的技术支持。这种能力展现了在复杂和快速变化的全球安全环境中，如何利用高级分析工具保持战略优势的重要性。

2.1 跨模态分析技术

在现代战争的复杂环境中，综合网络舆情分析显得尤为重要，特别是当应用跨模态分析技术时，其潜力得到极大的发挥。跨模态分析技术通过整合来自不同类型的数据信息，包括图像、短视频、长短文等综合交错的开源信息，构建一个全面、多维的舆情态势图^[6]。这种多源数据融合不仅极大增强了网络舆情分析的准确性和时效性，还使得网络战士能够获得全局舆论场的宝贵信息，同时能够监测立场变化和舆情走向，为舆情战术决策提供实时的数据支持。

跨模态分析技术能够有效地识别和解析社交媒体平台上发布的多媒体内容。在现代社交媒体中，用户不仅发布文字内容，还分享大量的图片和视频。这些视觉内容往往包含丰富的信息，如情绪表达、事件现场以及品牌或人物的形象等。传统的文本分析方法难以充分捕捉这些信息，而视觉与文本相结合的跨模态分析技术则能够将图像中的信息与文本内容进行融合，从而提供更为全面的舆情分析。例如，在一个突发事件中，分析图像和视频可以帮助了解事件的实际情况和影响范围，而文本分析则可以揭示公众的情绪和观点^[7]。

这种技术能够更准确地检测和理解多模态数据中的情感和情绪。网络舆情分析的一个重要任务是监测公众情绪的变化。通过结合视觉和文本数据，跨模态分析技术能够更精确地识别情绪。例如，通过分析表情图片、视频中的肢体语言以及配套的文字评论，系统可以更好地判断用户的情感状态。这对于及时发现和应对潜在的舆情危机具有重要意义。

此外，跨模态分析技术还可以提升信息的关联和理解能力。在网络舆情中，信息的来源和传播路径复杂多样，通过单一模态进行分析往往无法全面捕捉信息的关联性。而通过结合图像和文本，系统可以更好地理解信息之间的关联。例如，用户在发布有关某一事件的文字时，往往会附上相关的图片，通过分析图片和文字的关联性，系统可以更准确地理解事件的背景和用户的真实意图。

而最后，跨模态分析技术在舆情预测和趋势分析中也具有显著优势。通过对多模态数据的综合分析，系统可以更好地预测舆情的发展趋势。例如，通过分析一段时间内的图像和文本数据，可以发现公众关注点的变化，从而提前采取措施应对可

能的舆情危机。

总而言之，视觉与文本相结合的跨模态分析技术通过提供更全面的信息、更准确的情感分析、更强的信息关联理解能力以及更有效的舆情预测能力，在网络舆情分析中发挥了重要作用。这种技术的应用不仅提升了舆情分析的深度和广度，还为相关决策提供了更为坚实的数据支持。

2.2 行为和意图识别技术

在行为和意图识别方面，LVLMs 在情报分析中的应用显现出卓越的能力。这些模型通过深度学习算法能够自动化识别并解释复杂的网民行为模式，为网络安全和舆论监控场景提供高级的预警和决策支持。例如，模型能够从多模态帖子内容中分析人群动态，快速识别潜在的抗议活动、集会或其他公共事件。

在社交媒体环境中，用户的行为和意图往往通过多种形式表达，包括文字、图片和视频等。单一的文本分析方法难以全面捕捉用户行为和意图中的所有信息，而视觉与文本相结合的技术能够弥补这一不足。例如，通过分析社交媒体上的图片和视频，系统可以识别出用户的具体行为，如集会、游行或其他活动。同时，文本分析可以解析用户发布的文字内容，了解他们的观点、情感和意图。结合这两种数据，系统能够全面、深入地理解用户的实际行为和背后动机。

这一技术在情感和意图识别方面表现尤为突出。通过分析用户在社交媒体上发布的图片和视频，系统可以识别出用户的面部表情、肢体语言等情感线索。同时，文本分析技术可以提取文字中的情感词汇和语义信息，综合这两方面的数据，系统能够准确判断用户的情感状态和意图。例如，在一场公共事件中，用户发布的图片

可能显示愤怒或悲伤的表情，文本内容则可能包含对事件的评论和观点。通过结合这两种信息，系统可以更准确地了解公众的情绪反应和态度，从而及时识别潜在的舆情危机^[8]。

此外，视觉与文本相结合的行为和意图识别技术还能够提升信息的关联和理解能力。在网络舆情分析中，不同信息之间的关联性和上下文理解非常重要。通过将图像和文本数据结合，系统可以更好地理解信息之间的关联。例如，用户在发布与某事件相关的文字时，通常会附上相关图片，通过分析这些图片和文字的关联，系统可以更全面地了解事件的背景和用户的真实意图。这种多模态信息的结合不仅能够提升分析的准确性，还能够提供更深入的见解和洞察。

在舆情预测和趋势分析方面，这种技术也展现了显著优势。通过对大量图像和文本数据的综合分析，系统可以识别出潜在的舆情热点和趋势。例如，通过分析社交媒体上的图片和文字，可以发现公众关注的焦点和话题变化，从而提前预警潜在的舆情危机。这样的预测能力对于相关部门及时应对舆情、制定有效的应对策略具有重要意义。

视觉与文本相结合的行为和意图识别技术通过全面解析用户行为和意图，提供更精准的情感和意图识别、更强的信息关联理解能力以及更有效的舆情预测能力，在网络舆情分析中发挥了关键作用。这种技术的应用不仅提升了舆情分析的深度和广度，还为相关决策提供了坚实的数据支持，有助于更好地理解和应对复杂的网络舆情环境。

2.3 决策支持能力

在军事情报分析领域，LVLMs 与决策

支持系统（DSS）的结合展现出显著的潜力，特别是在增强舆情分析的精确性、及时性和相关性方面。这些系统通过综合视觉数据和其他模态的信息，为决策者提供了更加全面和深入的分析，帮助他们做出更明智和有效的策略和战术决策^[9]。

LVLMs 在舆情分析领域中提升了决策支持系统的效能，特别是通过其增强的情境感知能力和复杂数据集成分析能力。这些模型能够从多个数据源——如图像、视频、文本、音频和传感器数据中——提取信息，形成一个多维度的网络舆情视图。在实时监控敏感区域时，模型能识别潜在的安全威胁或非法活动，并迅速整合这些信息，提供全面的情报视图，加快响应速度，使决策者能基于完整的数据做出迅速而有效的反应。

此外，LVLMs 还支持决策过程的自动化和优化，通过先进的算法自动推荐或生成决策选项，特别是在处理大规模数据和复杂战场环境时。这种自动化能减少人为错误，加速决策流程，确保在关键时刻提供快速且可靠的响应。例如，在舆情灾害响应中，模型能自动分析受影响的网络区域的损害情况，并提出最佳的引导策略和资源分配方案。

综上所述，LVLMs 在网络舆情管控系统中的应用不仅改善了操作效率和战术执行的质量，还提供了快速、精确的决策支持，显著提升了舆论引导和战略决策的整体质量，为现代军事网络作战提供了关键的技术支持，优化了整个决策过程，并在保障国家安全和有效执行网络整改行动中发挥了至关重要的作用。

3 应用场景分析

视觉语言大模型通过结合图像和文本

信息，能够提供更加准确和全面的舆情分析支持。本节将从舆情监测与预警、情感分析与情绪识别以及事件识别与追踪三个方面，介绍 LVLMs 在网络舆情分析中的应用。

3.1 舆情监测与预警

在未来作战中，陆、海、空、天、电等多域作战空间所产生的信息洪流，对舆情监测与预警提出了更高要求^[10]。针对这一挑战，LVLMs 展现出了强大的可应用能力。其能够对来自不同传感器和信息源的多模态数据进行整合，并实时监测舆情动态与舆论走向，提供全面而细致的全局舆论场图景，并针对危险的舆论场进行预警。

在现代社交媒体环境中，信息传播速度极快，传统的单一文本分析方法难以全面捕捉和解析多样化的数据形式。LVLMs 通过整合文本、图像和视频等多模态数据，为舆情监测和预警提供了更为精准的手段。这种技术能够实时收集和分析海量的社交媒体内容，通过图像识别技术解析事件现场的视觉信息，结合文本分析揭示公众的情感和观点，从而形成全面的舆情图景。

