CM2024 第十四届中国数学会计算机数学大会

http://www.mmrc.iss.ac.cn/cscm/cm2024/

2024年6月13-16日，中国·福州

主办单位

中国数学会计算机数学专业委员会

承办单位

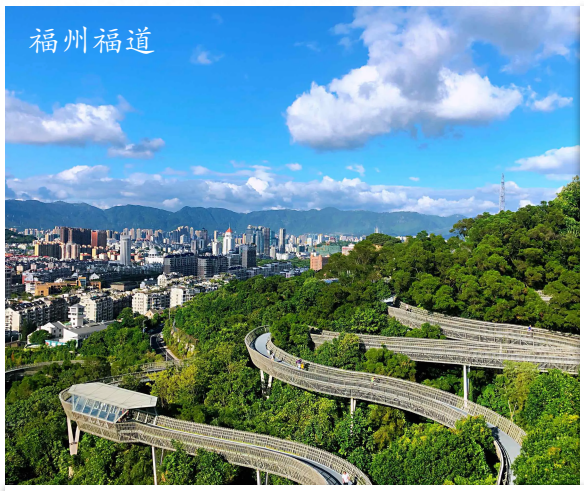
福建师范大学
中国科学院数学机械化重点实验室

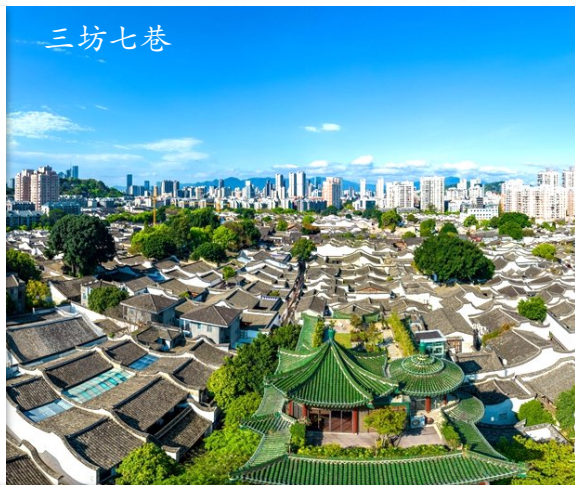
协办单位

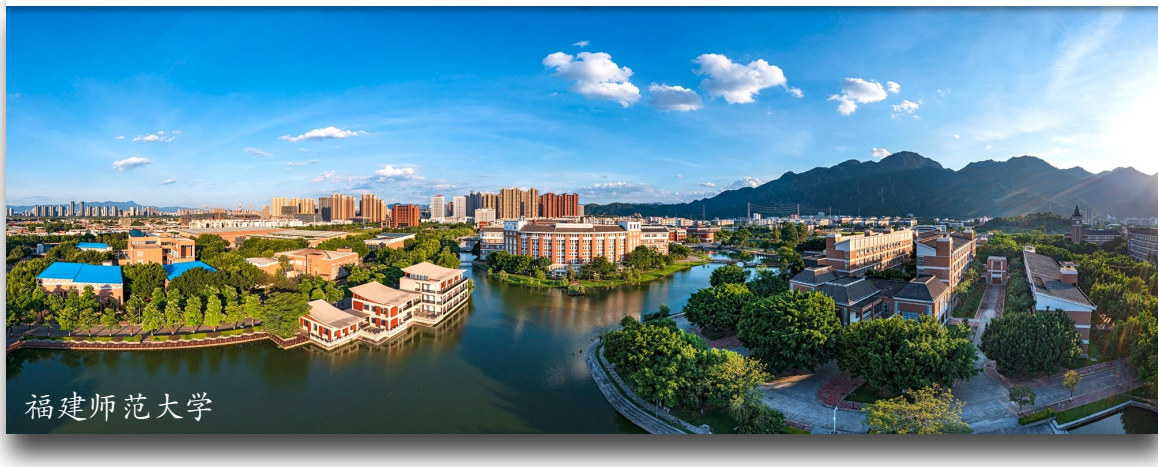
中国数学会

会议资助

国家自然科学基金委
中国数学会
Maplesoft中国
福建师范大学
数学与统计学院







大会主席　王长平　福建师范大学

程序委员会共同主席

陈长波　中国科学院重庆绿色智能技术研究院
林昌露　福建师范大学

■ “计算机代数”专题

程进三　中国科学院数学与系统科学研究院
董　波　大连理工大学（专题联合主席）
黄　博　北京航空航天大学
黄巧龙　山东大学
李冬梅　湖南科技大学
李　楠　深圳大学
牟晨琪　北京航空航天大学（专题联合主席）
吴文渊　中国科学院重庆绿色智能技术研究院
孙　瑶　中国科学院信息工程研究所
叶　科　中国科学院数学与系统科学研究院

■ “计算几何与智能制造”专题

陈中贵　厦门大学
李　明　浙江大学
李　新　中国科学技术大学（专题主席）
申立勇　中国科学院大学
朱春钢　大连理工大学
辛士庆　山东大学

■ “编码与密码”专题

金玲飞　复旦大学
刘美成　中国科学院信息工程研究所
刘　姝　电子科技大学
潘彦斌　中国科学院数学与系统科学研究院
王保仓　西安电子科技大学
孙　兵　国防科技大学
周正春　西南交通大学（专题主席）
张　俊　首都师范大学

■ “人工智能与数学软件”专题

曹钦翔　上海交通大学
李文达　英国爱丁堡大学
秦小林　中国科学院成都计算机应用研究所
施智平　首都师范大学
王　杰　中国科学院数学与系统科学研究院
夏壁灿　北京大学
杨争峰　华东师范大学
郁文生　北京邮电大学（专题联合主席）
詹博华　华为技术有限公司（专题联合主席）
周　立　中国科学院软件研究所

■ “量子算法”专题

李彤阳　北京大学
刘锦鹏　美国麻省理工学院
陆朝阳　中国科学技术大学
邵长鹏　中国科学院数学与系统科学研究院（专题主席）
向　华　武汉大学
姚鹏晖　南京大学

■ “组合数学”专题

曹海涛　南京师范大学
陈绍示　中国科学院数学与系统科学研究院
林启忠　福州大学
林志聪　山东大学
刘　丽　曲阜师范大学
汪　毅　安徽大学
夏先伟　苏州科技大学
祝宝宣　江苏师范大学（专题主席）

大会邀请报告

丁　剑　北京大学
王华雄　新加坡南洋理工大学
冯　勇　中国科学院重庆绿色智能技术研究院
邢朝平　上海交通大学
杨立波　南开大学
范更华　福州大学

青年邀请报告

上官冲　山东大学
李昊坤　华为2012可信费马实验室
郑晓朋　大连理工大学
高奕博　北京国际数学研究中心
胡胜龙　杭州电子科技大学
唐春明　西南交通大学
袁　骁　北京大学前沿计算研究中心
薛　白　中国科学院软件所

组织委员会

陈宇臻　福建师范大学
柯品惠　福建师范大学（主席）
梁克龙　福建师范大学
张玲玲　福建师范大学
胡慧丹　福建师范大学
乐雪靖　福建师范大学
平璐翔　福建师范大学
周　鑫　福建师范大学
黄可可　福建师范大学
李　佳　中国科学院数学与系统科学研究院
周代珍　中国科学院数学与系统科学研究院

大会联系人

陈长波：chenchangbo@cigit.ac.cn
林昌露：cllin@fjnu.edu.cn

福建师范大学简介

福建师范大学坐落于素有“海滨邹鲁”之誉的历史文化名城福州，是一所历史悠久、声誉斐然的百年省属高等学府。学校肇始于 1907 年清朝帝师陈宝琛先生创办的“福建优级师范学堂”，后由华南女子文理学院、福建协和大学、福建省立师范专科学校等单位几经调整合并，于 1953 年成立福建师范学院，1972 年易名为福建师范大学并沿用至今。福建师范大学是福建省人民政府与教育部共建高校、福建省重点建设的高水平大学、福建省一流大学建设高校、福建省第二轮“双一流”建设 A 类高校。

学校本部共有旗山、仓山两个校区，占地面积 4000 多亩。现有本科专业 84 个（2023 年全日制普通本科招生专业 78 个），全日制普通本科学生 2.5 万余人，各类研究生 1 万余人。学校充分发挥学科龙头带动作用，着力构建一流文科、高水平理科、有特色工科的学科体系，基本形成了综合性大学的学科布局。拥有国家重点学科 1 个、福建省第二轮“双一流”建设主干学科 3 个、省高峰学科 9 个和高原学科 13 个，博士后科研流动站 20 个，博士学位授权一级学科 19 个，博士专业学位授权点 3 个，硕士学位授权一级学科 32 个，硕士专业学位类别 26 个。化学、工程学、材料科学、计算机科学、环境科学与生态学、农学、社会科学总论、植物与动物学 8 个学科进入 ESI 全球排名前 1%，其中 5 个学科进入 ESI 前 5‰。

叶圣陶、郭绍虞、董作宾、林兰英、郑作新、黄维垣、唐仲璋、唐崇惕、姚建年等诸多蜚声海内外的大师巨匠曾在学校任教。经过一代又一代福建师大人的传承创新，学校砥砺出“知明行笃，立诚致广”的校训精神，孕育了“重教、勤学、求实、创新”的优良校风，着力推动各项事业不断向前发展，荣获“全国文明单位”“全国文明校园”等一大批高级别荣誉称号。建校以来，学校向社会培养输送各级各类人才近 60 万名，为国家和福建经济社会发展作出了突出贡献。

走过 117 年光荣历程的福建师范大学，不忘立德树人初心，牢记为党育人、为国育才使命，全面深化综合改革，全面推进内涵发展，全面提高办学质量，正朝着加快建成富有鲜明特色的综合性全国一流大学的奋斗目标大踏步前进，努力为谱写全面建设社会主义现代化国家福建篇章、实现中华民族伟大复兴的中国梦作出新的更大贡献。

福建师范大学数学与统计学院简介

福建师范大学数学与统计学院肇始于 1907 年陈宝琛先生创办的“福建优级师范学堂”的数学科。后由华南女子文理学院、福建协和大学、福建省立师范专科学校等院校几经调整合并，于 1953 年成立福建师范学院，保留和发展了数学系。1972 年，改名为福建师范大学数学系。1996 年，成立计算机科学系，与数学系合称为福建师范大学数学系、计算机科学系。2002 年，成立数学与计算机科学学院。2017 年 6 月，数学与计算机科学学院、软件学院整合成立数学与信息学院。2021 年 6 月，数学与信息学院分设数学与统计学院、计算机与网络空间安全学院（软件学院）。

学院现设数学系和统计学系，拥有数学与应用数学（师范类）、统计学、数据科学 3 个本科专业，现有在读学生 1622 人，其中研究生 398 人、本科生 1224 人。数学与应用数学专业是国家级特色专业、入选国家级一流本科专业建设点、通过教育部师范类专业二级认证；统计学专业入选国家级一流本科专业建设点。近年来，学院获得国家级教学成果二等奖 4 项，福建省教学成果奖特等奖 1 项、一等奖 2 项。学院教师担任人民教育出版社中学数学教材的主编工作。获批国家级一流课程 3 门、省级一流课程 4 门，国家级资源共享课程 1 门，省级教育教学改革项目 5 项（重点项目 1 项、一般项目 4 项），省级人才培养模式创新实验区 1 个，省级研究生教育创新基地 1 个。

现有，数学、统计学 2 个一级学科博士学位授权点，数学、统计学 2 个博士后科研流动站，数学、统计学 2 个一级学科硕士学位授权点，学科教学（数学）、应用统计 2 个专业学位硕士点。数学是福建省高峰学科，统计学是福建省重点学科。现有分析数学及应用教育部重点实验室、福建省分析数学及应用重点实验室、统计学与人工智能福建省高校重点实验室、福建省应用数学中心、福建师范大学数学研究中心和福建数学基础教育研究中心等科研平台。学院自 1958 年以来，主办《福建中学数学》杂志。学院还是福建省中小学数学学科教学带头人培养基地。

近年来，学院主动融入国家战略和地方经济社会发展，强化有组织的科研。学院教师获国家自然科学基金等国家级项目 30 多项；其中，国家自然科学杰出青年项目 1 项、国家自然科学优秀青年项目 1 项、国家自然科学基金重点项目 3 项（含参加）；获教育部自然科学奖一等奖 1 项、福建省自然科学奖一等奖、二等奖、三等奖各 1 项以及福建省社会科学奖二等奖 1 项、三等奖 1 项。学院学生在全国大学生数学竞赛、全国大学生数学建模竞赛、全国高校师范生教学技能大赛等高水平赛事中取得优异成绩。

学院高度重视高层次人才队伍建设，学院现有在职教职工 117 人，其中教授 28 人，副教授 46 人，博士生导师 16 人；其中，长江学者特聘教授 1 人，国家杰出青年科学基金获得者 2 人，国家优秀青年科学基金获得者 1 人，国务院政府特殊津贴 2 人，闽江学者 7 人，入选福建省“百人计划”

2 人，福建省“雏鹰计划”青年拔尖人才 2 人，福建省“百千万人才工程”3 人，福建省优秀教师 1 人，福建省“运盛”青年科技奖 2 人，建有“随机分析及相关领域”福建省高校科技创新团队、“非线性分析及应用”福建省博士生导师团队。2024 年学院获批国家留学基金委创新型人才国际合作培养项目。

学院已为党和国家培养了许多优秀的人才，他们积极工作，奋发向上，成为各行业的骨干，为教育发展、经济建设和社会进步做出了重要的贡献。江文哉、张远南、王毓泉、李必成、刘金星、林风、林群、叶青柏、林顺来、郑一平、李迅、林燎、邵东生、徐明杰、周灵、黄金德、赵祥枝、王奇南、林亚南、李海北等校友荣获“福建省杰出人民教师”荣誉称号。广大校友爱国爱校，慷慨解囊，捐资助学。2006 年，福建师范大学数学系 61 级学生、香港知名企业家、福建师范大学客座教授吴维新先生捐资设立“吴维新教育基金”；2015 年，吴维新先生再次捐资设立“吴维新研究生奖学金”。

学院党委认真履行党建工作主体责任，汇聚人心，凝聚力量，推动学院各项工作不断取得新的成绩。学院党委被福建省委教育工委评为“福建省学校创先争优先进基层党组织”、1 个学生党支部被福建省委教育工委评为“先进基层党组织”。学院工会被中华全国总工会评为“模范职工小家”、被福建省总工会评为“五一先锋号”。学院团委获得“全国五四红旗团委创建单位”“福建省新长征突击手”“福建省五四红旗团委标兵”“福建省五四红旗团委”“福建省基层