在突发事件中，LVLMs 能够快速识别并追踪事件的动态发展。通过对实时视频和图像的分析，系统可以迅速了解事件的具体情境和影响范围，及时捕捉公众的反应和情绪变化。与此同时，文本分析技术能够解析社交媒体上的评论和讨论，提取关键信息并进行情感分析，从而准确评估事件的潜在影响和公众情绪的走向。结合多模态数据的综合分析，决策者可以获得更为全面的舆情预警信息，提前采取应对措施，有效防范潜在的舆情危机。

3.2 情感分析与情绪识别

LVLMs 通过其强大的数据处理能力，

可以高效筛选和分析多源数据，包括但不限于图像处理、文本分析、视频理解等^[11]。在网络舆情分析中，情感和情绪的识别是理解公众反应和预测舆情走势的关键。视觉语言大模型通过融合视觉和文本信息，显著提升了情感分析和情绪识别的准确性。通过分析用户发布的图片和视频，系统能够识别面部表情、肢体语言等视觉情感线索，并结合文本中的情感词汇和语义信息，全面解析用户的情感状态。

例如，在社交媒体上的某一事件讨论中，用户上传的图片可能显示愤怒或悲伤的面部表情，视频中的肢体语言也可能传递出强烈的情绪信号。视觉语言大模型通过对这些视觉信息的解析，结合用户的文字评论，能够准确识别出他们的情感状态和态度。这种多模态情感分析技术不仅提高了情感识别的准确性，还能够捕捉到单一模态分析难以察觉的细微情感变化，从而为舆情分析提供更深入的见解。

3.3 事件识别与追踪

在复杂的网络舆情环境中，事件的识别与追踪是舆情分析的重要任务。LVLMs 通过融合多模态数据，提供了强大的事件识别与追踪能力。通过对社交媒体上的图像和视频进行分析，系统可以识别出与事件相关的视觉信息，如地点、人物和具体活动等，并将这些信息与文本数据进行关联，全面解析事件的背景和发展过程。

例如，在军事领域的舆情分析中，战场图片和视频常常包含关键的视觉信息。视觉语言大模型可以通过分析这些图像，识别出具体的军事行动、装备和人员，并结合相关的文字报道，全面了解事件的背景和具体细节。这种多模态数据的融合分析，使得系统不仅能够识别单一的信息，还能够理解信息之间的关联和上下文，从

而提供更为准确和深入的事件追踪。

经过历史数据的微调和基于真实或仿真场景的强化学习^[12]，LVLMs可以通过结合历史数据和实时信息，对未来事件进行精准预测。通过对大量图像和文本数据的综合分析，LVLMs还能够识别出事件的发展趋势和潜在的舆情热点。例如，通过长时间的多模态数据监测，系统可以发现公众关注的焦点和话题变化轨迹，及时预警潜在的舆情危机。这种事件识别和追踪能力，为决策者提供了全面、准确的信息支持，使其能够更好地理解和应对复杂的舆情环境。

除此之外，模型的设计和训练还可以借鉴军事理论中的成熟思想，如可以结合联合全域指挥与控制（Command and Control, C2）的相关概念^[13]，运用体系C2过程机理，从筹划-准备-执行-评估（Planning-Readiness-Execution-Assessment, PREA）环的角度对模型进行强化训练，以支持模型在网络舆情分析中的准确性和可解释性。

4 面临的挑战和解决方案

网络舆情分析在现代社会中扮演着至关重要的角色，但同时也面临着多重挑战。在隐私与安全方面，网络舆情分析必须确保收集和处理的 data 受到严格保护，避免信息泄露和滥用。针对模型偏见与公共性问题，需要警惕 LVLMs 可能带来的偏见，确保分析结果客观公正，并考虑其对公共利益的影响。技术局限性与发展则要求正视技术局限性，同时关注技术发展带来的新挑战。此外，伦理与法律问题也是网络舆情分析不可忽视的方面，必须确保网络舆情分析符合伦理标准并遵守相关法律法规。为了应对这些挑战，

需要建立严格的隐私保护机制，加强算法和模型的审核与监管，推动技术创新和应用，以及加强伦理和法律教育，确保网络舆情分析在维护国家安全、促进公共利益的同时，也能保护个人隐私、维护社会公正。

4.1 数据隐私与安全

在网络舆情分析中，数据隐私与安全的重要性不言而喻。这些数据不仅涉及国家机密和军事战略，还直接关系到国家的安全和稳定。因此，确保网络舆情分析中的数据隐私与安全，是军事领域必须面对和解决的重大问题。网络舆情数据中包含了大量敏感信息，这些信息一旦泄露，将对国家造成巨大的损失。同时，黑客攻击、病毒和恶意软件、内部人员泄露等，都是网络舆情数据可能面临的威胁。而且，网络舆情分析需要处理大量的数据，包括结构化数据和非结构化数据，这要求网络舆情数据的处理和分析系统必须具备高度的安全性和可靠性。例如，在使用 GPT 进行舆情分析时，有用户发现，通过输入特定的“神秘代码”或关键词组合，GPT 竟然能够“泄露”出某些个人的敏感信息，如电话号码、住址和邮箱等。这些信息原本只是作为训练数据被 GPT 吸收，但在特定条件下被意外输出。对此的解决方案是加强数据隐私保护措施，确保训练数据在使用过程中得到严格的安全控制。同时，对 LVLMs 的输出结果进行严格的审查与过滤，防止敏感信息的泄露。此外，开发更加先进的隐私保护算法，如差分隐私、数据脱敏处理等，以降低数据泄露的风险^[14]。

随着技术的发展和威胁的演变，保护数据安全的方法和技术也在不断更新和完善。以下将从数据、算法、系统、制度四

方面展开介绍。

对于不同级别的数据，应设置不同的访问权限，通过身份验证、授权和审计等手段，严格控制对网络舆情数据的访问权限，确保只有经过授权的人员才能访问敏感数据。除此之外，采用数据脱敏手段能够帮助在保护个人隐私的同时，有效地进行舆情分析，提供有价值的信息洞察。数据脱敏涉及识别并标记数据集中的敏感信息，随后运用诸如替换、加密、哈希、模糊化或泛化等脱敏方法来处理这些敏感数据。数据脱敏技术的关键在于，脱敏过程需精心设计，以确保数据的统计特性和语义关系得以保留，从而使舆情分析的结果既准确又具有代表性。

从算法角度，可以对军事机密信息使用高强度的加密算法进行加密处理，确保数据在传输和存储过程中的安全，加密技术的应用范围应涵盖所有涉及机密信息的领域，包括网络通信、数据存储等。差分隐私是一种先进的隐私保护措施，它通过在原始数据上添加精心设计的随机噪声，使数据分析结果对任何单个记录的存在与否变得不敏感，从而在保护个人隐私的同时，支持有效的舆情分析。在舆情分析场景下，即使数据包含了敏感信息，差分隐私也能确保分析者无法从最终的统计结果中反推出个体的具体情况。这种技术通过严格的数学框架确保了隐私泄露的风险被控制在一个可接受的范围内，允许研究人员和分析师在不侵犯个人隐私的前提下，对大规模数据集进行聚合查询和模式挖掘，获取关于公众情绪和舆论趋势的宝贵见解。

相关部门还需要建立完善的网络安全防护体系，包括防火墙、入侵检测系统、安全事件管理系统等，及时发现和应对网络安全威胁，加强网络安全监测和预警，

确保网络环境的稳定和安全^[6]。

除此之外，相关的审查制度和教育对保障网络舆情数据的隐私与安全也至关重要。对从事网络舆情分析工作的人员进行严格的政治审查、业务考核和心理素质测试，确保他们具备从事保密工作的能力和素质；加强保密意识教育，提高全体人员的保密意识和敌情观念。对涉密计算机、通信设备等实行严格的管理和控制，防止信息泄露，包括限制设备的访问权限、定期检查和更新设备的安全设置、防止非法入侵和恶意攻击等。对网络舆情数据的生成、处理、传输、存储等全过程进行审计，确保信息安全可控，审计制度应涵盖信息的各个环节，及时发现和纠正信息安全问题。复制军事秘密载体应严格履行相应审批手续，任何个人不得私自留存或者擅自处理，严禁将涉密信息上传至互联网或通过其他途径进行传播，以防止信息泄露等。

通过上述措施的综合运用，可以在相当大程度上保障网络舆情分析中的数据隐私与安全。然而，随着技术的不断发展和数据隐私威胁的演变，保护数据安全的方法和技术也需要不断更新和完善。因此，军事组织需要持续投资于最新的安全技术和人才培养，以保持其数据安全防护的先进性和有效性。

4.2 模型的偏见与公平性

模型偏见与公平性在 LVLMS 中是一个至关重要的议题^[15]。在网络舆情分析领域，LVLMS 的引入为处理和分析包含图像与文本的数据提供了强大的工具。然而，这些模型在处理多模态数据（如图像和文本）时，可能会继承或放大训练数据中的偏见，从而对网络舆情分析产生负面影响。这些偏见大多来源于训练数据偏见、

标注偏见以及视觉编码器偏见等。训练数据偏见体现在由于训练数据的不完整、不准确或不具有代表性，导致模型存在偏见。例如，如果训练数据中的图像和文本主要来源于某一特定文化或地区，那么模型可能会对这些文化或地区产生偏好，而对其他文化或地区产生偏见。标注偏见指的是在标注过程中，标注者可能会受到自身背景、经验和主观判断的影响，导致标注结果存在偏见。这种偏见会被模型学习并放大，从而影响模型的预测结果。而视觉编码偏见是由于视觉语言大模型通常使用预训练的视觉编码器（如 CLIP）将图像转换为文本表示。然而，这些编码器可能存在对特定视觉特征的偏好或偏见，导致模型在处理某些图像时产生偏差^[16]。

如果 LVLMs 在网络舆情分析中存在偏见，那么它们可能会提供不准确或误导性的信息，从而影响决策的准确性，误导决策。例如，模型可能过度关注某些特征而忽略其他重要信息，或者对某些群体或主题产生不公正的评价。偏见问题可能导致网络舆情分析中对不同群体或主题的评估存在不平等，加剧不平等。例如，某些群体可能因为其图像或文本数据在训练数据中的不足而被忽视或低估，而其他群体则可能因为其数据在训练数据中的过度代表而被过度强调。这种不平等可能加剧社会不公和歧视问题^[17]。例如，在使用“文心一言”进行情报分析时，有研究人员发现该模型在某些问题上存在明显的偏见。在回答关于性别平等或种族歧视的问题时，模型也可能会给出带有偏见的回答。这些偏见可能源自于训练数据中的不平衡或偏见性内容。

对于 LVLMs 偏见的评估可以分为两种主要方式：模型的内部表征偏差以及模型在下游任务中体现的外部偏差。模型的内

部偏差是指大模型的输出表示中存在的偏差，与具体任务无关，常用样本嵌入表示的差异来衡量模型的内部偏差，常见方法有两类：基于相似度的衡量以及基于概率分布的衡量。前者通过比较表示在不同敏感属性群体间的相似性差异（如余弦相似度）来发掘隐藏其中的偏见，而后者则通过计算模型在数据集上得出的候选项的概率分布差异来衡量其中的偏见。相较之下，模型的外部偏差则是指模型经过微调或提示等手段适配特定的下游任务时产生的偏差，可以通过特定下游任务输出的性能差距来衡量。可以通过一些常见的公平性指标来衡量，如统计平衡性指标（Statistical/Demographic Parity）衡量不同敏感属性群体的预测正例率的差值。针对舆情分析的场景，还检查模型的结果是否全面覆盖了各群体的视角，确保情感表达的平衡，以及主题讨论的平等性，防止任何群体的意见被放大或忽视。此外，还需要考察模型的语境敏感性以解读跨文化的语言差异。

面对 LVLMs 在网络舆情分析中存在的偏见，应积极探索兼顾性能和公平的训练和推理方式，并采取适当的应对措施，最大程度上确保网络舆情分析的准确性和公正性。从模型本身出发，考虑到 LVLMs 的大规模参数和训练成本，有研究从推理阶段入手，尝试通过修改相应的解码策略来减少生成内容中的偏见。如可以通过限制生成某些有害或是有偏见的内容，采用束搜索、对数抑制和温度采样等方式鼓励一些低频词汇的生成以增加结果的多样性，避免陷入刻板印象。除此之外，可以通过收集和整理来自不同群体、文化和社会背景的多样化训练数据，减少模型中的偏见。设计透明、可解释的算法，使得人们能够理解模型是如何工作的，从而更

容易识别和纠正模型中的偏见。对 LVLMS 进行定期的审计和监管，以确保其符合公平性和无偏见的要求。对用户进行教育和培训，使其了解 LVLMS 可能存在的偏见问题，并教会他们如何识别和处理这些问题。建立健全的监管机制和评估体系，对视觉语言大模型进行定期评估和监督。及时发现和纠正模型中的偏见和错误，确保其在网络舆情分析中的准确性和公正性。

综上所述，视觉语言大模型在网络舆情分析中的应用具有巨大的潜力，但同时也需要关注其可能存在的偏见问题。通过采取适当的应对策略，最大限度地减少偏见对网络舆情分析的影响，确保网络舆情分析的准确性和公正性。

4.3 技术限制与发展

网络舆情分析是一个复杂且不断发展的领域，它依赖于先进的技术工具和方法来提取、处理、分析和解释大量的信息。然而，当前的技术在网络舆情分析领域仍存在一定的局限性，同时也展现出了未来的发展方向。例如，在金融科技行业中，某家大型银行利用 GPT 模型进行金融市场的舆情分析，旨在监测市场动态、评估投资者情绪以及预测潜在风险。然而，在实际应用过程中，银行发现 GPT 模型在处理该行业特有的复杂金融数据、专业术语以及深度分析方面存在显著的技术限制。技术局限性方面，随着信息时代的到来，数据量呈爆炸式增长，传统的数据处理方法已难以满足网络舆情分析的需求。如何从海量的数据中提取有价值的信息，是当前技术面临的一大挑战。网络舆情信息来源广泛，包括文本、图像、视频、音频等多种形式。如何有效地整合这些不同形式的信息，实现跨媒体的信息融合，是当前技

术需要解决的问题。尽管自然语言处理（NLP）技术取得了显著进展，但在复杂的语境和语义理解方面仍存在不足。这可能导致网络舆情分析中的误解或遗漏。虽然人工智能（AI）在网络舆情分析中的应用越来越广泛^[18]，但 AI 系统仍难以完全替代人类分析师的直觉和判断。此外，AI 系统的训练数据可能存在偏见，这会影响其分析结果的准确性。未来发展方向方面，未来的网络舆情分析将更加注重跨媒体信息融合，通过整合不同形式的信息，提高分析的全面性和准确性。未来的网络舆情分析将也更加注重人机协同，通过结合人类分析师的直觉和判断与 AI 系统的数据处理能力，实现更高效、更准确的网络舆情分析。随着数据量的不断增长和网络舆情分析技术的不断进步，数据安全和隐私保护将成为未来网络舆情分析领域的重要议题。未来的技术将更加注重保障数据的安全性和隐私性，防止数据泄露和滥用。总之，网络舆情分析领域的技术限制和发展方向是相互关联的。随着技术的不断进步和创新，未来的网络舆情分析将更加高效、准确和全面。同时，也需要关注技术发展中可能带来的问题和挑战，并采取相应的措施加以解决。

4.4 伦理与法律问题

在网络舆情分析中使用视觉语言大模型可能引发伦理和法律问题。有关伦理问题方面^[19]，首先，就个人隐私而言，视觉语言大模型在处理图像和自然语言文本时，可能会涉及个人隐私信息的泄露。例如，在图像识别过程中，如果模型能够识别出个人的面部特征、衣着、行为等，那么这些信息就有可能被用于不正当的用途，如身份盗窃、跟踪监视等，从而侵犯个人隐私权。其次，如果视觉语言大模型