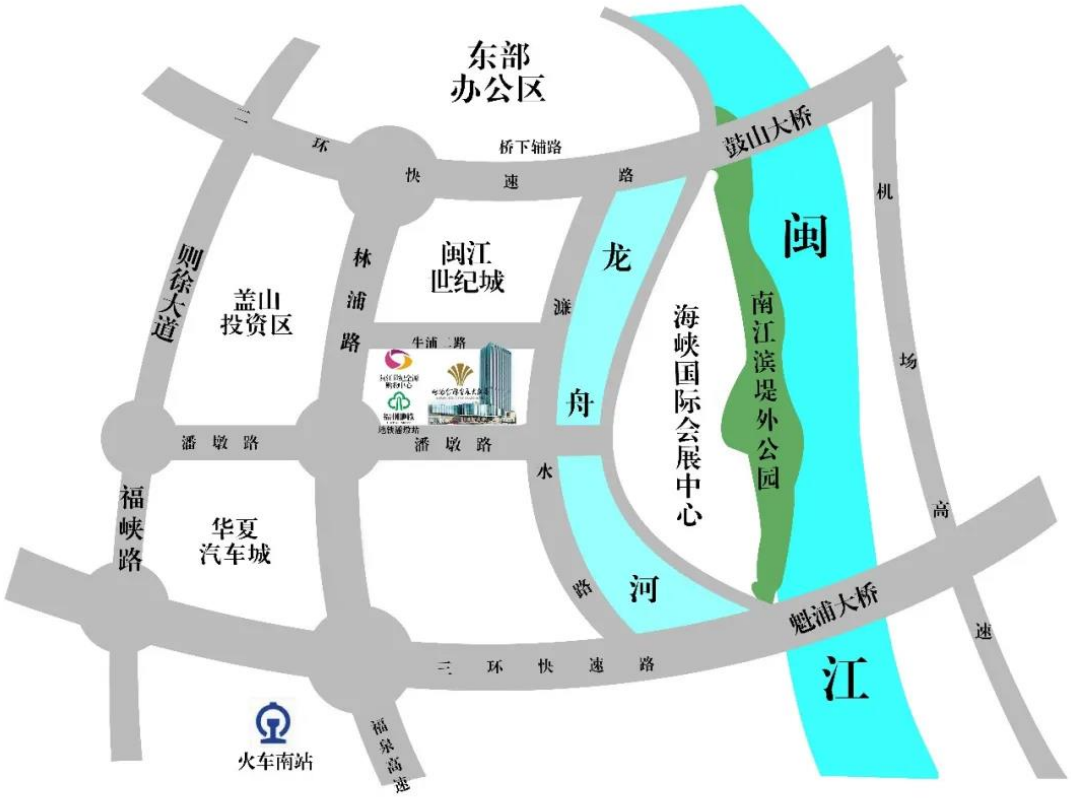
团建示范单位”等荣誉称号。学院教师还获得“福建青年五四奖章”“福建省优秀共青团干部”“福州市青年五四奖章”“校五一劳动奖章”等荣誉称号。

会议住宿与交通

会议地点：闽江世纪金源会展大饭店。

详细地址：中国福建省福州市仓山区潘墩路 188 号。

联系电话：0591-88889888。



福州闽江世纪金源会展大饭店区位示意图

Empark Exhibition Grand Hotel location sketch map

交通信息：闽江世纪金源会展大饭店坐落于林浦路与潘墩路交接口，距福州火车南站、福州火车站需 15 分钟左右车程，距福州长乐机场需 45 分钟左右车程。

- **火车南站：**酒店距离火车南站约为 8.6 公里。步行至地铁潘墩站（A 口）（停车场旁），乘坐地铁 6 号线（万寿方向）至梁厝站，换乘地铁 1 号线（象峰方向）至福州火车南站（C 口）下车，C 口通往福州南站 F1 层（地铁费用 3 元，费时约 25 分钟左右）。
- **福州火车站：**酒店距离福州火车约 16 公里。步行至地铁潘墩站（A 口）（停车场旁），乘坐地铁 6 号线（万寿方向）至梁厝站，换乘地铁 1 号线（象峰方向）至福州火车站（A2 东北口）下车，步行至福州火车站入口（约 200 米）（地铁费用 5 元，费时约 40 分钟左右）。
- **长乐机场：**酒店距离长乐机场约 40 公里。（1）乘坐网约车：全程约 40 公里途径东三环、机场高速、沈海高速（打车费用约 100 元，费时 40 分钟左右）；（2）乘坐地铁前往至福州火车南站，乘坐空港快线火车南站线至福州长乐国际机场（下客点）站，步行至福州长乐国际机场（约 50 米）（地铁费用 3 元、大巴费用 31 元，费时约 76 分钟左右）。

会议日程概览

6月13日，星期四		
10:00-18:00	注册报到（闽江世纪金源会展大饭店大堂）	
18:00-19:30	晚餐（大宴会A厅）	
6月14日，星期五		
8:00-8:30	注册报到（闽江世纪金源会展大饭店大堂）	
	大宴会C厅	
8:30-9:00	开幕式与合影	
9:00-10:00	大会邀请报告1	
10:00-10:10	茶歇	
10:10-11:10	大会邀请报告2	
11:10-12:10	大会邀请报告3	
12:10-14:00	午餐（大宴会A厅）	
	重庆厅	昆明厅
14:00-14:30	青年邀请报告1	青年邀请报告2
14:30-15:30	分组报告	分组报告
15:30-15:50	茶歇	
15:50-16:20	青年邀请报告3	青年邀请报告4
16:20-17:50	分组报告	分组报告、JSSC期刊宣讲
18:00-19:30	晚餐（大宴会A厅）	
20:00-22:00	计算机数学专业委员会会议（重庆厅）	
6月15日，星期六		
	大宴会C厅	
9:00-10:00	大会邀请报告4	
10:00-10:10	茶歇	
10:10-11:10	大会邀请报告5	

11:10-12:10	大会邀请报告6	
12:10-14:00	午餐（大宴会A厅）	
	重庆厅	昆明厅
14:00-14:30	青年邀请报告5	青年邀请报告6
14:30-15:30	分组报告	分组报告
15:30-15:50	茶歇	
15:50-17:35	分组报告	分组报告
18:00-20:00	晚餐（大宴会A厅）	
6月16日，星期日		
	重庆厅	昆明厅
9:00-9:30	青年邀请报告7	青年邀请报告8
9:30-10:30	分组报告	分组报告
10:30-10:50	茶歇	
10:50-12:05	分组报告	分组报告
12:05-14:00	午餐（大宴会A厅）	
	重庆厅	昆明厅
14:00-15:30	分组报告	分组报告
15:30-15:50	茶歇	
15:50-17:05	分组报告	分组报告
17:10-17:30	闭幕式（重庆厅）	
18:00-19:30	晚餐（大宴会A厅）	
6月17日，星期一		
离会		

备注：

（1）6场大会邀请报告均在大宴会C厅；

（2）午餐与晚餐地点均在大宴会A厅。

第十四届中国数学会计算机数学大会

2024 年 6 月 13 日 ~ 16 日

福建福州

2024 年 6 月 13 日

注册报到	6 月 13 日 10:00-18:00　闽江世纪金源会展大饭店大堂

晚餐	6 月 13 日 18:00-19:30　大宴会 A 厅

2024 年 6 月 14 日

注册报到	6 月 14 日 8:00-8:30　闽江世纪金源会展大饭店大堂

开幕式与合影	6 月 14 日 8:30-9:00　大宴会 C 厅

大会邀请报告 (1): 范更华	6 月 14 日 9:00-10:00　大宴会 C 厅

主持人:　支丽红

9:00 - 10:00　四色问题与子图覆盖(abstract)　P.20

范更华 (福州大学)

茶歇	6 月 14 日 10:00-10:10　大宴会厅公区

大会邀请报告 (2): 王华雄

6 月 14 日 10:10-11:10 大宴会 C 厅

主持人: 唐春明

10:10 - 11:10 Algebra, Combinatorics and Cryptography (abstract) P.20

王华雄 (新加坡南洋理工大学)

大会邀请报告 (3): 邢朝平（线上）

6 月 14 日 11:10-12:10 大宴会 C 厅

主持人: 李洪波

11:10 - 12:10 Fast Fourier Transform via automorphism groups of rational function fields (abstract) P.20

邢朝平 (上海交通大学)

午餐

6 月 14 日 12:10-14:00 大宴会 A 厅

青年邀请报告 (1): 高奕博

6 月 14 日 14:00-14:30 重庆厅

主持人: 牟晨琪

14:00 - 14:30 Symmetric structures in the Bruhat order (abstract) P.21

高奕博 (北京国际数学研究中心)

青年邀请报告 (2): 唐春明

6 月 14 日 14:00-14:30 昆明厅

主持人: 周正春

14:00 - 14:30 Linear codes from Boolean functions with high (fast) algebraic immunity (abstract) P.21

唐春明 (西南交通大学)

分组报告 (1): 计算机代数

6 月 14 日 14:30-15:30 重庆厅

主持人: 黄巧龙

14:30 - 14:45 Complexity of Skew Polynomial Multiplication (abstract) P.22

陈琦元 (中科院数学与系统科学研究院)

14:45 - 15:00 Applicability of the Cayley Transform (abstract) P.22

陆镜宇 (中国科学院数学与系统科学研究院)

15:00 - 15:15 Sparse Polynomial Interpolation With Error Correction: Higher Error Capacity by Randomization (abstract) P.23

杨志红 (中南大学数学与统计学院)

15:15 - 15:30 Reduced Grobner Bases of Schubert Determinantal Ideals (abstract) P.23

宋秋叶 (北京航空航天大学)

分组报告 (2): 编码与密码

6 月 14 日 14:30-15:30 昆明厅

主持人: 张俊

14:30 - 14:45 Lightweight Dynamic Broadcast Proxy Re-Encryption for Data Sharing in Clouds (abstract) P.24

胡慧丹 (福建师范大学)

14:45 - 15:00 Linear Complementary Dual Codes Constructed from Reinforcement Learning (abstract) P.25

吴严生 (南京邮电大学计算机学院)

15:00 - 15:15 Generalized Hamming weights of linear codes from defining sets (abstract) P.25

刘超 (湖北大学)

15:15 - 15:30 基于双循环编码的同态密文矩阵操作(abstract) P.26

杨林翰 (重庆交通大学信息科学与工程学院)

茶歇 6 月 14 日 15:30-15:50 重庆厅门口

青年邀请报告 (3): 上官冲

6 月 14 日 15:50-16:20 重庆厅

主持人: 祝宝宣

15:50 - 16:20 Recent progress on graph chromatic thresholds and graph homomorphism thresholds (abstract) P.26

上官冲 (山东大学)

青年邀请报告 (4): 薛白

6 月 14 日 15:50-16:20 昆明厅

主持人: 吴文渊

15:50 - 16:20 A Framework for Safe Probabilistic Invariance Verification of Stochastic Dynamical Systems (abstract) P.27

薛白 (中国科学院软件所)

分组报告 (3): 组合数学与计算机代数

6 月 14 日 16:20-17:50 重庆厅

主持人: 陈绍示

16:20 - 16:35 Unimodality of certain partition polynomials (abstract) P.27

Guo Wan-Ming （School of Mathematical Sciences, Qufu Normal University ）

16:35 - 16:50 Explicit formulas for a family of hypermaps beyond the one-face case (abstract) P.27

Bai Ziwei （合肥工业大学)

16:50 - 17:05 Fast Numerical Evaluation of Generalized Todd Polynomials (abstract) P.28

张英瑞 (中国科学院数学与系统科学研究院)

17:05 - 17:20 多元多项式矩阵等价的进一步的结果(abstract) P.28

关剑成 (湖南科技大学)

17:20 - 17:35 The Smith normal form and reduction of weakly linear matrices (abstract) P.29

吴弢 （湖南科技大学)

17:35 - 17:50 三维空间中顶点同构型的多面体(abstract) P.29

武斌 (上海财经大学浙江学院)

分组报告 (4): 人工智能与数学软件

6 月 14 日 16:20-17:20　昆明厅

主持人:　王杰

16:20 - 16:35　Hybrid Controller Synthesis for Nonlinear Systems Subject to Safety Constraints (abstract)　P.30

Qi Niuniu （East China Normal University ）

16:35 - 16:50　滤子扩张原则的 Coq 形式化(abstract)　P.30

窦国威 (北京邮电大学)

16:50 - 17:05　基于 Lean 的组合恒等式自动化证明(abstract)　P.31

熊贝贝 (华东师范大学)

17:05 - 17:20　Maple 2024 新功能介绍(abstract)　P.31

林成青 (Maplesoft)

JSSC 期刊宣讲

6 月 14 日 17:20-17:50　昆明厅

主持人:　冯如勇

17:20-17:50　提升期刊服务水平，扩大期刊影响力
吴国云 (JSSC 期刊编辑部)

晚餐

6 月 14 日 18:00-19:30　大宴会 A 厅

计算机数学专业委员会会议

6 月 14 日 20:00-22:00　重庆厅

2024 年 6 月 15 日

大会邀请报告 (4): 丁剑	6 月 15 日 9:00-10:00 大宴会 C 厅

主持人: 夏壁灿

9:00 - 10:00 Recent progress on random graph matching problems (abstract) P.31

丁剑 (北京大学)

茶歇	6 月 15 日 10:00-10:10 大宴会厅公区

大会邀请报告 (5): 冯勇	6 月 15 日 10:10-11:10 大宴会 C 厅

主持人: 王定康

10:10 - 11:10 零误差计算(abstract) P.32

冯勇 (中国科学院重庆绿色智能技术研究院)

大会邀请报告 (6): 杨立波	6 月 15 日 11:10-12:10 大宴会 C 厅

主持人: 冯如勇

11:10 - 12:10 Symbolic approach to combinatorial relations (abstract) P.32

杨立波 (南开大学)

午餐	6 月 15 日 12:10-14:00 大宴会 A 厅

青年邀请报告 (5): 胡胜龙

6 月 15 日 14:00-14:30 重庆厅

主持人: 叶科

14:00 - 14:30 Quantifying low rank approximations of third order symmetric tensors (abstract) P.33