的训练数据存在偏见或歧视，那么模型在进行网络舆情分析时也可能产生类似的问题。例如，模型可能基于肤色、性别、种族等特征对个体进行不公平的判断或分类，从而导致歧视现象的发生。最后，视觉语言大模型能够处理和生成大量的信息，但如果这些信息被用于不正当的用途，如传播谣言、煽动仇恨等，就可能对社会造成负面影响。此外，如果模型被用于窥探他人隐私或进行非法监视，也可能引发严重的伦理问题。有关法律问题，一方面，在训练视觉语言大模型时，可能需要使用大量的图像和文本数据。如果这些数据的来源不明确或存在侵权行为，就可能引发知识产权纠纷。此外，如果模型生成的图像或文本被用于商业用途而未获得原作者的许可，也可能构成侵权行为。另一方面，在处理和析图像和文本数据时，可能涉及敏感信息的泄露和滥用。这些信息可能包括个人隐私、商业秘密等，如果未能得到妥善保护，就可能违反数据保护法规。此外，当视觉语言大模型在网络舆情分析中出现错误或造成损失时，如何确定责任归属是一个重要的问题。由于模型的工作方式复杂且难以预测，因此，很难确定是由模型本身的问题还是由使用者的问题导致的损失。例如，针对模型本身的问题，一家媒体机构在利用文心一言生成新闻报道的摘要时，发现模型在某些情况下会生成误导性信息或夸大事实的描述。这些信息一旦被传播出去，就可能引发公众误解、社会恐慌甚至法律纠纷。

为了应对这些伦理和法律问题，有必要采取一定措施。例如，确保在收集、存储和使用图像和文本数据时遵守相关的数据保护法规，并采取必要的技术和管理措施来保护数据的安全性和隐私性。在使用图像和文本数据时，应确保数据来源的合

法性和合规性，并尽可能获得原作者的许可或遵循相关的版权法规^[20]。对视觉语言大模型进行严格的监管和评估，确保其符合伦理和法律要求，并及时发现和纠正模型中存在的问题。在使用视觉语言大模型进行网络舆情分析时，应明确责任归属机制，确保在出现问题时能够及时追责和解决问题。

5 未来展望

随着技术的迅猛发展，视觉语言大模型在网络舆情分析领域展现出了广阔的应用前景和发展潜力。首先，多模态融合的深化将极大提升网络舆情分析的精度和效率。未来的视觉语言大模型将能够更加高效地整合图像、文本、音频和视频等多种数据形式，实现信息的全面整合和综合分析。这将为网络舆情分析提供更全面和深入的洞察，使决策过程更加科学和精准。此外，实时分析与推理能力的提升也将显著增强网络舆情分析的响应速度和决策能力。通过利用更强大的计算能力，这些模型将能够实时处理和分析大规模数据，支持即时决策。这在军事和安全等高风险领域尤为重要，能够大大提高响应速度和应对能力。同时，自适应学习能力的增强也是未来视觉语言大模型的重要发展方向。未来的模型将能够根据不同情境和需求自动调整其分析策略和方法，提高模型的灵活性和适应性。这将使得网络舆情分析更加灵活和高效，能够应对不断变化的网络舆情需求和复杂多变的网络舆情环境。最后，视觉语言大模型还将推动智能监控和预警系统的发展。通过实时分析视频和传感器数据，模型能够识别潜在威胁和异常行为，及时预警和采取措施，防止安全事件的发生。这将极大提升公共安全和国家

安全的防护能力。

通过不断的技术创新和应用探索，视觉语言大模型在网络舆情分析领域的未来前景将更加广阔，其技术优势和应用价值也将得到充分体现。

参考文献

- 1 ACHIAM J, ADLER S, AGARWAL S, et al. Gpt-4 technical report [J]. arXiv preprint arXiv: 2303. 08774, 2023.
- 2 TEAM G, ANIL R, BORGEAUD S, et al. Gemini: a family of highly capable multimodal models [J]. arXiv preprint arXiv: 2312. 11805, 2023.
- 3 ALAYRAC J B, DONAHUE J, LUC P, et al. Flamingo: a visual language model for few-shot learning [J]. Advances in neural information processing systems, 2022, 35: 23716-23736.
- 4 BAI J, BAI S, YANG S, et al. Qwen-vl: A frontier large vision-language model with versatile abilities [J]. arXiv preprint arXiv: 2308. 12966, 2023.
- 5 柯灵. 基于人工智能的信息安全威胁情报分析研究 [J]. 信息与电脑 (理论版), 2024, 36 (4): 229-231, 235.
- 6 谭小伟. 基于人工智能的网络威胁情报分析与网络信息安全防护体系研究 [J]. 信息记录材料, 2023, 24 (12): 59 - 61. DOI: 10. 16009/j. cnki. cn13-1295/tq. 2023. 12. 005.
- 7 陈明, 汤文娟. 智能化条件下网络威胁情报分析研究 [J]. 情报杂志, 2023, 42 (3): 8.
- 8 王小光. 人脸识别技术应用于侦查情报分析的偏差控制 [J]. 情报杂志, 2023, 42 (4): 50-56.
- 9 贾莹. 大数据背景下情报分析预测系统构建研究 [J]. 信息与电脑 (理论版), 2020, 32 (14): 43-46.
- 10 沈弼龙. 大模型技术的军事应用 [EB/OL]. http://www.81.cn/zt/2023nzt/flsxjbnmbjkcsjyljd/esdsjyy_244131/16216688.html.
- 11 汲克山, 刘思培, 李清玉, 等. 大模型在军事领域的应用与展望 [C] //中国指挥与控制学会 (Chinese Institute of Command and Control). 第十二届中国指挥控制大会论文集 (下册). 北京: 兵器工业出版社, 2024: 5. DOI: 10. 26914/c. cnkihy. 2024. 006548.
- 12 蔡磊, 孟宪波, 韩冬梅, 等. 大模型在军事垂直领域的应用 [J]. 舰船科学技术, 2024, 46 (5): 171-175.
- 13 易侃, 钟元带, 曾逸凡, 等. 联合全域指挥与控制机理模型及应用分析 [J]. 指挥与控制学报, 2022, 8 (1): 1-13.
- 14 CARLINI N, TRAMER F, WALLACE E, et al. Extracting training data from large language models [C] //30th USENIX Security Symposium (USENIX Security 21). 2021: 2633-2650.
- 15 GALLEGOS I O, ROSSI R A, BARROW J, et al. Bias and fairness in large language models: A survey [J]. Computational Linguistics, 2024: 1-79.
- 16 LIU H, XUE W, CHEN Y, et al. A survey on hallucination in large vision - language models [J]. arXiv preprint arXiv: 2402. 00253, 2024.
- 17 LEAPE L L, PARK R E, BASHORE T M, et al. Research on the Effect, Model and Solution of Intelligence Culture [J]. Journal of Intelligence, 2010, 9 (3): 95-97. DOI: 10. 1016/S1062-1458 (00) 00053-2.
- 18 郭逸彪, 马垒, 陈忻. 人工智能技术在开源情报生产中的实证研究与案例分析 [J]. 无线互联科技, 2024, 21 (8): 56-58.
- 19 王英, 马海群. 情报工作古老而又前沿的维度: 情报伦理的问题缘起、概念与意义情报工作古老而又前沿的维度: 情报伦理的问题缘起、概念与意义 [J]. 现代情报, 2022, 42 (9): 5-17.
- 20 杨倩, 林鹤. 大语言模型背景下情报研究的数字化应对策略及实践场景 [J]. 竞争情报, 2023, 19 (3): 2-13.

通信网络与 AI 大模型的融合发展研究

瞿崇晓¹ 唐宇波² 吴高洁² 范长军^{1*} 张永晋¹ 刘 硕¹

摘要 通信网络与 AI 大模型的融合发展正成为学术界与产业界的研究热点。随着生成式 AI 技术，特别是大模型的突破，研究者们正在深入挖掘 AI 大模型与通信网络的协同潜力。文章综述了 AI 大模型在提升通信网络智能化方面的最新进展，重点探讨了基于 Transformer 架构的大模型如何通过智能化应用优化网络设计、诊断、配置、安全及语言理解等领域，并分析了通信网络如何通过云边协同和多智能体技术支持 AI 大模型的训练与部署。

首先，文章介绍了大模型的基础架构与训练过程，包括自注意力机制、智能涌现机制及其在自然语言处理任务中的卓越表现，并详细分析了大模型在通信网络中的六大应用场景：网络设计、诊断、配置、安全、语言理解和规范分析。通过处理海量数据、生成故障报告、自动配置网络、加强网络安全、理解和映射网络语言以及分析技术规范，大模型极大提升了通信网络的智能化水平。

其次，文章探讨了大模型赋能通信网络领域任务的具体途径，包括预训练与微调、提示工程以及检索增强生成。这些技术手段共同推动了大模型在通信网络智能化中的应用。例如，预训练与微调使大模型能适应特定领域的知识；提示工程通过精心设计的查询输入引导模型生成预期响应；检索增强生成结合大模型与信息检索技术，提升模型的记忆和事实准确性。

此外，通信网络在 AI 大模型的训练、推理和部署中也扮演了关键角色，特别是在数据传输、资源分配、多智能体协同和智能服务提供方面。文章讨论了通过云边协同计算和多智能体网络构建来赋能 AI 大模型，具体探讨了边缘云计算与多智能体协同的优势，以及如何通过分布式计算、云边端协同和多智能体网络等技术手段为用户提供更便捷的智能服务。

最后，文章指出了 AI 大模型与通信网络融合过程中面临的挑战，如大模型的可解释性、通信数据与大模型架构的适配、设备端大模型部署和资源管理等。通过应对这些挑战，将为通信网络与 AI 大模型的融合开辟新的发展路径，实现更智能的通信网络和网络化的通用智能服务。

总体而言，文章揭示了 AI 大模型与通信网络融合的广阔前景，为实现更智能、高效、安全的通信网络提供了理论依据和技术路线，并指出了未来研究的方向，旨在推动通信网络与 AI 大模型的深度融合，共同应对当前和未来的挑战。

关键词 AI 大模型，通信网络，融合与协同，Transformer，云边协同

A Study on the Integrated Development of Communication Networks and Large Language Models

QU Chong-Xiao¹ TANG Yu-Bo² WU Gao-Jie² FAN Chang-Jun^{1*} ZHANG Yong-Jin¹ LIU Shuo¹

Abstract The integration and development of communication networks and large AI models are becoming a focal

* 通讯作者

1. 中国电子科技集团公司第五十二研究所 2. 智能博弈重点实验室

1. The 52nd Research Institute of China Electronics Technology Group Corporation 2. State Key Laboratory of Intelligent Game

point of research in both academia and industry. With breakthroughs in generative AI technologies, particularly largelanguage models (LLMs), researchers are exploring the potential for synergy between LLMs and communication networks. This paper reviews the latest advancements in enhancing the intelligence of communication networks through LLMs, focusing on how models based on the Transformer architecture can optimize areas such as network design, diagnostics, configuration, security, and language understanding through intelligent applications. It also analyzes how communication networks, through cloud-edge collaboration and multi-agent technologies, support the training and deployment of LLMs.

First, the paper introduces the fundamental architecture and training process of LLMs, including the self-attention mechanism, emergent intelligence, and their exceptional performance in natural language processing tasks. It provides a detailed analysis of six major application scenarios for LLMs in communication networks: network design, diagnostics, configuration, security, language understanding, and standard analysis. By processing massive amounts of data, generating fault reports, automatically configuring networks, enhancing network security, understanding and mapping network languages, and analyzing technical standards, LLMs significantly enhance the intelligence level of communication networks.

Next, the paper explores specific approaches for LLMs to empower tasks in the communication network field, including pre-training and fine-tuning, prompt engineering, and retrieval-augmented generation. These techniques collectively drive the application of LLMs in the intelligentization of communication networks. For example, pre-training and fine-tuning enable LLMs to adapt to domain-specific knowledge; prompt engineering guides models to generate desired responses through carefully designed input queries; retrieval-augmented generation combines LLMs with information retrieval technologies, improving the model's memory and factual accuracy.

In addition, communication networks play a key role in the training, inference, and deployment of LLMs, particularly in data transmission, resource allocation, multi-agent collaboration, and intelligent service provision. The paper discusses how LLMs are empowered through cloud-edge collaborative computing and multi-agent network construction, specifically exploring the advantages of edge cloud computing and multi-agent collaboration, and how technologies such as distributed computing, cloud-edge collaboration, and multi-agent networks can provide more convenient intelligent services to users.

Finally, the paper identifies the challenges faced in the integration of LLMs with communication networks, such as the interpretability of LLMs, the adaptation of communication data to LLMs' architectures, deployment of LLMs on devices, and resource management. Addressing these challenges will open new development paths for the integration of communication networks and LLMs, enabling more intelligent communication networks and network-based general intelligent services.

Overall, this paper reveals the broad prospects for the integration of LLMs and communication networks, providing a theoretical foundation and technical roadmap for achieving more intelligent, efficient, and secure communication networks. It also points out directions for future research, aiming to promote the deep integration of communication networks and LLMs to jointly address current and future challenges.

Key words large AI models, communication networks, integration and collaboration, Transformer, cloud-edge collaboration

一种基于知识图谱的检索增强生成情报问答技术**

成志宇¹ 陈星霖² 王 菁³ 周中元⁴ 张志政^{5*}

摘 要 现有的基于文档的 RAG 主要在开放域任务上进行训练和评估。然而，军事领域的知识通常以结构化形式存储，如知识图谱，这使得文档型检索器无法有效检索信息，导致 RAG 在以知识图谱为数据源的知识库中难以获得有效信息，需要探索以知识图谱为数据源的 RAG 方案解决以上问题。此外，军事情报中的多约束问题会导致 RAG 检索时生成大量信息，导致上下文过长，增加成本并影响模型性能，因此，有必要对输入给大语言模型的知识进行精炼。提出了一种基于知识图谱的检索增强生成框架以实现军事情报问答解决上述问题。该框架工作流程主要包括问题分类、实体识别、实体链接、知识检索、知识精炼、问题求解六个阶段。在问题分类阶段使用 K-BERT 作为问题分类的预训练模型，将结构化的军事知识图谱知识融入模型，从而提高对军事领域知识的理解能力和模型的性能。在实体识别阶段提出了 K-BERT-BiLSTM-CRF 模型，在军事命名实体识别数据集上进行训练并用于军事命名实体识别，以检索自然语言问题上的候选实体与属性，为实体链接提供数据基础。在实体链接阶段通过预训练模型将候选实体指称与候选属性指称通过向量相似度计算等方式与知识图谱中的唯一实体和多候选属性对齐，从而获得问题相关实体以及求解相关约束。在预训练模型选择上，使用命名实体识别任务中预训练的 K-BERT-BiLSTM-CRF 模型中 K-BERT 的编码层作为编码器以充分理解军事术语的含义和差异。在知识检索阶段通过兵器类型与实体获取问题相关背景知识，并使用回答集编程进行表示，为问题的求解提供数据基础。框架通过以上四个阶段有效地获取了背景知识。考虑到多约束问题的特点，使用回答集编程设计规则，在知识上通过硬约束与软约束限制来减少知识数量或者直接获得答案。最后，在问题求解阶段，考虑到在军事情报问答中属性指称识别与链接面临隐晦性、模糊性和稀疏性的问题，使用大语言模型在精炼后的知识上对问题进行求解，以减少问题理解过程中的属性识别与链接。在 MiRE 数据集随机抽取每类问题的 5 个样本，涵盖了 23 个不同类别的总计 115 个问题进行实验，框架在检索准确率和问答准确率上均超过 90%。实验结果表明，框架能够提供基于知识图谱的增强知识检索功能，并提供了较好的军事情报问题解答能力。

关键词 情报问答，回答集编程，大语言模型，检索增强生成，知识图谱

** 军科委国防科技重点实验室基金 (6142101210205) 和军科委国防科技创新特区资助项目

** Supported by the Pre-research Key Laboratory Fund for Equipment (Grant No. 6142101210205)

* 通讯作者

1. 东南大学苏州联合研究生院 2. 东南大学软件学院 3. 信息系统工程全国重点实验室 4. 中国电子科技集团公司第二十八研究所 5. 东南大学计算机科学与工程学院

1. Joint graduate school, Southeast University 2. College of software engineering, Southeast University 3. Science and Technology on Information Systems Engineering Laboratory 4. The 28nd Research Institute of China Electronics Technology Group Corporation 5. School of computer science and engineering, Southeast University

An Intelligence Question Answering Technique Based on Retrieval-Augmented Generation^{**}