胡胜龙 (杭州电子科技大学)

青年邀请报告 (6): 袁骁

6 月 15 日 14:00-14:30 昆明厅

主持人: 邵长鹏

14:00 - 14:30 Quantum advantage for near-term and fault-tolerant quantum computers (abstract) P.33

袁骁 (北京大学前沿计算研究中心)

分组报告 (5): 计算机代数

6 月 15 日 14:30-15:30 重庆厅

主持人: 李楠

14:30 - 14:45 Krylov subspace methods based quaternion tensor form for generalized Sylvester quaternion tensor equation with application to color video denoising (abstract) P.34

吴玉玲 (福建师范大学)

14:45 - 15:00 Structural Analysis by Generalized Embedding Method for Integro-differential-algebraic Equations (abstract) P.34

杨文强 (中国科学院重庆绿色智能技术研究院)

15:00 - 15:15 Computation of Regular Tucker Decompositions by Tensor QR Method (abstract) P.35

Zhai Ziqi (苏州科技大学)

15:15 - 15:30 Logarithmic norm minimization of quaternion matrix decomposition for color image sparse representation (abstract) P.35

蔡小敏 (福建师范大学)

分组报告 (6): 量子算法

6 月 15 日 14:30-15:30 昆明厅

主持人: 徐鸣

14:30 - 14:45 Quantum spectral method for gradient and Hessian estimation (abstract) P.36

张宇欣 (中国科学院数学与系统科学研究院)

14:45 - 15:00 Quantum-Inspired Classical Algorithms for Solving Linear Feasibility Problems (abstract) P.36

Zuo Qian （Peking University ）

15:00 - 15:15 Quantum recurrent neural networks for sequential learning (abstract) P.37

Wang Zhimin （Ocean University of China ）

15:15 - 15:30 Quantum circuits for block encoding of structured matrices in ocean acoustics (abstract) P.37

Yao Hongmei （Harbin Engineering University ）

茶歇

6 月 15 日 15:30-15:50 重庆厅门口

分组报告 (7): 计算机代数

6 月 15 日 15:50-17:35 重庆厅

主持人: 李冬梅

15:50 - 16:05 Whitney Stratification of Algebraic Boundaries of Convex Semi-algebraic Sets (abstract) P.38

代梓灏 (中国科学院数学与系统科学研究院)

16:05 - 16:20 Qualitative Investigation of the Lorenz-84 System Using Computer Algebra Methods (abstract) P.38

Song Jichao （Beihang University ）

16:20 - 16:35 Efficient detection of redundancies in systems of linear inequalities (abstract) P.39

谢岩峰 (中国科学院数学与系统科学研究院)

16:35 - 16:50 Computing the greatest common divisor of several parametric univariate polynomials via generalized subresultant polynomials (abstract) P.39

Jing Yang （Guangxi Minzu University ）

16:50 - 17:05 The Geometry of Cylindrical Algebraic Decomposition (abstract) P.40

陈日增 (北京大学数学科学学院)

17:05 - 17:20 Exploiting Sign Symmetries in Minimizing Sums of Rational Functions (abstract) P.41

郭峰 (大连理工大学)

17:20 - 17:35 Strengthening Lasserre's Hierarchy in Real and Complex Polynomial Optimization (abstract) P.41

王杰 (中国科学院数学与系统科学研究院)

分组报告 (8): 组合数学	6 月 15 日 15:50-17:35 昆明厅

主持人: 黄辉

15:50 - 16:05 Algorithms for Hadamard products of rational functions (abstract) P.41

Chen Shaoshi (中国科学院数学与系统科学研究院)

16:05 - 16:20 Symbolic Summation in Multivariate Difference Fields (abstract) P.42

卫亚蓉 (天津理工大学)

16:20 - 16:35 基于图运算的多智能体系统通信拓扑优化(abstract) P.42

徐仝友 (安徽建筑大学)

16:35 - 16:50 Parity statistics on restricted permutations and the Catalan-Schett polynomials (abstract) P.43

刘静 (山东大学)

16:50 - 17:05 Critical Points of Symmetric Forms over the Unit Sphere (abstract) P.43

Xu Jia (Department of Mathematics, Southwest Minzu University)

晚餐	6 月 15 日 18:00-20:00 大宴会 A 厅

2024 年 6 月 16 日

青年邀请报告 (7): 李昊坤	6 月 16 日 9:00-9:30 重庆厅

主持人: 詹博华

9:00 - 9:30 无量词非线性公式可满足性问题的求解方法(abstract) P.44

李昊坤 (华为 2012 可信费马实验室)

青年邀请报告 (8): 郑晓朋

6 月 16 日 9:00-9:30 昆明厅

主持人: 李新

9:00 - 9:30 结构化网格生成中的关键问题及其计算共形几何解决方案(abstract) P.45

郑晓朋 (大连理工大学)

分组报告 (9): 人工智能与数学软件

6 月 16 日 9:30-10:30 重庆厅

主持人: 秦小林

9:30 - 9:45 Numerical simulation of heat transfer and entropy generation due to the nanofluid natural convection with viscous dissipation in an inclined square cavity (abstract) P.45

吕龙杰 (大连海事大学)

9:45 - 10:00 A heuristic quantum-behavior algorithm for scheduling optimization problems (abstract) P.46

李真 (北京邮电大学)

10:00 - 10:15 A dataset for suggesting variable orderings for cylindrical algebraic decompositions (abstract) P.46

Zhao Yuegang (Jiangsu University)

10:15 - 10:30 A study on denoising seismic signals based on convolutional self-encoder (abstract) P.47

霍雨欣 (国防科技大学应用数学研究中心)

分组报告 (10): 计算几何与智能制造

6 月 16 日 9:30-10:30 昆明厅

主持人: 袁春明

9:30 - 9:45 连续区间上积分值的三次三角样条插值(abstract) P.47

吴金明 (浙江工商大学)

9:45 - 10:00 Tolerance-Based Geometry Constraint Update Scheme for High-precision Direct Modeling (abstract) P.48

Chen Hui （ University of Chinese Academy of Sciences ）

10:00 - 10:15 Efficient tool path planning and CAM process development (abstract) P.48

马鸿宇 (中国科学院大学)

10:15 - 10:30 High quality LSPIA method for NURBS curves and surfaces with weights and knots optimization (abstract) P.49

Lan Lin （大连理工大学)

茶歇

6 月 16 日 10:30-10:50 重庆厅门口

分组报告 (11): 人工智能与数学软件

6 月 16 日 10:50-12:05 重庆厅

主持人: 李树光

10:50 - 11:05 数据驱动的复杂系统建模(abstract) P.49

朱群喜 (复旦大学)

11:05 - 11:20 基于改进黏菌算法的风电场布局优化研究(abstract) P.50

谢嘉诚 (广西民族大学)

11:20 - 11:35 Utilizing symmetry-enhanced physics-informed neural network to obtain the solution beyond sampling domain for partial differential equations (abstract) P.50

Li Jie-Ying (Minzu University of China)

11:35 - 11:50 Symmetry group based domain decomposition to enhance physics-informed neural networks for solving partial differential equations (abstract) P.51

Liu Ye (Minzu University of China)

11:50 - 12:05 脉冲噪声下鲁棒的盲图像去模糊算法(abstract) P.52

李喆 (长春理工大学)

分组报告 (12): 计算几何与智能制造

6 月 16 日 10:50-12:05 昆明厅

主持人: 张举勇

10:50 - 11:05 High speed corner trajectory planning method for CNC machining with confined jerk (abstract) P.52

孟可欣 (中国科学院数学与系统科学研究院)

11:05 - 11:20 点云曲面上的 Voronoi 图(abstract) P.53

张子扬 (山东大学)

11:20 - 11:35 实体钣金建模(abstract) P.54

王文嵩 (山东大学计算机科学与技术学院)

午餐 6 月 16 日 12:05-14:00 大宴会 A 厅

分组报告 (13): 计算机代数 6 月 16 日 14:00-15:30 重庆厅

主持人: 黄博

14:00 - 14:15 Rational Solutions of First-Order Algebraic Ordinary Difference Equations (abstract) P.54

Zhang Yi (Xi'an Jiaotong-Liverpool University)

14:15 - 14:30 Hilbert's Irreducibility Theorem for Linear Differential Operators (abstract) P.54

陆伟 (湖北大学)

14:30 - 14:45 Two complete reduction systems for Airy functions (abstract) P.55

Du Hao (Beijing University of Posts and Telecommunications)

14:45 - 15:00 An Additive Decomposition in Exponential Extensions (abstract) P.55

高艺漫 (中国科学院数学与系统科学研究院)

15:00 - 15:15 Fast Normalization of Indexed Differentials (abstract) P.56

刘姜 (上海理工大学)

15:15 - 15:30 Safety Verification for Regime-Switching Jump Diffusions via Barrier Certificates (abstract) P.56

刘凯荣 (北京航空航天大学)

分组报告 (14): 编码与密码

6 月 16 日 14:00-15:30 昆明厅

主持人: 林富春

14:00 - 14:15 TFHE-like Functional Bootstrapping in General Cyclotomic Ring (abstract) P.57

刘登发 (中国科学院数学与系统科学研究院)

14:15 - 14:30 Fast, Lagre Scale Dimensionality Reduction Schemes Based on CKKS (abstract) P.57

Yuan Haonan （Chongqing Key Laboratory of Secure Computing for Biology, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences ）

14:30 - 14:45 Leveled homomorphic encryption based on NTRU without relinearization (abstract) P.58

代小康 (中科院重庆绿色智能技术研究院)

14:45 - 15:00 Classification of a class of planar quadrinomials (abstract) P.59

Chan Chin Hei （香港科技大学)

15:00 - 15:15 基于全同态加密的高效隐私保护聚类算法(abstract) P.60

杨晨 (中国科学院重庆绿色智能技术研究院)

15:15 - 15:30 基于可解正交阵列的 Ramp 密钥共享方案(abstract) P.61

邓扬眉 (中国民航大学)

茶歇

6 月 16 日 15:30-15:50 重庆厅门口

分组报告 (15): 计算机代数

6 月 16 日 15:50-17:05　重庆厅

主持人: 郑涛

15:50 - 16:05 A Basis-preserving Algorithm for Computing the B´ezout Matrix of Newton Polynomials (abstract) P.61

Yang Wei （Guangxi Minzu University）

16:05 - 16:20 Affine geodesic convex polynomials are rare (abstract) P.61

王愚（中国科学院数学与系统科学研究院机械化实验室）

16:20 - 16:35 A Generalization of Habicht's Theorem for Subresultants of Several Univariate Polynomials (abstract) P.62

蒙嘉奇（广西民族大学）

16:35 - 16:50 Extensions of S-Lemma for Noncommutative Polynomials (abstract) P.62

闫斯卓（中国科学院数学与系统科学研究院）

16:50 - 17:05 基于强弦图的 F_2 上三角分解的复杂度分析(abstract) P.62

齐朝星（北京航空航天大学）

分组报告 (16): 计算机代数

6 月 16 日 15:50-17:05　昆明厅

主持人: 鲁东

15:50 - 16:05 Monotonic optimization with application to the selection of parameters for LWE-based encryption schemes (abstract) P.63

徐娟 (中国科学院重庆绿色智能技术研究院)

16:05 - 16:20 A Positivstellensatz on the Matrix Algebra of Finitely Generated Free Group (abstract) P.64

Liang Hao (Academy of Mathematics and Systems Science)

16:20 - 16:35 An algorithm for computing comprehensive order basis systems of parametric polynomial matrices (abstract) P.64

杨润河 (中国科学院信息工程所)

16:35 - 16:50 Gröbner Basis of the Defining Ideal of Quaternionic Polynomial Ring in Symbolically Many Quaternionic Variables (abstract) P.64

王正阳 (中国科学院数学与系统科学研究院数学机械化重点实验室)

16:50 - 17:05 Construction of three class of at most four-weight binary linear codes and their applications (abstract) P.65

张同慧 (福建师范大学)

闭幕式

6 月 16 日 17:10-17:30　重庆厅

晚餐

6 月 16 日 18:00-19:30　大宴会 A 厅

[P000113]

四色问题与子图覆盖

* 范更华 (福州大学)

1976 年，数学史上有着重要影响的四色问题在计算机的帮助下被解决了，这是数学发展史上的一个标志性事件，开启了使用计算机解决数学问题的时代。数学家寻求四色定理的纯推理证明仍在继续。我们将简要介绍与四色问题相关的若干图论著名问题，如哈密顿圈问题、整数流理论、子图覆盖等，同时简述图论在芯片设计 EDA 软件中的某些应用。

– – –– o – – –– o – – –– o – – –– o – – ––

[P000114]

Algebra, Combinatorics and Cryptography

* 王华雄 (新加坡南洋理工大学)

Algebra and combinatorics play crucial roles in the field of cryptography. Algebraic structures, such as groups, rings, and fields, form the foundation of many cryptographic algorithms. For example, the RSA encryption algorithm relies on properties of prime numbers and modular arithmetic, both of which are rooted in algebra. Elliptic curve cryptography (ECC) is another application that uses the algebraic structure of elliptic curves over finite fields to create efficient and secure cryptographic schemes. Combinatorics, the study of counting, arrangement, and combination, is essential for analyzing and designing cryptographic protocols. It helps in understanding the complexity and security of these protocols. For instance, combinatorial designs and permutations are used in the construction of block ciphers like the Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The synergy of algebra and combinatorics provides robust tools for developing and analyzing cryptographic systems.