CHENG Zhi-Yu¹ CHEN Xing-Lin² WANG Jing³
ZHOU Zhong-Yuan⁴ ZHANG Zhi-Zheng^{5*}

Abstract Existing document-based RAG models are primarily trained and evaluated on open-domain tasks. However, knowledge in the military domain is often stored in structured forms, such as knowledge graphs. This makes document-based retrievers ineffective at retrieving information, leading to difficulties for RAG in obtaining relevant information from knowledge bases that use knowledge graphs as data sources. Therefore, it is necessary to explore RAG solutions that utilize knowledge graphs as data sources to address these issues. Additionally, the multi-constraint nature of military intelligence problems can lead to the generation of excessive information during RAG retrieval, resulting in overly long contexts that increase costs and degrade model performance. Hence, it is essential to refine the knowledge input to large language models. A knowledge graph-based retrieval-augmented generation framework is proposed to achieve military intelligence question answering. The workflow of the framework mainly includes six stages: question classification, entity recognition, entity linking, knowledge retrieval, knowledge refinement, and problem solving. In the question classification stage, K-BERT is used as a pre-trained model for question classification, incorporating structured military knowledge graph information into the model to enhance its understanding and performance in the military domain. In the entity recognition stage, we propose the K-BERT-BiLSTM-CRF model, which is trained on a military named entity recognition dataset and used for military named entity recognition to retrieve candidate entities and attributes for entity linking. During the entity linking stage, candidate entities and attributes are aligned with unique entities and multiple candidate attributes in the knowledge graph through vector similarity calculations using a pre-trained model, thereby obtaining relevant entities and solving constraints. For the pre-trained model, we utilize the encoding layer of K-BERT from the K-BERT-BiLSTM-CRF model trained on the named entity recognition task to fully understand the meanings and differences of military terms. In the knowledge retrieval stage, relevant background knowledge is obtained through weapon types and entities, and represented using Answer Set Programming to provide a data basis for problem solving. The framework effectively acquires background knowledge through these four stages. Considering the characteristics of multi-constraint problems, the knowledge refinement stage uses Answer Set Programming to reduce the amount of knowledge or directly obtain answers by applying hard and soft constraints. Finally, in the problem-solving stage, considering the challenges of ambiguity, vagueness, and sparsity in attribute mention recognition and linking in military intelligence question answering, a large language model is used to solve the problem based on the refined knowledge, reducing attribute recognition and linking during the problem understanding process. Experiments were conducted on the MilRE dataset, randomly selecting 5 samples of each question type, covering a total of 115 questions from 23 different categories. The framework achieved retrieval and question-answering accuracies exceeding 90%. Experimental results demonstrate that the framework provides enhanced knowledge retrieval capabilities based on knowledge graphs and effectively answers military intelligence questions.

Key words intelligence question-answering, answer set programming, large language models, retrieval-augmented generation, knowledge graph

一种结合敏感词匹配和提示词构建的 仇恨言论检测方法**

徐磊^{1,2} 孙家栋² 胡亚豪¹ 潘志松^{1*}

摘要 尽管大型语言模型在各种自然语言处理任务中展示了卓越的能力，但其在识别隐晦仇恨言论方面的有效性尚未得到充分探索。基于此，文章提出了一种结合敏感词匹配和提示词构建的仇恨言论检测方法——Filter-Prompt。首先，通过关键词匹配获取待检测文本中的敏感词信息，然后，根据这些信息设计提示词输入，以提高大型语言模型对隐式仇恨言论的检测效果。实验结果显示，与传统方法相比，Filter-Prompt 在仇恨言论检测二分类任务中的各项评价指标上均取得了显著提升。

关键词 仇恨言论检测，大型语言模型，敏感词匹配，提示学习

A Hate Speech Detection Method combining Sensitive Word Matching and Prompt Construction**

XU Lei^{1,2} SUN Jia-Dong² HU Ya-Hao¹ PAN Zhi-Song^{1*}

Abstract Despite the impressive capabilities of large language models in various natural language processing tasks, their effectiveness in detecting implicit hate speech has not been fully explored. To address this, we propose a hate speech detection method called Filter-Prompt, which combines sensitive word matching with prompt construction. First, sensitive word information is obtained from the text to be detected through keyword matching. Then, prompts are designed based on this information to improve the detection of implicit hate speech by large language models. Experimental results show that compared to traditional methods, Filter-Prompt significantly enhances various evaluation metrics in binary classification tasks for hate speech detection.

Key words hate speech detection, large language models, sensitive word matching, prompt learning

0 引言

随着网络技术的快速发展，诸如抖音

和微博这样的在线社交媒体变得越发活跃。然而，这也带来了各种形式的侮辱和攻击性言论的滋生。例如，网络暴力中施

** 国家自然科学基金 (62076251) 资助

** Supported by National Natural Science Foundation of China (62076251)

* 通讯作者

1. 陆军工程大学指挥控制工程学院 2. 中国电子科技集团公司第二十八研究所信息系统工程全国重点实验室
1. College of Command & Control Engineering, Army Engineering University of PLA 2. National Key Laboratory of Information System Engineering, The 28nd Research Institute of China Electronics Technology Group Corporation

暴者的不负责任言论给受害者造成了心理和身体上的双重创伤。为维护绿色健康的网络环境，国家互联网信息办公室于2023年7月7日发布了《网络暴力信息治理规定（征求意见稿）》。尽管当前互联网平台的监管日益完善，但对于识别包含隐喻和讽刺的间接性侮辱，现有识别系统仍然效果不佳。为此，本文提出了一种利用大型语言模型进行仇恨言论检测的新方法。

1 相关工作

1.1 仇恨语言检测方法

早期针对仇恨言论检测的方法主要基于规则挖掘文本特征来检测仇恨言论。例如，通过建立包含常见仇恨言论词汇、负面情感词汇和刻板话语的词典，在文本中搜索和计数这些词的频率，并用频率作为特征或评估分数，最终通过规范化步骤或正则表达式判断言论是否具有仇恨性^[1-3]。同时，针对采用谐音词或侮辱性词的指代词这种逃避检测的方法，也有研究提出使用距离度量来对基于词典的方法进行补充，如 Levenshtein 距离，将一个字符串转化为另一个字符串所需要的最小编辑次数^[4]。

在统计学习方法阶段，研究重点是训练算法模型捕捉数据中的复杂关系和变化趋势，而不仅仅局限于处理一些固定的问题。如与词典方法相类似的词袋模型（Bag-of-Words, BOW），其基于训练数据中的单词，而非预定义的词典集合，但该方法忽略了词的序列关系，也忽视了句法和语义内容。一旦词语在不同的语境中使用，就可能会错误分类。为了克服这一限制，N-gram 方法被提出。N-gram 在

仇恨言论检测中应用广泛，能包含每个单词的上下文，因此检测效果较好。然而，当 N 值很大时，处理速度会显著降低，因此有研究表明，N-gram 与其他特征提取方法结合效果更佳^[5]。

深度学习（DL）方法在检测多种形式的冒犯性或辱骂性语言方面标志着一个重要的进步。它们允许使用词向量，如 Word2Vec^[6]、Glove^[7] 或 ELMo^[8]，而不是词袋表示。此外，深度学习模型如长短期记忆网络（LSTM）或卷积神经网络（CNN）在多个自然语言处理任务中比支持向量机、逻辑回归或决策树模型等较为简单的分类器取得了显著的结果。巴贾提亚（Badjatiya）等（2017年）在一个包含16000条标注英语推文的数据集上进行了多种实验，以检测仇恨言论。他们证明总体上深度学习方法优于基于字符和词的 N-gram 模型^[9]。

1.2 确定有限状态自动机

确定有限状态自动机（Deterministic Finite Automaton, DFA）是一种用于表示有限状态系统的数学模型。它通常由一个有限的状态集合、一个输入符号集合、一个转移函数、一个初始状态和一个或多个接受状态组成。DFA 在模式匹配、词法分析、网络协议验证等领域中扮演着关键角色。本文使用 DFA 算法来构建敏感词过滤模块，具体方法实现见 4.1 节。

1.3 提示学习

尽管基于 Transformer 架构的大型语言模型已经得到广泛应用，但模型的能力仍然依赖于用户提供的输入“提示”（Prompt）。尽管提示词可以是多模态的，但已有研究表明自然语言形式的提示能使模型更加易于互动，且灵活应用于广泛的

使用场景^[10]。

提示学习旨在通过使用简单的提示词来引导大模型的涌现能力，从而解决相应的下游任务。随着大语言模型的研究，提示学习的研究也一直进行着。其中，较为经典的两种方法分别是少次提示学习（Few-Shot Learning）^[11]和零次提示学习（Zero-Shot Learning）^[12]。前者通过输入范例或指令，使大模型快速学习技能并完成任务，仅需少量样本；而后者则更进一步，直接指定输出要求，无须使用任何提示样例，即可实现任务的完成。随着研究的深入，研究人员提出了模拟人类思维生成的提示学习方法，如思维链提示^[13]、类比推理提示^[14]、思维线索提示^[15]等。而基于人类解决困难问题往往会先将其分解为简单问题的思想，相应的问题分解技术也随之提出，如最少到最多提示学习（Least-to-Most Prompting）^[16]、思维树提示（Tree-of-Thought, ToT）等。