In this talk, I will present several concrete examples to illustrate how the interplay between algebra and combinatorics enriches cryptography in the constructions of cryptographic schemes such as secret sharing and secure multiparty computation.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000098]

Fast Fourier Transform via automorphism groups of rational function fields

* 邢朝平 (上海交通大学)

The Fast Fourier Transform (FFT) over a finite field $\mathbb{F}_q$ computes evaluations of a given polynomial of degree less than n at a specifically chosen set of n distinct evaluation points in $\mathbb{F}_q$. If q or $q-1$ is a smooth number, then the divide-and-conquer approach leads to the fastest known FFT algorithms. Depending on the type of group that the set of evaluation points forms, these algorithms are classified as multiplicative (Math of Comp. 1965) and additive (FOCS 2014) FFT algorithms. In this talk, we provide a unified framework for FFT algorithms that include both multiplicative and additive FFT algorithms as special cases, and beyond: our framework also works when $q+1$ is smooth, while all known results require q or $q-1$ to be smooth. For this new smooth $q+1$ case, we show that if n is a divisor of $q+1$ that is B-smooth for a real $B>0$, then our FFT needs $O(B\cdot n\cdot \log n)$ arithmetic operations in $\mathbb{F}_q$. Our unified framework is a natural consequence of introducing the algebraic function fields into the study of FFT.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000105]

Symmetric structures in the Bruhat order

* 高奕博 (北京国际数学研究中心)

The Bruhat order encodes algebraic and topological information of Schubert varieties in the flag manifold and possesses rich combinatorial properties. In this talk, we discuss some interrelated stories regarding the Bruhat order: self-dual Bruhat intervals, minimal exponents in the Kazhdan-Lusztig polynomials, Billey-Postnikov decompositions and automorphisms of the Bruhat graph. This is joint work with Christian Gaetz.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000107]

Linear codes from Boolean functions with high (fast) algebraic immunity

* 唐春明 (西南交通大学)

In the talk, we propose a new parameter to measure the resistance of a Boolean function to fast algebraic attack. We also introduce the notion of fast immunity profile and show that it informs both on the resistance to standard and fast algebraic attacks. Further, a coding-theory approach to the characterization of perfect algebraic immune functions is presented. Via this characterization, infinite families of binary linear complementary dual codes (or LCD codes for short) are obtained from perfect algebraic immune functions. Moreover, two methodologies for constructing minimal binary codes from sets, Boolean functions and vectorial Boolean functions with high algebraic immunity, are proposed. More precisely, a general construction of new minimal codes using minimal codes contained in Reed-Muller codes and sets without nonzero low degree annihilators is presented. The other construction allows us to yield minimal codes from certain subcodes of Reed-Muller codes and vectorial Boolean functions with high algebraic immunity.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000003]

COMPLEXITY OF SKEW POLYNOMIAL MULTIPLICATION

* 陈琦元 (中科院数学与系统科学研究院)　叶科 (中科院数学与系统科学研究院)

We establish a lower bound for the complexity of multiplying two skew polynomials. The lower bound coincides with the upper bound conjectured by Caruso and Borgne in 2017, up to a log factor. We present algorithms for three special cases, indicating that the aforementioned lower bound is quasi-optimal. In fact, our lower bound is quasi-optimal in the sense of bilinear complexity.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000032]

Applicability of the Cayley Transform

* 陆镜宇 (中国科学院数学与系统科学研究院)　叶科 (中国科学院数学与系统科学研究院)

Cayley transform is a technique to project from Lie algebra to the underlying Lie group. The

transform is widely employed as a retraction map for Riemannian optimization. In this talk, we consider the applicability of the Cayley transform of the general Lie group and its representations, which is closely related to the power span property of the representation of Lie algebra. For semisimple Lie algebra, the weights of the representation can be characterized in detail, under the assumption of power span property.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000050]

Sparse Polynomial Interpolation With Error Correction: Higher Error Capacity by Randomization

Kaltofen Erich L. (Department of Mathematics, North Carolina State University; Department of Computer Science, Duke University) * 杨志红 (中南大学数学与统计学院)

In [IEEE Trans. Information Theory, vol. 67, nr. 1 (2021)] we have presented error-correcting algorithms that interpolate sparse univariate polynomials from values at arguments which the algorithms compute. We have assumed that the input polynomials are sparse in terms that are powers of the variable (standard basis) or sparse in Chebyshev basis polynomials. We recover all polynomials of sparsity $\leq B$ that from our N input points interpolate at least $N - E$ of the points, that is, correct $\leq E$ errors in the values at the error capacity E/N. Our IEEE Transactions algorithms have, roughly, an error capacity of $0.75/B$ for power basis and $0.66/B$ for Chebyshev basis.

We present algorithms which randomly select values from sufficiently large finite sets before evaluation, and then return the sparse interpolant in a list of valid interpolants with high probability. The error capacity of our algorithms for both power and Chebyshev bases is, roughly, $1/B$. More precisely, we recover the interpolant from $N = \lfloor E/2 + 1 \rfloor (2B + 1)$ values with probability $\geq 1 - \epsilon$ when sampling from sets that have $\geq 16 \lfloor E/2 + 1 \rfloor D B^2/\epsilon$ elements, where D is an upper bound on the degree of the polynomial. Our algorithms are based on Prony's interpolation algorithm and perform exact arithmetic in the field of scalars, which for Chebyshev basis is required to have characteristic $\neq 2$. The running time is polynomial in the bounds B, E and D or $\log(D)$, depending on the representation of the scalar field elements.

In the special case of evaluations at positive real numbers, as a consequence of Descartes's Rule of Signs, our algorithms recover a unique real interpolant for $B, E \geq 2$, and for sparsity in both standard and Chebyshev bases can be de-randomized to deterministic versions.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000067]

Reduced Grobner Bases of Schubert Determinantal Ideals

牟晨琪 (北京航空航天大学)　* 宋秋叶 (北京航空航天大学)

Schubert determinantal ideals are an important class of polynomial ideals that have attracted significant attention in algebraic combinatorics, representation theory, and computational algebra in the last two decades. The Schubert determinantal ideal of a permutation is naturally associated with the matrix Schubert variety and is closely related to the double Schubert polynomial of that permutation.

In particular, with Fulton generators identified as Grobner bases of Schubert determinantal ideals w.r.t. any anti-diagonal term order, minimal Grobner bases for such ideals were also studied, where the authors introduced the notion of elusive minors and proved that they form minimal Grobner bases of Schubert determinantal ideals. Furthermore, for Schubert determinantal ideals, while all the elusive minors form the reduced Grobner bases when the defining permutations are vexillary, in the non-vexillary case we derived an explicit formula for computing the reduced Grobner basis from elusive minors which avoids all algebraic operations. Based on this explicit formula, we developed an algorithm named RedGBSchubert to compute the reduced Grobner bases of Schubert determinantal ideals, where this new algorithm outperforms the built-in function InterReduce in Maple for computing the reduced grobner bases for complex Schubert determinantal ideals in terms of computational efficiency.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000014]

Lightweight Dynamic Broadcast Proxy Re-Encryption for Data Sharing in Clouds

* 胡慧丹 (福建师范大学)　曹珍富 (华东师范大学)　董晓蕾 (华东师范大学)　陆鹏浩 (华东师范大学)

Cloud computing has become prevalent in the sharing of outsourced data because of its strong computing power and storage capacity. Ensuring data security is vitally important for data sharing in clouds. Recently, numerous broadcast proxy re-encryption (BPRE) schemes have been designed to solve the data security issues of such applications. But no BPRE schemes are designed to resolve the issues of re-encryption key updating for data sharing in a dynamic cloud environment. Therefore, we put forward a lightweight dynamic broadcast proxy re-encryption scheme (LD-BPRE) to resolve the above-mentioned issue in dynamic settings in which the data owner can dynamically change a group of data users and he/she does not need to update the re-encryption key for a new set of data users. That is, the proxy can re-set a re-encryption ciphertext for a new set of delegatees using the original re-encryption key. It is significant in a dynamic cloud setting and causes convenience for cloud users. LD-BPRE is lightweight for

the user with low-power devices because most computing overhead is offloaded to the clouds. We formally provide the definition for LD-BPRE and prove its security under a decision n-BDHE assumption without the random oracle. Finally, extensive comparisons and experiments indicate that LD-BPRE is efficient and practical.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000015]

Linear Complementary Dual Codes Constructed from Reinforcement Learning

* 吴严生 (南京邮电大学计算机学院)　马金 (南京邮电大学计算机学院)　杨尚东 (南京邮电大学计算机学院)

Abstract: Recently, Linear Complementary Dual (LCD) codes have garnered substantial interest within coding theory research due to their diverse applications and favorable attributes. This study centers around the generation of binary and ternary LCD codes via a curiosity-driven Reinforcement Learning (RL) approach, where custom-designed reward functions direct the AI in structuring new LCD codes. It particularly emphasizes optimizing action-state mappings to craft ternary LCD codes. Experimental results reveal that RL-based LCD codes demonstrate superior error correction properties compared to conventionally constructed LCD codes and those derived from general RL methods. The paper introduces novel binary and ternary LCD codes with enhanced minimum distance bounds. Finally, it showcases how Random Network Distillation aids agents in exploring beyond local optima, enhancing the overall performance of the models without compromising convergence.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000022]

Generalized Hamming weights of linear codes from defining sets

* 刘超 (湖北大学)

The generalized Hamming weight of linear codes is a natural generalization of the minimum Hamming distance. They convey the structural information of a linear code and determine its performance in various applications, and have become one of important research topics in coding theory. Recently, Li (IEEE Trans. Inf. Theory, 67(1): 124-129, 2021) and Li and Li (Discrete Math., 345: 112718, 2022) obtained the complete weight hierarchy of linear codes from quadratic forms over finite fields of odd characteristic

by analysis of the solutions of the restricted quadratic equation in its subspace. In this talk, we further determine the complete weight hierarchy of linear codes from quadratic forms over finite fields of even characteristic by carefully studying the behavior of the corresponding restricted quadratic forms to the subspaces of the field, and complement the results of Li and Li. In addition, we investigate the generalized Hamming weights of a class of linear code over $_q$, which is constructed from defining sets. These defining sets are either special simplicial complexes or their complements in ^m_q. We determine the complete weight hierarchies of these codes. This talk is based on a joint work with Dabin Zheng and Xiaoqiang Wang.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000059]

基于双循环编码的同态密文矩阵操作

陈经纬 (中国科学院重庆绿色智能技术研究院生物计算安全重庆市重点实验室)　* 杨林翰 (重庆交通大学信息科学与工程学院)　吴文渊 (中国科学院重庆绿色智能技术研究院生物计算安全重庆市重点实验室)　刘洋 (重庆交通大学信息科学与工程学院)　冯勇 (中国科学院重庆绿色智能技术研究院生物计算安全重庆市重点实验室)

同态加密矩阵运算广泛用于各种隐私保护应用中，因而如何降低加密矩阵运算成本是一个关键的课题，目前已有众多研究对此进行了探讨。本文介绍了一种新的矩阵编码方法，名为双循环编码，在此基础上我们提出了几种新的加密矩阵乘法算法。其中基础双循环算法在理论上优于现有的最先进算法；而进一步改进双循环算法得到了适用于小规模矩阵运算的改进双循环算法，在理论和实践上均表现优异；另一个则结合分段策略设计的 LongRot 算法，在实践中表现良好，尤其适用于高维度矩阵。此外，我们的算法在矩阵尺寸上提供了更大的灵活性，而大多数以往的研究都集中在正方形矩阵乘法上。双循环编码的另一个值得注意的优势是，它允许完全免费地对加密矩阵进行转置。对比分析和实验结果表明，本文中引入的每种算法在特定场景下均优于现有算法，实现了从 2 倍至 38 倍的速度提升。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000101]

Recent progress on graph chromatic thresholds and graph homomorphism thresholds

* 上官冲 (山东大学)

In this talk I will give a brief introduction to graph chromatic thresholds and graph homomorphism thresholds, and survey some recent progress. In particular, I will discuss how they are related to discrete geometry and the theory of VC dimensions.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000109]

A Framework for Safe Probabilistic Invariance Verification of Stochastic Dynamical Systems

* 薛白 (中国科学院软件所)

Ensuring safety through set invariance has proven to be a valuable method in various robotics and control applications. This paper introduces a comprehensive framework for the safe probabilistic invariance verification of both discrete- and continuous-time stochastic dynamical systems over an infinite time horizon. The objective is to ascertain the lower and upper bounds of the liveness probability for a given safe set and set of initial states. This probability signifies the likelihood of the system remaining within the safe set indefinitely, starting from the set of initial states. To address this problem, we propose optimizations for verifying safe probabilistic invariance in discrete-time and continuous-time stochastic dynamical systems. These optimizations adapt classical stochastic barrier certificates, which are based on Doob's non-negative supermartingale inequality, and the equations described in [Xue21, Xue23], which can precisely define the probability of reaching a target set while avoiding unsafe states. Finally, we demonstrate the effectiveness of these optimizations through several examples using semi-definite programming tools.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000006]

Unimodality of certain partition polynomials

* Guo Wan-Ming (School of Mathematical Sciences, Qufu Normal University) Zhu Bao-Xuan (School of Mathematics and Statistics, Jiangsu Normal University)

Let β be an integer and satisfy $0 \leq \beta \leq 5$. In this paper, we prove that the partition polynomial

$$\prod_{k=1}^{n}[1+(2+\beta)q^k+q^{2k}]$$

is symmetric and unimodal for $n \geq 1$.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000011]

Explicit formulas for a family of hypermaps beyond the one-face case

* Bai Ziwei (合肥工业大学)

Enumeration of hypermaps (or Grothendieck' s dessins d' enfants) is widely studied in many fields. In particular, enumerating hypermaps with a fixed edge-type according to the number of faces and genus is one topic of great interest. The first systematic study of hypermaps with one face and any fixed edge-type is the work of Jackson (1987) [23] using group characters. Stanley later (2011) obtained the genus distribution polynomial of one-face hypermaps of any fixed edge-type expressed in terms of the backward shift operator. There is also enormous amount of work on enumerating one-face hypermaps of specific edge-types. Hypermaps with more faces are generally much harder to enumerate and results are rare. Our main results here are formulas for the genus distribution polynomials for a family of typical two-face hypermaps including almost all edge-types, the purely imaginary zeros property of these polynomials, and the log-concavity of the coefficients.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000030]

Fast Numerical Evaluation of Generalized Todd Polynomials

辛国策 (首都师范大学)　* 张英瑞 (中国科学院数学与系统科学研究院)　张子豪 (首都师范大学)

The Todd polynomials $td_k = td_k(b_1, b_2, \ldots, b_m)$ are defined by their generating functions

$$\sum_{k\geq 0} td_k s^k = \prod_{i=1}^{m} \frac{b_i s}{e^{b_i s} - 1}.$$

It appears as a basic block in Todd class of a toric variety, which is important in the theory of lattice polytopes and in number theory. We find generalized Todd polynomials arise naturally in MacMahon's partition analysis, especially in Ehrhart series computation. We give a fast evaluation of generalized Todd polynomials for numerical b_i's. In order to do so, we develop fast operations in the quotient ring $\mathbb{Z}_p[[s]]$ modulo s^{d+1} for large prime p. As an application, we recompute the Ehrhart series of magic squares of order 6, which was first solved by the first named author. The running time is reduced from 70 days to about 1 day.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000068]

多元多项式矩阵等价的进一步的结果

* 关剑成 (湖南科技大学)　刘金旺 (湖南科技大学)　李冬梅 (湖南科技大学)

这篇论文研究了行列式是某个一元不可约的 2 阶多元多项式矩阵的等价问题。我们首先把 Vaserstein 的一个整体-局部定理从行向量的情形推广到矩阵的情形，然后我们利用这个结果给出了行列式是某个一元不可约的 2 阶多元多项式矩阵等价于它的 Smith 型的一个充要条件。

– – –– o – – –– o – – –– o – – –– o – – ––

[P000071]

The Smith normal form and reduction of weakly linear matrices

刘金旺 (湖南科技大学)　* 吴弢 (湖南科技大学)　康莹 (湖南科技大学)

Smith normal Form play the important role in the reduction of a multidimensional system; In this paper, we investigate the reduction of weakly linear multivariate polynomial matrix which with the determinant is the product of two distinct multivariate weakly linear polynomials;We give the sufficient and necessary conditions for such a matrix to be equivalent to its Smith normal Formal.Furthermore by the new results, we will extend an algorithm of reducing weakly linear multivariate polynomial matrices to their Smith normal forms.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000029]

三维空间中顶点同构型的多面体

曾振柄 (上海大学理学院数学系)　* 武斌 (上海财经大学浙江学院)　斯亚民 (上海财经大学浙江学院)　饶永生 (广州大学计算科技学院)

本文研究三维空间中具有顶点同构型性质的多面体的分类问题. 这种多面体包括正多面体、阿基米德多面体、棱柱、反棱柱, 其表面不限于正多边形. 本文证明这样的多面体，除了棱柱、反棱柱以外, 最多有有限种不同组合型. 我们构造了顶点类型参数满足的一个不定方程, 并借助计算机辅助推理得到该不定方程的所有整数解, 证明除了棱柱体和反棱柱体以外, 这类多面体可分为有限种.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000036]

Hybrid Controller Synthesis for Nonlinear Systems Subject to Safety Constraints

* Qi Niuniu (East China Normal University) Zeng Xia (Southwest University) Liu Banglong (East China Normal University) Yang Zhengfeng (East China Normal University)

This paper has presented an iterative approach to synthesizing hybrid polynomial-DNN controllers for nonlinear systems such that the closed-loop system can be both well-performing and easily verified upon required properties. Our approach has creatively integrated low-degree polynomial fitting and knowledge distillation into the RL method during the construction process. Thanks to the special feature of the hybrid controller, the controlled system can be transformed into the polynomial form. By utilizing the SOS relaxation method and solving LMI constraints efficiently, we can generate barrier certificates to verify the safety properties of the nonlinear control systems equipped with our synthesized hybrid controllers. Extensive experiments consistently demonstrate the effectiveness and scalability of the proposed approach.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000077]

滤子扩张原则的 Coq 形式化

* 窦国威 (北京邮电大学) 郁文生 (北京邮电大学)

数学定理的计算机形式化证明，近年来随着计算机科学的迅猛发展，特别是证明辅助工具 Coq 的出现，取得了长足的进展。Coq 是一个交互式定理证明与程序开发系统，可用于描述定理内容和验证定理证明。Coq 的交互式编译环境使用户以人机对话的方式一问一答，边设计边修改，使证明中的疏漏及时得到补证。进入 21 世纪以来，随着“四色定理”、“有限单群分类定理”及“Kepler 猜想”等一系列著名数学难题形式化证明的实现，各种计算机证明辅助工具在学术界得到广泛认可。

滤子扩张原则 (Filter Extension Principle) 是滤子 (filter) 相关理论中的一个重要定理，它断言每一个滤子都可以扩张成为一个超滤 (ultrafilter)。非主超滤 (non-principal ultrafilter) 作为一类特殊超滤，在逻辑学、集合论、拓扑学、模型论等领域均有运用。特别地，非主超滤还可用于代数结构的非标准扩张，例如非标准分析基础——超实数 (hyper-real numbers) 的构造。目前尚未见到直接构造非主超滤的方法，其存在性一般需要借助选择公理 (Axiom of Choice) 进行证明。作为选择公理的结论，滤子扩张原则可简化非主超滤存在性的证明，使其在形式化的过程中更易使用。

滤子扩张原则的形式化基于 Coq 中的 Morse-Kelley(MK) 公理化集合论形式化系统。MK 公理化集合论承认比集合更广之“类 (class)”作为基本研究对象，一个类被称为集合当且仅当它可属于任意另一个类。相比数学上使用较多的 Zermelo-Fraenkel(ZFC) 公理化集合论，MK 是 ZFC 的真扩展，在形式化过程中使用起来更为便利。

滤子扩张原则的形式化涉及诸多滤子概念，包括且不限于滤子 (filter)、超滤 (ultrafilter)、主超滤 (principal ultrafilter)、非主超滤 (non-principal ultrafilter) 等。所有相关定义、定理以及滤子扩张原则均在 Coq 证明工具中得到完整形式化描述和验证。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000086]

基于 Lean 的组合恒等式自动化证明

* 熊贝贝 (华东师范大学)　王怡然 (青岛大学)　王建林 (河南大学)　杨争锋 (华东师范大学)

在大型语言模型和 *Lean* 等证明助手的帮助下, 自动化证明数学定理展现出了广阔的前景. 然而, 由于公开数据匮乏, 数据专业性强以及计算量庞大的问题, 形式化证明的机器学习方法面临瓶颈. 为了解决数据稀缺的问题, 本文构建了一个专注于组合数学的全新基准, 名为 *Comlib*. 具体地, 首先通过 *Lean* 形式化证明了 500 多个新定理, 其中包括吸收定理, 并行求和等多个经典组合数学定理. 在此基础上, 本文提出了一种融合搜索和预测的数据增强方法, 进一步扩大了基准的数据量. 在一组标准基准上进行了对比评估所提出的数据增强方法, 结果验证了我们数据集的有效性和数据增强方法的适用性.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000116]

Maple 2024 新功能介绍

* 林成青 (Maplesoft)

Maple MapleSim 2024 版本已发布，本次报告将介绍 Maple 2024 中的新功能，包括新增加的 AI 公式助手和自然语言包、Simplify 命令增强、命令的自动参数补全、Matroid 和 Hypergraphs 函数包、信号处理、更多问题的分步求解步骤、可视化、以及更多的高级数学功能等。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000094]

Recent progress on random graph matching problems

* 丁剑 (北京大学)

A basic goal for random graph matching is to recover the vertex correspondence between two correlated graphs from an observation of these two unlabeled graphs. Random graph matching is an important and active topic in combinatorial statistics: on the one hand, it arises from various applied fields such as social network analysis, computer vision, computational biology and natural language processing; on the other hand, there is also a deep and rich theory that is of interest to researchers in statistics, probability, combinatorics, optimization, algorithms and complexity theory.

Recently, extensive efforts have been devoted to the study for matching two correlated Erdős–Rényi graphs, which is arguably the most classic model for graph matching. In this talk, we will review some recent progress on this front, with emphasis on the intriguing phenomenon on (the presumed) information-computation gap. In particular, we will discuss progress on efficient algorithms thanks to the collective efforts from the community. We will also point out some important future directions, including developing robust algorithms that rely on minimal assumptions on graph models and developing efficient algorithms for more realistic random graph models.

This is based on joint works with Hang Du, Shuyang Gong, Zhangsong Li, Zongming Ma, Yihong Wu and Jiaming Xu.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000097]

零误差计算

* 冯勇 (中国科学院重庆绿色智能技术研究院)

符号计算获得准确值, 一些领域如自动推理需要准确值, 人们就采用符号计算来获得. 由于符号计算存在中间结果膨胀等问题使得其计算的效率不高, 解决问题的规模不大等劣势, 已成为制约这一领域发展的瓶颈. 数值计算有计算效率高、解决问题规模大的优势, 然而数值计算获得的是近似值, 近似计算的结果与准确值之间有一个间隙. 研究采用有误差的数值计算来获得无误差的准确结果就具有重要的理论价值和应用价值. 采用数值计算获得准确值又称为零误差计算. 本报告首先回答哪类数可以开展零误差计算: 可以归结为一致离散集合中的数可以开展零误差计算, 即有非零隔离界的数集. 这是“数”可以零误差计算的一个充要条件. 以此为基本出发点, 分析了代数数零误差计算的最低理论. 该理论就是近似代数数恢复其准确值的必要的误差控制, 但是这一理论因算法条件的限制, 往往不能保证成功恢复出代数数的准确值. 因此, 本报告将给出采用 PSLQ 算法进行代数数零误差计算所需的误差控制, 与基于 LLL 的算法相比, 关于代数数次数的依赖程度由二次降低为拟线性. 最后, 本报告也将探讨零误差计算未来的研究趋势.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000115]

Symbolic approach to combinatorial relations

* 杨立波 (南开大学)

In recent years symbolic computation algorithms have been proven to be powerful tools for solving longstanding open problems in combinatorics, such as George Andrews' and David Robbins' q-TSPP-conjecture and Ira Gessel's lattice path conjecture. In this talk, I will present some combinatorial relations via symbolic approach, including some identities in enumerative combinatorics, some congruences in combinatorial number theory, and some inequalities in analytic combinatorics.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000106]

Quantifying low rank approximations of third order symmetric tensors

* 胡胜龙 (杭州电子科技大学)

In this talk, we present a method to certify the approximation quality of a low rank tensor to a given third order symmetric tensor. Under mild assumptions, best low rank approximation is attained if a control parameter is zero or quantified quasi-optimal low rank approximation is obtained if the control parameter is positive. This is based on a primal-dual method for computing a low rank approximation for a given tensor. The certification is derived from the global optimality of the primal and dual problems, and is characterized by easily checkable relations between the primal and the dual solutions together with another rank condition. The theory is verified theoretically for orthogonally decomposable tensors as well as numerically through examples in the general case.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000108]

Quantum advantage for near-term and fault-tolerant quantum computers

* 袁骁 (北京大学前沿计算研究中心)

Quantum computer have the potential to solve classically intractable problems. However, realizing a universal quantum computer is challenging with current technology. Before having a fully-fledged

quantum computer, a more realistic question is what we can do with current and near-term quantum hardware. In this talk, I will first review the quantum algorithms that are designed for near-term and fault-tolerant quantum computers and discuss the challenges and possibilities to realize quantum advantages. Then, I will propose to focus more on the early-fault tolerant era and discuss what we should do next to achieve quantum advantage.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000009]

Krylov subspace methods based quaternion tensor form for generalized Sylvester quaternion tensor equation with application to color video denoising

蔡小敏 (福建师范大学)　* 吴玉玲 (福建师范大学)　柯艺芬 (福建师范大学)　廖日威 (福建师范大学)　谢亚君 (福州外语外贸学院)

In this paper, we consider Krylov subspace methods based quaternion tensor form for a class of generalized Sylvester quaternion tensor equation. A novel quaternion tensor product and a global quaternion Arnoldi process based on the tensor form are proposed. Then, the quaternion tensor Krylov subspaces and their orthogonal bases are constructed via the proposed global quaternion Arnoldi process. The quaternion full orthogonalization method based on tensor format (denoted by QFOM−BTF) and the quaternion generalized minimal residual method based on tensor format (denoted by QGMRES−BTF) are established to solve the quaternion tensor equation. The theoretically analyze results of the proposals are discussed on the quaternion tensor form. Finally, we demonstrate the feasibility of QFOM−BTF and QGMRES−BTF methods on some numerical examples including the color video denoising.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000061]

Structural Analysis by Generalized Embedding Method for Integro-differential-algebraic Equations

* 杨文强 (中国科学院重庆绿色智能技术研究院)　吴文渊 (中国科学院重庆绿色智能技术研究院)　冯勇 (中国科学院重庆绿色智能技术研究院)　Reid Greg (University of Western Ontario)

Structural analysis is essential for understanding the characteristics of integro differential algebraic equations (IDAEs) before numerical analysis. The Σ-method, utilizing the signature matrix, effectively

analyzes differential-algebraic equations (DAEs) and extends to IDAEs. Challenges arise when the signature matrix becomes undefined or overestimated due to integrated derivatives in IDAEs. Additionally, when a singular Jacobian matrix is yielded after applying the Σ-method, existing conversion methods may fail to ensure process termination. This paper addresses these issues by splitting an IDAE into two parts, redefining the signature matrix for each, and introducing a new degrees of freedom measure to ensure conversion method termination. Furthermore, a point-based on a detection method corrects signature matrix overestimation. Finally, an embedding method regularizes nonlinear IDAEs with singular Jacobian matrices. When coupled with the collocation method, it can effectively solve a general IDAE numerical

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000081]

Computation of Regular Tucker Decompositions by Tensor QR Method

Xu Changqing (苏州科技大学) * Zhai Ziqi (苏州科技大学) Wang Li (苏州科技大学)

The theory of tensor has gained significant attentions and has been applied in many fields such as computer vision, clustering, quantum mechanics at el. due to its capability to extract essential information from high-order complex dataset. In this paper, we introduce the definition of regular Tucker decomposition for high order tensors, and use the Tensor QR method to compute a regular Tucker decomposition.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000005]

Logarithmic norm minimization of quaternion matrix decomposition for color image sparse representation

* 蔡小敏 (福建师范大学) 柯艺芬 (福建师范大学) 马昌凤 (福建师范大学) 谢亚君 (福州外语外贸学院) 廖日威 (福建师范大学)

In this paper, incorporating the quaternion matrix framework, the logarithmic norm of quaternion matrices is employed to approximate rank. Unlike conventional sparse representation techniques for matrices, which treat RGB channels separately, quaternion-based methods maintain image structure by representing color images within a pure quaternion matrix. Leveraging the logarithmic norm, factorization

and truncation techniques can be applied for proficient image recovery. Optimization of these approaches is facilitated through an alternate minimization framework, supplemented by meticulous mathematical scrutiny ensuring convergence. Finally, some numerical examples are used to demonstrate the effectiveness of the proposed algorithms.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000016]

Quantum spectral method for gradient and Hessian estimation

* 张宇欣 (中国科学院数学与系统科学研究院)　邵长鹏 (中国科学院数学与系统科学研究院)