2 问题定义

仇恨言论检测任务本质上可以理解为一个二分类任务^[17]，假设仇恨语言文本数据集为 $D = \{(x_i, y_i)\}_{i=1}^n$ ，其中 x_i 表示的是第 i 个文本样本， $y_i \in \{0, 1\}$ 表示其对应的类别标签（0 代表着文本不具有仇恨性，1 代表着文本具有仇恨性）。首先使用过滤模块对输入 X 进行过滤，如式（1）所示：

$$key = filter(X) = \{key \mid key \in X\} \quad (1)$$

依据所得到的关键词构建 Prompt 提示词，如式（2）所示：

$$P = f_{prompt}(key) \quad (2)$$

最终模型的学习目标是：

$$f(P): X \rightarrow \{0, 1\} \quad (3)$$

3 数据集与评估指标

3.1 实验数据集

由于现阶段社交媒体平台对于仇恨言论的监管策略，本文以 COLDataset 数据集^[18]和 Cdial 数据集^[19]为基准进行数据增强。传统的数据增强方法最简单的莫过于通过将句子中的性别进行替换从而得到新数据，该方法灵活且有效^[20]。受性别替换方法的启发^[21]，本文使用大模型，从性别、地域、种族和职业四个方面对数据进行增广。例如，对于“黑命就是没有白命值钱”这样的话语，可以将其中对于种族的指代进行替换，如“白命就是没有黄命值钱”。

除了对具体词汇的指代，也可以使用提示词，让大模型输出与样本相似的语句，从而达到扩充数据集的目的。数据增广的同时，还需要剔除生成的不通顺的句子。最终可以得到的数据集分布如表 1 所示。

表 1 数据集样本分布表

仇恨类别	样本数量
性别	6138
地域	7910
种族	9736
职业	3021

3.2 评价指标

仇恨言论检测任务本质上仍然属于一个文本的二分类任务，因此，采用经典的二分类评估指标，精确率（Precision）、召

回率 (Recall)、准确值 (Accuracy) 和 $F1$ 值来衡量模型的效果。假设真正类为 TP , 假正类为 FP , 真负类为 TN , 假负类为 FN 。那么精确率 P 、召回率 R 、准确率 A 和 $F1$ 值的计算方式为:

$$P = \frac{TP}{TP + FP}$$

$$R = \frac{TP}{TP + FN}$$

$$Acc = \frac{TP + TN}{TP + FP + TN + FN}$$

$$F1 = \frac{2 \times P \times R}{P + R}$$
(4)

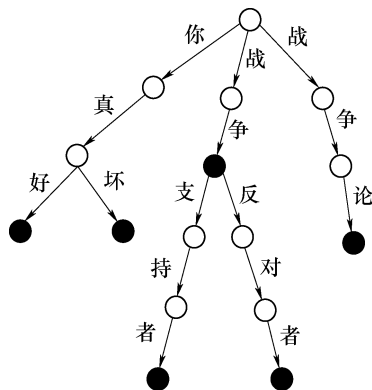


图1 敏感词状态树

4 实验研究

4.1 实验方法

首先使用 DFA 算法对需要过滤的敏感词进行状态树的构建，假设敏感词词库中包含“你真好”“你真坏”“战争支持者”“战争反对者”“战争论”，状态树如图1所示。以“战争反对论”为例，可以将其拆分为“战”“战争”“战争反”“战争反对”“战争反对者”五个文本片段，每个片段即对应着一个状态，状态树中的空心节点即代表着状态，而实心节点则代表着一个完整的关键词。而当敏感词表构建完成后，用户给定大模型输入，通过过滤模块匹配出其中的敏感词，并将敏感词填入构建的提示词模板中，从而构建出新的提示词，最终使用新构建的提示词来对大模型进行提示学习，最终使得大模型完成对仇恨言论的检测，Filter-Prompt 完整方法架构如图2所示。

假设待检测文本为“程序员就是新生代农民工，门槛低，北大×鸟培训一个月上岗?”，Filter 过滤模块匹配到“素质”



图2 Filter-Prompt 方法结构

和“北京”，将敏感词和输入样本填入提示词中，提示词模板以“你作为一名网络内容审查员，结合句子中的关键词 {word}，判断该句子是否含有偏见，以及包含哪种偏见”为例，最终输入给大模型，从而引导大模型输出正确的分类结果。

4.2 对比实验

为了验证 Filter-Prompt 方法的有效性，本文将 Filter-Prompt 方法分别与在 ChatGLM2-6B 模型上的零样本提示学习方法和少样本提示学习方法，以及通过 P-tuning 微调后的 ChatGLM2-6B 进行对比。实验结果如表2所示。

表 2 对比实验结果

模型方法	精确率 P	召回率 R	准确率 A	$F1$ 值
Textfilter	0.657	0.190	0.525	0.295
Zero-Shot	0.464	0.558	0.642	0.506
Few-shot	0.749	0.497	0.601	0.598
P-tuning	0.7368	0.828	0.815	0.780
Filter-Prompt	0.843	0.874	0.886	0.858

从实验结果中可以看出，文本过滤方法能够根据预先搜集的敏感词表准确匹配出待检测文本中的敏感信息。然而，当待检测文本的内容为对负面信息的否定，如“我们要反对黄赌毒”这样的样本时，文本过滤方法仍然会将其判定为含有仇恨信息。如果包含敏感词但表达反对仇恨言论的句子增多，文本过滤方法的准确率将急剧下降，这表明该方法的准确性与实验样本中正反立场的分布有很大关系。而仅仅依靠大模型自身的能力，对于一些已经被普遍认为具有仇恨性的词句识别是没有问题，但对于一些新出现的带有仇恨、讽刺意味的词语，大模型自身的能力并不能很好地解决这些问题。通过少次学习后，大模型的能力有所改善，但这需要为不同输入样本精心设计提示词，因此，尽管准确率有所提升，该方法也不够实用。而 Filter-Prompt 方法，则是依据过滤出来的关键词来进行通用提示词的设计，并且取得了和 P-tuning 微调后的模型相似的结果。

4.3 消融实验

为了深入分析 Filter-Prompt 算法各部分对其效果的影响，本文进行了各个模块的单独实验。

具体方法为分别使用过滤模块（DFA 匹配算法）、提示学习模块进行实验。传统的 DFA 算法能够在已知关键词的情况下

达到高精度的识别率，但其局限性也显而易见，即无法理解待检测文本的语义。例如，在倡导和平的背景下，“支持战争”作为关键词，可能会导致“我们支持战争！”和“我们难道应该支持战争吗？”这两个相反观点的文本都被错误判定为与主题相悖。而相比之下，提示学习方法能够较好地理解语义，并给出对句子的判断，但是针对不同的句子需要人为编写提示词模板，否则会面临识别效果不佳的问题。并且有的时候提示学习方法并不能很好地以关键敏感词为重点去判断待检测文本中是否包含仇恨性。为兼顾两者优势，Filter-Prompt 利用过滤模块精准识别关键敏感词，并以此为基础构建 Prompt，激发大型语言模型在理解和分类待检测文本时的学习能力和理解能力，从而提高仇恨言论检测的效果。具体实验结果如图 3 所示，为了使热力图更加具有区分性，本文对真正类、假正类等结果进行了百分比计算。

5 结束语

本文提出了一种 Filter-Prompt 方法，具体来说，该方法通过 DFA 算法来检测敏感词信息，并根据匹配到的敏感词构建提示词来对大模型进行提示学习。Filter-Prompt 方法与单一的 DFA 算法和提示学习方法相比在仇恨言论检测任务上取得了更好的性能。同时，与在 ChatGLM2-6B 模型上进行的 Zero-Shot、Few-Shot 和 P-tuning 方法相比，Filter-Prompt 方法的性能远远超过了 Zero-Shot 和 Few-Shot，并且和使用 P-tuning 微调之后的模型性能相当，证明了其在仇恨言论检测任务中的有效性。在下一步的工作中，应该考虑如何进一步构建泛化性更强的提示词模块，以及 Filter-Prompt 方法在长上下文和多轮对话语境下的性能。