In [GAW19], Gilyén, Arunachalam and Wiebe proposed a quantum algorithm for computing the gradient of real-valued smooth functions $f : \mathbb{R}^d \to \mathbb{R}$. The algorithm is optimal for a class of smooth functions with query complexity $\widetilde{O}(\sqrt{d}/\varepsilon)$. In this work, we consider the same problem but for complex-valued analytic functions $f : \mathbb{C}^d \to \mathbb{C}$. Assuming that $f(x) \in \mathbb{R}$ for all $x \in \mathbb{R}^d$, we propose a quantum algorithm of complexity $\widetilde{O}(1/\varepsilon)$, which is only polylogarithmic in dimension. As f is complex-valued, we assume an oracle in the form $|x\rangle|0\rangle \to |x\rangle|f_1(x)\rangle|f_2(x)\rangle$, where $f_1(x), f_2(x)$ are respectively the real and imaginary parts of $f(x)$. In addition, we assume that $x = x_1 + ix_2 \in \mathbb{C}^d$ is stored as $|x_1\rangle|x_2\rangle$ in quantum registers. These settings differ from those in [GAW19], explaining why our algorithm does not contradict the optimality of their result. As an application, we provide a new quantum algorithm for estimating multiple expectation values. Under certain conditions, our algorithm uses exponentially fewer resources than the one given in [HWM22]. Finally, as a generalisation, we gave two quantum algorithms for computing the Hessian of f.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000033]

Quantum-Inspired Classical Algorithms for Solving Linear Feasibility Problems

* Zuo Qian (Peking University)　Li Tongyang (Peking University)

We present a classical algorithm for linear feasibility problems, where the input matrix A is stored in a data structure suitable for QRAM-based state preparation. Specifically, given an matrix $A \in R^{m\times n}$ with a vector $b \in R^m$ which supports certain efficient ℓ_2-norm importance sampling queries. Then, after $T = O(\|A\|_F^2 L^2 \log(1/\epsilon^2))$ steps of iteration, for some vector $x \in R^n$ satisfying $d(x_T, P) \leq \epsilon d(x, P)$, we can

output a measurement of $|x\rangle$ in the computational basis and output an entry of x with classical algorithms that run in $O(\|A\|_F^6\kappa_F^6 L^6/\epsilon^2)$ time, where L be a Hoffman constant and $\kappa_F = \|A\|_F\|A^\dagger\|$. Our work combines techniques from sketching algorithms and optimization with the quantum-inspired literature. This avenue shows promise for feasible implementations of classical linear inequality in quantum-inspired settings, offering a basis for comparison against future quantum computers.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000056]

Quantum recurrent neural networks for sequential learning

Li Yanan (Ocean University of China) * Wang Zhimin (Ocean University of China) Han Rongbing (Ocean University of China) Shi Shangshang (Ocean University of China) Li Jiaxin (Ocean University of China) Shang Ruimin (Ocean University of China) Zheng Haiyong (Ocean University of China) Zhong Guoqiang (Ocean University of China) Gu Yongjian (Ocean University of China)

Quantum neural network (QNN) is one of the promising directions where the near-term noisy intermediate-scale quantum (NISQ) devices could find advantageous applications against classical resources. Recurrent neural networks are the most fundamental networks for sequential learning, but up to now there is still a lack of canonical model of quantum recurrent neural network (QRNN), which certainly restricts the research in the field of quantum deep learning. In the present work, we propose a new kind of QRNN which would be a good candidate as the canonical QRNN model, where, the quantum recurrent blocks (QRBs) are constructed in the hardware-efficient way, and the QRNN is built by stacking the QRBs in a staggered way that can greatly reduce the algorithm' s requirement with regard to the coherent time of quantum devices. That is, our QRNN is much more accessible on NISQ devices. Furthermore, the performance of the present QRNN model is verified concretely using three different kinds of classical sequential data, i.e., meteorological indicators, stock price, and text categorization. The numerical experiments show that our QRNN achieves much better performance in prediction (classification) accuracy against the classical RNN and state-of-the-art QNN models for sequential learning, and can predict the changing details of temporal sequence data. The practical circuit structure and superior performance indicate that the present QRNN is a promising learning model to find quantum advantageous applications in the near term.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000054]

Quantum circuits for block encoding of structured matrices in ocean acoustics

Yang Chunlin (Harbin Engineering University) * Yao Hongmei (Harbin Engineering University) Zhang Guofeng (Department of Applied Mathematics, The Hong Kong Polytechnic University) Fan Zhaobing (Harbin Engineering University) Li Zexian (Department of Applied Mathematics, The Hong Kong Polytechnic University) Liu Jianshe (College of Underwater Acoustic Engineering, Harbin Engineering University)

ince operator in quantum computer can only be unitary, an input model is needed to make nonunitary operator can be implemented on a quantum computer. Block encoding is the technique that embeds a matrix A satisfying A 1 into a larger unitary matrix UA. In this paper, we discuss how to construct quantum circuits of block encoding for structured matrices and give some block encoding schemes. Two examples in fluid dynamics is used to illustrate the feasibility of our block encoding schemes. The corresponding codes of the quantum circuits in MATLAB are also given.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000017]

Whitney Stratification of Algebraic Boundaries of Convex Semi-algebraic Sets

* 代梓灏 (中国科学院数学与系统科学研究院) 李子佳 (中国科学院数学与系统科学研究院) 杨志红 (中南大学) 支丽红 (中国科学院数学与系统科学研究院)

Algebraic boundaries of convex semi-algebraic sets are closely related to polynomial optimization problems. Building upon Rainer Sinn’ s work, we refine the stratification of iterated singular loci to a Whitney (a)-regular stratification, which gives a list of candidates of varieties whose dual is an irreducible component of the algebraic boundary of the dual convex body. We also present an algorithm based on Teissier’ s criterion to compute Whitney (a) stratifications, which employs ideal saturation and prime decompositions of conormal spaces.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000018]

Qualitative Investigation of the Lorenz-84 System Using Computer Algebra Methods

* Song Jichao (Beihang University) Niu Wei (Beihang University) Huang Bo (Beihang University) Deng Le (Beihang University)

Lorenz-84 system was proposed about four decades ago, however, there are almost no analytical results on the equilibria and their local stability. The first objective of this paper is to fill this gap. We discuss the possibility of the existence of multiple equilibria and establish the conditions for a given number of equilibria to exist by using algebraic methods of resultant. Furthermore, we derive the stability conditions on the parameters of the system by using symbolic methods for solving semi-algebraic systems. The second objective is to investigate the zero-Hopf bifurcation of the Lorenz-84 system. By using the averaging method, we provide sufficient conditions for the existence of one limit cycle bifurcating from a zero-Hopf equilibrium of Lorenz-84 system. Several examples and numerical simulations are presented to verify the established results.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000019]

Efficient detection of redundancies in systems of linear inequalities

荆瑞娟 (江苏大学) Moreno Maza Marc (University of Western Ontario) * 谢岩峰 (中国科学院数学与系统科学研究院) 袁春明 (中国科学院数学与系统科学研究院)

Fourier-Motzkin elimination is a fundamental operation in polyhedral geometry. It can be performed by several equivalent procedures, which can be regarded as an adaptation of Gaussian elimination to systems of linear inequalities. Those procedures tend to generate large numbers of redundant inequalities. Efficiently detecting those redundancies is essential to obtain software implementation of practical interest. In this paper, we propose a detection technique. We demonstrate its benefits over alternative approaches. A detailed experimentation is reported.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000024]

Computing the greatest common divisor of several parametric univariate polynomials via generalized subresultant polynomials

Hong Hong (North Carolina State University) * Jing Yang (Guangxi Minzu University)

In this paper, we tackle the following problem: compute the gcd for *several* univariate polynomials with *parametric* coefficients. It amounts to partitioning the parameter space into "cells" so that the gcd has a uniform expression over each cell and constructing a uniform expression of gcd in each cell. We tackle the problem as follows. We begin by making a natural and obvious extension of subresultant polynomials of two polynomials to several polynomials. Then we develop the following structural theories about them.

1. We generalize Sylvester's theory to several polynomials, in order to obtain an elegant relationship between generalized subresultant polynomials and the gcd of several polynomials, yielding an elegant algorithm.
2. We generalize Habicht's theory to several polynomials, in order to obtain a systematic relationship between generalized subresultant polynomials and pseudo-remainders, yielding an efficient algorithm.

Using the generalized theories, we present a simple (structurally elegant) algorithm which is significantly more efficient (both in the output size and computing time) than algorithms based on previous approaches.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000042]

The Geometry of Cylindrical Algebraic Decomposition

* 陈日增 (北京大学数学科学学院)

Cylindrical Algebraic Decomposition (CAD) is a classical construction in real algebraic geometry. The original cylindrical algebraic decomposition was proposed by Collins, using the classical elimination theory. In this talk, we will show a geometric approach to the cylindrical algebraic decomposition developed in a recent preprint by the speaker. Instead of polynomials, the central object in the new geometric theory is region. We relate the construction of CAD to the geometric fiber classification problem in algebraic geometry, which allows a new perspective using techniques like Grothendieck's Generic Freeness and Hermite's Quadratic Forms, and a new algorithm for Cylindrical Algebraic Decomposition is developed.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000074]

Exploiting Sign Symmetries in Minimizing Sums of Rational Functions

* 郭峰 (大连理工大学)　王杰 (中科院数学与系统科学研究院)

In this talk, we will focus on the optimization problem of minimizing a sum of rational functions over a basic semialgebraic set. We provide a hierarchy of semidefinite relaxations that is dual to the generalized moment problem (GMP) approach due to Bugarin, Henrion, and Lasserre. The exploration of the dual aspect not only allows us to conduct a convergence rate analysis, but also leads to a sign symmetry adapted hierarchy of semidefinite relaxations. Moreover, we further reduce the complexity of semidefinite relaxations by exploiting both correlative sparsity and sign symmetries. Numerical experiments demonstrate the efficiency of our approach.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000075]

Strengthening Lasserre's Hierarchy in Real and Complex Polynomial Optimization

* 王杰 (中国科学院数学与系统科学研究院)

We establish a connection between multiplication operators and shift operators. Moreover, we derive positive semidefinite conditions of finite rank moment sequences and use these conditions to strengthen Lasserre's hierarchy for real and complex polynomial optimization. Integration of the strengthening technique with sparsity is considered. Extensive numerical experiments show that our strengthening technique can significantly improve the bound (especially for complex polynomial optimization) and allows to achieve global optimality at lower relaxation orders, thus providing substantial computational savings.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000035]

Algorithms for Hadamard products of rational functions

* Chen Shaoshi (中国科学院数学与系统科学研究院)　Fang Hanqian (中国科学院数学与系统科学研究院)

Hadamard products of power series was first introduced and studied by Hadamard in 1899. According to Hadamard's multiplication theorem, the Hadamard product of two rational power series is still rational. Hadamard products have many applications including functional transcendence in number theory and zeta functions of graphs in combinatorics. In this work, we present several algorithms for computing the Hadamard products of two rational functions and describe a class of rational functions whose Hadamard square have only one pole.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000034]

Symbolic Summation in Multivariate Difference Fields

杜丽欣 (Johannes Kepler University) * 卫亚蓉 (天津理工大学)

The bivariate difference field provides an algebraic framework for a sequence satisfying a recurrence of order two. Based on this, we focus on sequences satisfying a recurrence of higher order, and consider the multivariate difference field, in which the summation problem could be transformed into solving the first order difference equations. We then show a criterion for deciding whether the difference equation has a rational solution and present an algorithm for computing one rational solution of such a difference equation, if it exists. Moreover we get the rational solution set of such an equation.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000070]

基于图运算的多智能体系统通信拓扑优化

谭莹莹 (安徽建筑大学) * 徐仝友 (安徽建筑大学) 寇菲丹 (安徽大学) 刘松 (安徽大学)

简单无向图的拉普拉斯矩阵的次小特征值被称为图的代数连通度。对于通信拓扑为无向图的一阶多智能体系统，代数连通度越大，系统的一致性收敛速率越快。本文将一种边重连（即删边再加边）的图运算方法，用于优化多智能体系统的通信拓扑结构，使其对应图的代数连通度增加幅度最大，并提出了增加通信拓扑图的代数连通度，降低系统通信量的算法。对一个含有六个多智能体组成的系统进行仿真实验可知，该算法可提高多智能体系统误差趋于零的速度，加快系统的一致性收敛速率，并且通过减少系统达到一致时的通信次数，降低系统的通信量。

– – –– o – – –– o – – –– o – – –– o – – ––

[P000078]

Parity statistics on restricted permutations and the Catalan-Schett polynomials

林志聪 (山东大学)　* 刘静 (山东大学)　严慧芳 (浙江师范大学)

Motivated by Kitaev and Zhang's recent work on non-overlapping ascents in stack-sortable permutations and Dumont's permutation interpretation of the Jacobi elliptic functions, we investigate some parity statistics on restricted permutations. Some new related bijections are presented and two refinements of the generating function for descents over 321-avoiding permutations due to Barnabei, Bonetti and Silimbanian are obtained. In particular, an open problem of Kitaev and Zhang about non-overlapping ascents on 321-avoiding permutations is solved. The stack-sortable permutations are at the heart of our approaches.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000069]

Critical Points of Symmetric Forms over the Unit Sphere

Hong Hoon (Department of Mathematics, North Carolina State University)　* Xu Jia (Department of Mathematics, Southwest Minzu University)　Yao Yong (Chengdu Computer Application Institute, Chinese Academy of Sciences)

A symmetric form is a multivariate polynomial that is symmetric in the variables and its monomials have the same degree. Symmetric forms are ubiquitous in various areas of mathematics, including combinatorics, invariant theory, inequalities and so on. In the study and the application of symmetric forms, one of the crucial challenge is to understand the structure of their critical points over the unit sphere. In this talk, we report on a recent progress on this challenge.

We begin by showing how to partition the set of critical points into "cells" so that every critical point in a cell has the same combinatorial structure. Then, by applying the obtained partition, we tackled the following tasks:

- Determine the number of critical points up to symmetry.
- Determine the structure of an optimal critical point.

For symmetric forms of degree 1 and 2, the tasks are trivial. However, for symmetric forms of degree 3, the tasks are non-trivial. Hence, we tackled the smallest non-trivial case (degree 3) and report on the findings. First, we briefly provide some notations in order to state our main theorems. Note that the critical set C has the following obvious symmetries.

- $c \in C \iff \pi(c) \in C$ for every permutation π.

We write $c \equiv c'$ if c and c' are equivalent up to the symmetry, that is $c' = \pi(c)$ for some π. Thus let $\#\overline{C}$ denote the number of the critical points up to symmetry.

The main results are the following two theorems.

Theorem 1 (Combinatorics). *Let $f \in \mathbb{R}[x_1, \ldots, x_n]$ be a symmetric form of degree $d = 3$. If the critical set C is finite, then we have*

$$\#\overline{C} = 1 + \#\ of\ positives\ in\ (D_{1,n-1}, \ldots, D_{n-1,1}),$$

where

$$D_{pq} = 9a_3^2 - 4pq\left(a_{21}^2 + 3a_{111}(3a_3 + na_{21})\right).$$

The second main theorem is derived from the following research history. In 1987, Choi, Lam and Reznick made a systematic study of even symmetric sextics. Their result implies that the optimal value of symmetric cubic forms on the standard simplex is always obtained at the center of some facets,

$$(0, \cdots, 0, \underbrace{\frac{1}{q}, \cdots, \frac{1}{q}}_{q}), \quad 1 \le q \le n.$$

What would happen if the standard simplex were replaced by the unit sphere? The answer is on $(s, t, \cdots, t)$.

Theorem 2 (Optimal). *Let $f \in \mathbb{R}[x_1, \ldots, x_n]$ be a symmetric form of degree $d = 3$. There is a maximizer (minimizer) of f over the unit sphere $\mathbb{S}^{n-1}$ with type $(s, t, \cdots, t)$ ($s = t$ $s = t$ is allowed).*

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000102]

无量词非线性公式可满足性问题的求解方法

* 李昊坤 (华为 2012 可信费马实验室)

非线性公式的可满足性问题不仅是理论研究的热点，也是程序验证中的一个核心问题。本报告专注于介绍无量词非线性公式的求解方法，包括利用多项式的弦结构优化圆柱代数分解（CAD）的投影序列，通过单胞腔投影操作符更有效地与冲突驱动的子句学习（CDCL）策略结合，以及使用局部搜索算法快速寻找解。报告最后还将介绍求解超越方程和混合三角多项式的方法。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000103]

结构化网格生成中的关键问题及其计算共形几何解决方案

* 郑晓朋 (大连理工大学)

网格生成对于高速、高精度仿真非常重要，是 CAD。结构化网格具有存储资源省、计算精度高、收敛速度快等优点，但其自动化生成一直是个巨大的挑战。本报告针对结构化四边形网格和六面体网格，分别分析其自动化生成的关键难题，给出基于计算共形几何的相关理论、算法和解决方案。

结构化四边形网格生成的奇异点分布合法性和合理性是其自动化高质量生成的关键。本报告介绍奇异点分布的 Abel-Jacobi 理论，该理论首次从根本上解决了奇异点合法性问题；本报告进一步介绍融合了 Ricci Flow 参数化、叶状结构和最优传输密度控制的结构化四边形网格自动化生成算法流程。

结构化六面体网格生成是网格生成领域的 “圣杯” 问题。表面四边形网格约束下的六面体网格生成是一类具有巨大工程应用价值的方法，其六面体网格存在性已被菲尔兹奖得主 Thurston 等数学家证明，但其普适算法仍是开放问题。本报告基于四边形和六面体网格拓扑变换给出一套自动化算法，该算法在施耐德金字塔等表面约束耦合复杂的上百个模型上测试成功。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000002]

Numerical simulation of heat transfer and entropy generation due to the nanofluid natural convection with viscous dissipation in an inclined square cavity

李树光 (大连海事大学)　* 吕龙杰 (大连海事大学)　廖明义 (大连海事大学)

In this work, the effects of viscous dissipation on heat transfer and entropy generation of the nanofluid natural convection in an inclined square cavity are numerically investigated. A fractional-step semiimplicit finite difference algorithm based on the projection method on a staggered grid is proposed to solve the laminar natural convection problem, which has the advantage of larger time steps. The square cavity is filled with a nanofluid composed of (Cu) copper nanoparticles and water,and the viscous dissipative behavior of the mixture flow is not negligible. The studied parameters are Rayleigh number Ra (104 and 105), Eckert number Ec ($0 - 2$), the volume fraction of solid particles $\phi(0{-}0.06)$, and inclination angle of square cavity $\alpha(0{-}\pi/2)$. The Prandtl number is fixed to $Pr = 6.2$. The results show that at any inclination angle, the increase in viscous dissipation leads to weakened heat transfer on the hot wall, enhanced heat transfer on the cold wall, and weakened flow in the square cavity. For the base solution without nanoparticles, the Eckert number has the greatest impact, with its effects on the average Nusselt number on the hot wall, maximum streamfunction, and average Nusselt number on the cold wall being 13, 0.15, 18.69%, and at $Ra = 104$, and 12, 0.5, 28.87% at $Ra = 105$, respectively. Research on entropy generation shows that as Eckert number increases, the entropy generation due to heat transfer increases,

while due to fluid friction decreases. As the Rayleigh number increases, the effect of viscous dissipation increases. As the inclination angle increases, the effects of volume fraction and Eckert number weaken. Adding solid particles can effectively weaken the effect of viscous dissipation.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000073]

A heuristic quantum-behavior algorithm for scheduling optimization problems

* 李真 (北京邮电大学)　李树荣 (北京邮电大学)

In this paper, we concern with the utilization and improvement of quantum-behavior heuristic algorithm for scheduling optimization problems. In order to solve a large-scale integral optimization problem with multiple extrema, a modified quantum-behavior algorithm with strong global searching ability is developed with the following measures, including a dynamic quantum rotation gate mechanism to improve the tendency of convergence, a criteria of annealing operation to improve global search ability, and a storage space and reconstruction operation for updating population. Meanwhile, a mathematical model of scheduling problem in container terminals is proposed named berth allocation, quay crane assignment and scheduling problem (BACASP). At last, several experimental studies of scheduling optimization problems are taken in the experiment section, which verifies the effectiveness and the superiority of the modified algorithm.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000082]

A dataset for suggesting variable orderings for cylindrical algebraic decompositions

Chen Changbo (Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences)　Jing Ruijuan (Jiangsu University)　Qian Chengrong (Jiangsu University)　Yuan Yaru (Jiangsu University)　* Zhao Yuegang (Jiangsu University)

Data have been playing a vital role in many successful applications of artificial intelligence. To embrace the power of modern AI technology to accelerate symbolic algorithms, it is indispensable to have a large amount of data of high quality. Unfortunately, such datasets are rare in the area of symbolic computation.Indeed, generation of a large dataset from scratch often costs a lot of time and effort. In this

work, we make public a random dataset on suggesting the variable ordering of cylindrical algebraic decomposition.We report in detail the design, generation as well as statistical information of the dataset.The value of this dataset is demonstrated by training and testing on it with several machine learning models.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000087]

A study on denoising seismic signals based on convolutional self-encoder

* 霍雨欣 (国防科技大学应用数学研究中心)

Seismic signal denoising is the most representative link in seismic data processing, which is related to the accuracy of earthquake early warning system. Therefore, in order to solve the problem of low signal-to-noise ratio and waveform distortion of seismic signals after denoising by traditional denoising algorithms, this paper introduces a deep learning method and constructs a new time-frequency denoising model based on convolutional auto-encoder (CAE-ED) to train and test the synthetic dataset containing multiple noise types constructed based on the Stanford seismic dataset (STEAD), and compares the denoising results with traditional methods. Comparison. The experimental results show that compared with bandpass filtering and wavelet threshold denoising, the CAE-ED model has significant improvement in the average signal-to-noise ratio and average correlation coefficient, while the root mean square error value is greatly reduced, which indicates that the denoising model in this paper has a strong denoising ability, while the waveform distortion is smaller after denoising. The constructed seismic signal denoising model can provide strong technical support for the earthquake early warning system.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000021]

连续区间上积分值的三次三角样条插值

* 吴金明 (浙江工商大学)　刘向云 (浙江工商大学)　王萍 (浙江工商大学)　朱春钢 (大连理工大学)

某些插值问题中, 插值点处的函数值是未知的, 而仅仅给定连续等距区间上的积分值. 如何利用连续区间上积分值信息来解决函数重构是一个重要的问题. 本文利用 C^2 连续的三次三角样条函数来解决此问题. 首先, 提出了 C^2 连续的三次三角样条插值格式. 该插值函数对 $1, x, sinx, cosx$ 具有再生性. 然后, 给出了三次三角样条插值函数逼近节点处的函数值和一阶导数值的收敛阶. 结果表明, 该插值函数在逼近节点处的一阶导数值时具有超收敛性. 最后, 数值实验表明该方法是可行且有效的.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000027]

Tolerance-Based Geometry Constraint Update Scheme for High-precision Direct Modeling

* Chen Hui (University of Chinese Academy of Sciences) Li-Yong Shen (University of Chinese Academy of Sciences) Shaoqiang Ma (Jinhang Digital Technology Co., Ltd)

Direct modeling in CAD offers a promising avenue for model modification through direct interaction. However, a critical impediment to the advancement of direct modeling technology is the inconsistency between modified geometry and unaltered constraints. While several methods have been proposed to rectify this challenge, they often fail to provide effective solutions, particularly in contexts demanding high model precision. In this paper, we introduce a novel approach by integrating tolerance analysis into the constraint update system, followed by the proposal of a constraint update scheme utilizing the extreme value tolerance model and the probability tolerance model. This innovative tolerance-based scheme adeptly resolves the inconsistency problem prevalent in direct modeling while satisfying the requisites of high-precision modeling. A comparative analysis against established methodologies is conducted to demonstrate the advantages of our proposed approach.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000037]

Efficient tool path planning and CAM process development

* 马鸿宇 (中国科学院大学)

High-end subtractive fabrication machining technology with high efficiency and high surface quality occupies a growing proportion in complex workpiece manufacturing. The whole frame includes computer aided design (CAD), computer aided manufacturing (CAM) and computer numerical control (CNC) processes. Currently, people require CAD and CAM to have higher precision and higher efficiency in practical CNC machining. Among them, tool path generation is a fundamental element, as it bridges the geometry designed in CAD and the machining process controlled in CAM. Therefore, the quality of the tool path intrinsically influences the machining accuracy and efficiency of the machined surface. In this talk, we will present the recent progress of our research group in the area of tool path planning. The construction of tool paths in free form surface machining can be based on plenty of quality objectives, such as less machining error, shorter path length, higher smoothness, and single start-end point constraints,

which would directly impact the performance and costs in the entire product lifecycle from design to recycling. And we will introduce several tool path planning methods optimized based on these criteria. After that, the specific CAM process development will be introduced, because there is still a long distance between the tool path planning methods at the scientific research level and the practical CAM processing modules. Some common CAM processes used in modern industry, such as Swarf Finishing, Surface Finishing, Steep and Shallow Finishing, and Corner Finishing, will be demonstrated and explained.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000041]

High quality LSPIA method for NURBS curves and surfaces with weights and knots optimization

* Lan Lin (大连理工大学) Ji Ye (大连理工大学) Wang Meng-yun (大连理工大学) Zhu Chun-gang (大连理工大学)

The Least-Squares Progressive-Iterative Approximation (LSPIA) method offers a robust and efficient approach for data fitting. Non-Uniform Rational B-splines (NURBS) are typically used as approximation functions due to their powerful shape representation. However, the traditional LSPIA application in NURBS comes with the restriction that only control points are adjusted to approximate the given data points, with weights and knots remaining fixed. To enhance fitting precision and overcome this constraint, we present Full-LSPIA, an innovative LSPIA method that jointly optimizes weights and knots alongside control points adjustments for superior NURBS curves and surfaces creation. We achieve this by constructing an objective function that incorporates control points, weights, and knots as variables, and solving the resultant optimization problem. Additionally, to construct lightweight geometry, we present a knot removal strategy named Decremental Full-LSPIA based on Full-LSPIA. This strategy adaptively removes the redundant knots within a specified threshold and determines optimal knot locations. The proposed approaches maximize the strengths of LSPIA. Compared to the classical LSPIA method, Full-LSPIA offers greater fitting quality for NURBS curves and surfaces while maintaining the same number of control points. Moreover, Decremental Full-LSPIA yields fitting results with fewer knots while maintaining the same error tolerance.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000092]

数据驱动的复杂系统建模

* 朱群喜 (复旦大学)

Recently, machine learning methods, including reservoir computing (RC), have been tremendously successful in predicting complex dynamics in many fields. However, a present challenge lies in pushing for the limit of prediction accuracy while maintaining the low complexity of the model. Here, we design a data-driven, model-free framework named higher-order Granger reservoir computing (HoGRC), which owns two major missions: The first is to infer the higher-order structures incorporating the idea of Granger causality with the RC, and, simultaneously, the second is to realize multi-step prediction by feeding the time series and the inferred higher-order information into HoGRC. We demonstrate the efficacy and robustness of the HoGRC using several representative systems, including the classical chaotic systems, the network dynamical systems, and the UK power grid system. In the era of machine learning and complex systems, we anticipate a broad application of the HoGRC framework in structure inference and dynamics prediction.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000093]

基于改进黏菌算法的风电场布局优化研究

* 谢嘉诚 (广西民族大学)　熊菊霞 (广西民族大学)　何镇江 (广西民族大学)

针对黏菌算法 (SMA) 在解决风电场布局优化 (WFLO) 问题时存在的寻优能力差、求解精度不足及 SMA 收敛速度慢、容易陷入局部极值等缺陷，提出了一种基于自适应收缩和遗传学习策略的改进型黏菌算法 (A-GLSMA)。首先，根据实际环境建立了风电场布局模型。然后，针对 SMA 易陷入局部极值等问题，提出了基于遗传学习策略的改进黏菌算法 (GLSMA)，以提升 SMA 的收敛速度和全局搜索能力。最后，针对风电场布局优化问题，采用最大值规则编码解向量，并设计了一种自适应收缩策略，利用风机的发电量来更新黏菌的位置，从而提高求解精度。仿真实验表明：在 19 个测试函数上，GLSMA 相比于 SMA、灰狼优化算法 (GWO)、樽海鞘群优化算法 (SSA)、鲸鱼优化算法 (WOA) 和遗传学习粒子群优化算法 (GLPSO) 等五种算法，具有更快的收敛速度和更高的寻优精度，并且 A-GLSMA 相比于遗传算法 (GA)，在求解两种风向分布下的 WFLO 问题时具有一定的性能优势。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000038]

Utilizing symmetry-enhanced physics-informed neural network to obtain the solution beyond sampling domain for partial differential equations