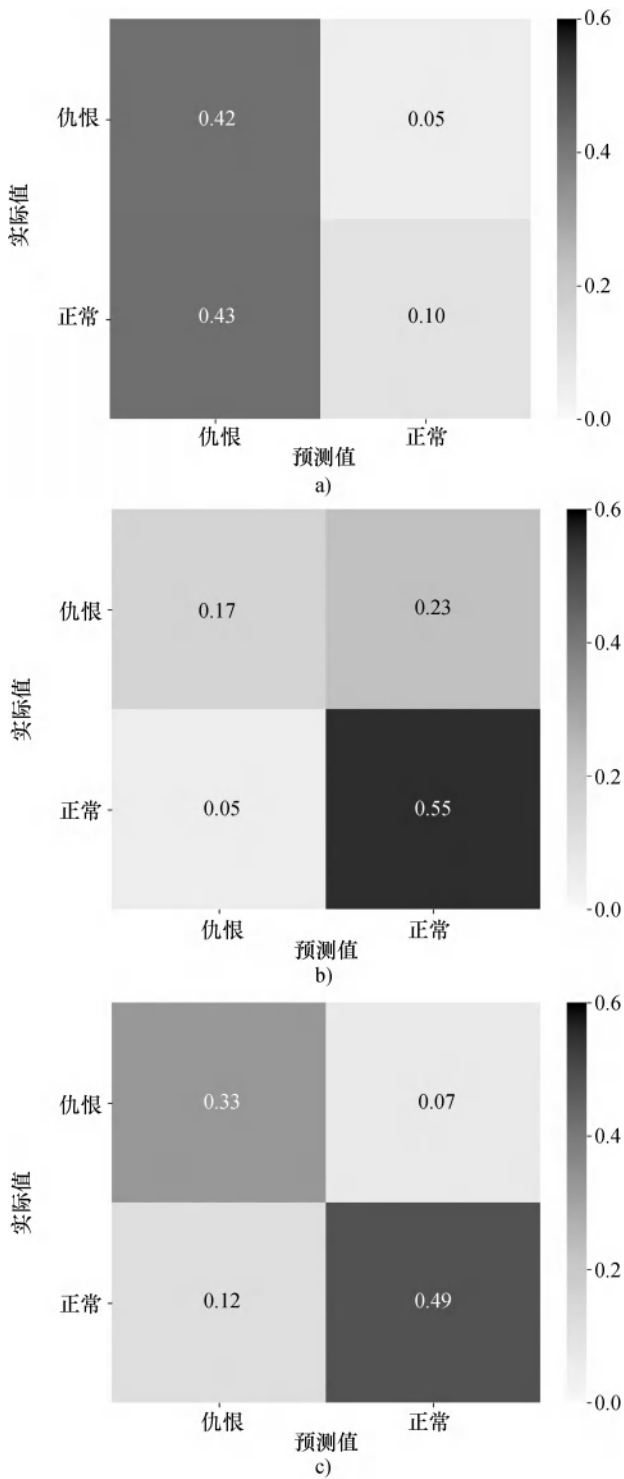


图3 消融实验结果

a) Filter 模块; b) 提示学习模块; c) Filter-Prompt

参考文献

- 1 DADVAR, MARAL. Improved cyberbullying detection using gender information [C] //Proceedings of the Twelfth Dutch-Belgian Information Retrieval Workshop (DIR 2012). Universiteit Gent, 2012: 23-25.
- 2 DINAKAR K, REICHART R, LIEBERMAN H. Modeling the Detection of Textual Cyberbullying [J]. Proceedings of the International AAAI Conference on Web and Social Media, 2021, 5 (3): 11-17. DOI: 10.1609/icwsm.v5i3.14209.
- 3 FORTUNA P, NUNES S. A Survey on Automatic Detection of Hate Speech in Text [J]. ACM Computing Surveys, 2018, 51 (4). DOI: 10.1145/3232676.
- 4 NANDHINI B S, SHEEBA J I. Cyberbullying Detection and Classification Using Information Retrieval Algorithm [C/OL] //Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015). Unnao India: ACM, 2015: 1-5 [2024-06-29]. https://dl.acm.org/doi/10.1145/2743065.2743085. DOI: 10.1145/2743065.2743085.
- 5 MEHDAD Y, TETREAULT J. Do Characters Abuse More Than Words? [C/OL] //Proceedings of the 17th Annual Meeting of the Special Interest Group on Discourse and Dialogue. Los Angeles: Association for Computational Linguistics, 2016: 299-303 [2024-06-29]. http://aclweb.org/anthology/W16-3638. DOI: 10.18653/v1/W16-3638.
- 6 CUI Y, YANG Z, YAO X. Efficient and Effective Text Encoding for Chinese LLaMA and Alpaca [J/OL]. arXiv, 2023. [2023-04-19]. http://arxiv.org/abs/2304.08177.
- 7 PENNINGTON J, SOCHER R, MANNING C. Glove: Global Vectors for Word Representation [C/OL] //Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP). Doha, Qatar: Association for Computational Linguistics. 2014: 1532-1543. [2023-05-29]. http://aclweb.org/anthology/D14-1162. DOI: 10.3115/v1/D14-1162.
- 8 PETERS M E, NEUMANN M, IYYER M, et al. Deep contextualized word representations [M/OL]. arXiv, 2018. [2023-10-29]. http://arxiv.org/abs/1802.05365.
- 9 BADJATIYA P, GUPTA S, GUPTA M, et al. Deep Learning for Hate Speech Detection in Tweets [C/OL] //Proceedings of the 26th International Conference on World Wide Web Companion - WWW '17 Companion. 2017: 759-760. [2024-06-29]. http://arxiv.org/abs/1706.00188. DOI: 10.1145/3041021.3054223.
- 10 SCHULHOFF S, ILIE M, BALEPUR N, et al. The Prompt Report: A Systematic Survey of Prompting Techniques [M/OL]. arXiv, 2024. [2024-06-28]. http://arxiv.org/abs/2406.06608.
- 11 BROWN T B, MANN B, RYDER N, et al. Language Models are Few-Shot Learners [J]. arXiv, 2020.
- 12 KOJIMA T, GU S S, REID M, et al. Large Language Models are Zero-Shot Reasoners [J/OL]. arXiv, 2023. [2024-03-18]. http://arxiv.org/abs/2205.11916.
- 13 LU H, HUANG H, ZHANG D, et al. Chain-of-Dictionary Prompting Elicits Translation in Large Language Models [J/OL]. arXiv, 2023. [2023-05-15]. http://arxiv.org/abs/2305.06575.
- 14 YASUNAGA M, CHEN X, LI Y, et al. Large Language Models as Analogical Reasoners [J/OL]. arXiv, 2024. [2024-06-29]. http://arxiv.org/abs/2310.01714.
- 15 ZHOU Y, GENG X, SHEN T, et al. Thread of Thought Unraveling Chaotic Contexts [J/OL]. arXiv, 2023. [2024-06-29]. http://arxiv.org/abs/2311.08734.
- 16 ZHOU D, SCHÄRLI N, HOU L, et al. Least-to-Most Prompting Enables Complex Reasoning in Large Language Models [J/OL]. arXiv,

2023. [2024-03-18]. <http://arxiv.org/abs/2205.10625>.
- 17 KOWSARI K, MEIMANDI K J, HEIDARYSAFA M, et al. Text Classification Algorithms: A Survey [J/OL]. *Information*, 2019, 10 (4): 150. DOI: 10.3390/info10040150.
- 18 DENG J, ZHOU J, SUN H, et al. COLD: A Benchmark for Chinese Offensive Language Detection [J/OL]. arXiv, 2022. [2024-01-24]. <http://arxiv.org/abs/2201.06025>.
- 19 ZHOU J, DENG J, MI F, et al. Towards Identifying Social Bias in Dialog Systems: Frame, Datasets, and Benchmarks [J/OL]. arXiv, 2022. [2023-05-15]. <http://arxiv.org/abs/2202.08011>.
- 20 ZHAO J, WANG T, YATSKAR M, et al. Gender Bias in Coreference Resolution: Evaluation and Debiasing Methods [J/OL]. arXiv, 2018. [2023-11-12]. <http://arxiv.org/abs/1804.06876>.
- 21 朱述承, 苏祺, 刘鹏远. 基于语料库的我国职业性别无意识偏见共时历时研究 [J]. *中文信息学报*, 2021, 35 (5): 11. DOI: 10.3969/j.issn.1003-0077.2021.05.017.