* Li Jie-Ying (Minzu University of China) Zhang Hui (Minzu University of China) Liu Ye (Minzu University of China) Guo Lei-Lei (North China University of Technology) Zhang Li-Sheng (North China University of Technology) Zhang Zhi-Yong (Minzu University of China)

Physics-informed neural network (PINN) provides an effective way to learn numerical solutions of partial differential equations (PDEs) in the sampling domain, but usually shows poor performances beyond the domain from which the training points are sampled, i.e., the limited solution extrapolation ability. In this paper, we propose a symmetry-enhanced physics-informed neural network (sePINN) to improve the extrapolation ability which incorporates the symmetry properties of PDEs into PINN. Specifically, we first explore the discrete and continuous symmetry groups of the PDEs under study, and then leverage them to further constrain the loss function of PINN to enhance the solution extrapolation ability. Numerical results of the sePINN method with different numbers of collocation points and neurons per layer for the modified Korteweg-de Vries equation show that both the accuracies of solutions in and beyond the sampling domain are improved concurrently by the proposed sePINN method.In particular, the accuracies of extrapolated solutions take a tendency of flat fluctuations with, even superior to, the ones of solutions directly trained via the PINN method.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000040]

Symmetry group based domain decomposition to enhance physics-informed neural networks for solving partial differential equations

* Liu Ye (Minzu University of China) Li Jie-Ying (Minzu University of China) Zhang Li-Sheng (North China University of Technology) Guo Lei-Lei (North China University of Technology) Zhang Zhi-Yong (Minzu University of China)

Domain decomposition provides an effective way to tackle the dilemma of physicsinformed neural networks (PINN) which struggle to accurately and efficiently solve partial differential equations (PDEs) in the whole domain, but the lack of efficient tools for dealing with the interfaces between two adjacent sub-domains heavily hinders the training effects, even leads to the discontinuity of the learned solutions. In this paper, we propose a symmetry group based domain decomposition strategy to enhance the PINN for solving the forward and inverse problems of the PDEs possessing a Lie symmetry group. Specifically,

for the forward problem, we first deploy the symmetry group to generate the dividing-lines having known solution information which can be adjusted flexibly and are used to divide the whole training domain into a finite number of non-overlapping sub-domains, then utilize the PINN and the symmetry-enhanced PINN methods to learn the solutions in each sub-domain and finally stitch them to the overall solution of PDEs. For the inverse problem, we first utilize the symmetry group acting on the data of the initial and boundary conditions to generate labeled data in the interior domain of PDEs and then find the undetermined parameters as well as the solution by only training the neural networks in a sub-domain. Consequently, the proposed method can predict high-accuracy solutions of PDEs which are failed by the vanilla PINN in the whole domain and the extended physics-informed neural network in the same sub-domains. Numerical results of the Korteweg-de Vries equation with a translation symmetry and the nonlinear viscous fluid equation with a scaling symmetry show that the accuracies of the learned solutions are improved largely.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000063]

脉冲噪声下鲁棒的盲图像去模糊算法

* 李喆 (长春理工大学)　刘鑫 (长春理工大学)

针对脉冲噪声下的模糊图像复原问题，本文分别建立了复原模糊核和骨架图像的盲去模糊模型，以及利用复原的模糊核恢复潜在清晰图像的非盲去模糊模型。在盲去模糊过程中，本文设计了一种简单有效的脉冲噪声标记方法用于计算噪声标记矩阵，构建了基于噪声标记矩阵和图正则化的盲图像去模糊模型，在对退化图像进行由粗到细的采样过程中，在不同尺度下利用加权图总变分正则化对模型进行求解，复原不同尺度下的骨架图像和模糊核。在非盲去模糊过程中，本文将 OID 模型中噪声权重矩阵 L1 范数约束替代为噪声标阵与噪声权重矩阵两者差的 L1 范数约束，实现脉冲噪声下模糊图像的复原。实验结果表明本论文的方法可有效降低脉冲噪声对去模糊任务的影响，进而恢复出高质量的潜在清晰图像。

– – –– o – – –– o – – –– o – – –– o – – ––

[P000043]

High speed corner trajectory planning method for CNC machining with confined jerk

* 孟可欣 (中国科学院数学与系统科学研究院)　袁春明 (中国科学院数学与系统科学研究院)　申立勇 (中国科学院大学数学学院)

Most tool paths in Computer Numerical Control (CNC) machining consist of a large amount of linear motion commands (G01). However, the discontinuity of curvatures and feedrates at corner junctions will cause machine tool vibration, resulting in a decreased surface quality and processing efficiency. Therefore, smooth corner transitions within specified tolerances and machine tool motion constraints are required during the interpolation process. In recent years, corner transition methods have evolved from simple corner removal to performance improvement, leading to the development of kinematics-based direct velocity planning methods that fully utilize the motion capabilities of each axis. However, most kinematics-based methods decelerate first and then accelerate at corners, limiting the potential velocity improvements.

We propose a novel jerk-confined interpolation algorithm that can achieve persistent acceleration at a series of corners. First, a two-phase asymmetric corner smoothing model for accelerating/decelerating (acc/dec) transitions at corners is introduced. Next, an optimal 7-stage S-shaped acc/dec algorithm is proposed for the remaining straight-line segments, which can be applied when the acceleration at both ends is not zero. Additionally, by a bidirectional planning adjustment strategy, we can look forward and backward several adjacent corners, and then determine the optimal acceleration state that can be achieved at each corner, even when the two corner points are close to each other.

Our method significantly improved the machining efficiency of machine tools. For a "clover" curve (See Fig. 1), our method can reduce the machining time by 52.4% compared to the method with constant jerk at corners[1](AU), 18.8% compared to the method with zero acceleration at the corner conjunction[2](KCS), and 6.7% compared to the asymmetric corner smoothing method[3](ASYM). Furthermore, using a look-ahead smoothing algorithm for computation results in short calculation times and low costs, we can obtain the real-time requirement in CNC machining. The experimental results have proven the effectiveness and efficiency of the method.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000045]

点云曲面上的 Voronoi 图

* 张子扬 (山东大学)　宋建涛 (山东大学)　陈双敏 (青岛科技大学)　辛士庆 (山东大学)　屠长河 (山东大学)

Voronoi 图 (VD) 是计算几何中用于空间划分的工具, 广泛应用于多个领域. 随着扫描技术的提升, 研究领域已从曲面内部拓展到点云曲面. 我们利用 VD 与 Delaunay 三角剖分（DT）的对偶关系直接计算受点云曲面约束的 VD. 通过 DT 生成候选面片, 评估其与点云曲面的贴合度, 并使用混合整数规划选取满足流形约束且最贴合的面片. 这种方法允许我们从保留的三角形中直接生成受约束的 VD. 据我们所知, 这是首次将点云曲面用作 VD 约束的研究, 且其有效性已通过实验证明.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000083]

实体钣金建模

* 王文嵩 (山东大学计算机科学与技术学院)　周子珺 (山东大学计算机科学与技术学院)　岳子佳 (青岛科技大学)　于昊 (山东大学计算机科学与技术学院)　陈双敏 (青岛科技大学)　辛士庆 (山东大学计算机科学与技术学院)　屠长河 (山东大学计算机科学与技术学院)

钣金加工是一种关键的金属制造技术，通过切割、弯曲和冲压等手段来改变金属板材的形状，广泛应用于各种薄壁金属构件的制造。面对传统算法在生成钣金结构时遇到的边缘不齐整、厚度不一致或产生自交等问题，本研究从计算机图形学的角度出发，提出了一种创新的钣金结构生成方法。这种方法特别注重解决曲面的光滑性、边缘的对齐性和厚度的均匀性等关键问题。通过引入带有偏移参数的 Alpha 包络算法，我们能够从曲面生成适当厚度的偏移层。接着，我们引入了一种新的距离场函数，并通过提取零等值面，构建了垂直于原始曲面的切割曲面。最后，通过对偏移层和边缘曲面进行布尔减运算，我们成功实现了曲面的平滑处理、边缘的精准对齐以及厚度的均匀生成，从而构建了具有等厚性的钣金三维模型。通过进一步的实验验证展示了该方法的实用性和高效率，为高精度的钣金建模发展提供了有力的技术支持。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000007]

Rational Solutions of First-Order Algebraic Ordinary Difference Equations

Vo Thieu N. (Ton Duc Thang University)　* Zhang Yi (Xi'an Jiaotong-Liverpool University)

We propose an algebraic geometric approach for studying rational solutions of first-order algebraic ordinary difference equations (AODEs). For an autonomous first-order AODE, we give an upper bound for the degrees of its rational solutions, and thus derive a complete algorithm for computing corresponding rational solutions.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000012]

Hilbert's Irreducibility Theorem for Linear Differential Operators

冯如勇 (中国科学院数学与系统科学研究院)　郭泽旺 (中国科学院数学与系统科学研究院)　* 陆伟 (湖北大学)

We prove a differential analogue of Hilbert's irreducibility theorem. Let $\mathcal{L}$ be a linear differential operator with coefficients in $C(\mathcal{X})(x)$ that is irreducible over $\overline{C(\mathcal{X})}(x)$, where $\mathcal{X}$ is an irreducible affine algebraic variety over an algebraically closed field C of characteristic zero. We show that the set of $c \in \mathcal{X}(C)$ such that the specialized operator $\mathcal{L}^c$ of $\mathcal{L}$ remains irreducible over $C(x)$ is Zariski dense in $\mathcal{X}(C)$.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000020]

Two complete reduction systems for Airy functions

* Du Hao (Beijing University of Posts and Telecommunications) Raab Clemens G. (Johannes Kepler University Linz)

The computation of indefinite integrals in certain kind of "closed form", which is known as symbolic integration, is an important research subarea of computer algebra. After implementing the recursive Risch algorithm partly, it was realized that efficient algorithms can be achieved by a parallel approach. This led to the famous Risch–Norman algorithm. However, this approach relies on an ansatz with heuristic degree bounds. Norman's completion-based approach provides an alternative for finding the numerator of the integral avoiding heuristic degree bounds. However, depending on the differential field and on the selected ordering of terms, it may happen that the completion process does not terminate and yields an infinite number of reduction rules. We apply Norman's approach to the differential fields generated by Airy functions, which play an important role in physics. By fixing adapted orderings and analyzing the process in the concrete case, we present two complete reduction systems for Airy functions by finitely many formulae to denote infinitely many reduction rules.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000044]

An Additive Decomposition in Exponential Extensions

陈绍示 (中国科学院数学与系统科学研究院) 杜昊 (北京邮电大学) * 高艺漫 (中国科学院数学与系统科学研究院) 李子明 (中国科学院数学与系统科学研究院)

We present an additive decomposition algorithm in a chain of exponential extensions. The algorithm decomposes such a chain as a direct sum of its integrable subspace and a C-linear subspace V, where C is the constant subfield of the chain. Remainders are exactly elements of V. The minimality of remainders can be described by supports of a carefully-chosen C-basis for the chain.

The algorithm is based on Hermite reduction for hyperexponential functions. It yields an alternative for computing elementary integrals over F_n. The alternative can compute the integrals that cannot be obtained by MAPLE nor MATHEMATICA.

This is joint work with Shaoshi Chen, Hao Du and Ziming Li.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000046]

Fast Normalization of Indexed Differentials

* 刘姜 (上海理工大学)

In differential geometry, massive calculation involving indexed differential expressions arises from various problems, such as tensor verification problem, and the problem of finding transformation rules of indexed functions under coordinate transformation. It is a fundamental problem in symbolic computation to judge whether two indexed differentials are equal or not. The general theory for this problem (or, for finding the canonical form of a polynomial) was established in our previous work by extending Gröbner basis theory and constructing "fundamental restricted ring". However, for an indexed differential monomial f with k lower indices and j upper indices, the general theory for finding the canonical form of the monomial has the complexity of at least $O((k!)^3 \prod_{i=0}^{j}(k-i)^3)$.

In this work, a much more efficient method is put forward. First, invariance of Leibniz expansion of indexed differentials under differential operators and monoterm symmetries is investigated. More precisely, we prove that the Leibniz expansion is invariant under both differential operator and monoterm symmetries. Then, much simpler generators of the ideal generated by the basic syzygies are found.

Finally, a normalization algorithm of indexed differentials with much lower complexity is provided. Especially, it has polynomial complexity $O(k^2)$ for op-monomials.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000080]

Safety Verification for Regime-Switching Jump Diffusions via Barrier Certificates

* 刘凯荣 (北京航空航天大学)　余志坤 (北京航空航天大学)

It is well known that for a stochastic hybrid system, if its failure probability does not exceed a given safety threshold, the safety of the system can be guaranteed. Thus, in this talk, we concern

with the upper bound of failure probability for failure analysis of a class of nonautonomous stochastic hybrid systems, denoted as Regime-Switching Jump Diffusions (RSJDs). We start with the definition of RSJDs, which contain not only continuous flows described by stochastic differential equations, but also instantaneous behavior described by Markovian switching and instantaneous behavior described by Lévy jump. Then we decompose the failure probability of RSJDs in $[t_0, +\infty)$ into two segments: one is defined over $[T, +\infty)$, and the other is defined over $[t_0, T]$. For failure probability over $[T, +\infty)$, by utilizing multiple vectorial barrier certificates, an asymptotically decreasing bound of failure probability with respect to T is established, where a general nonnegative matrix is used instead of a special nonnegative matrix defined by the exponent of essentially nonnegative matrix for a broader applicability. For failure probability over $[t_0, T]$, a generalized c-martingale condition is adopted to obtain a T-dependent failure probability bound, in which two non-negative scalar functions are utilized to relax the conservativeness of infinitesimal generators. Finally, for rational RSJDs, we transform the decomposed failure analysis problems into two semi-definite programming (SDP) problems, and then solve them via sum of squares programming. The applicabilities and effectiveness of our computable decomposition methodology are illustrated through three examples.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000010]

TFHE-like Functional Bootstrapping in General Cyclotomic Ring

* 刘登发 (中国科学院数学与系统科学研究院)　李洪波 (中国科学院数学与系统科学研究院)

The functional bootstrapping scheme plays a significant role in Fully Homomorphic Encryption(FHE). In the original TFHE/FHEW scheme, the functional bootstrapping procedure only works in power-of-two cyclotomic ring. With the development of FHE, it no longer meets the needs of practical application, especially in the field of research for SIMD mode of bootstrapping procedure. It has been a promising field how to extend TFHE/FHEW functional bootstrapping scheme to a general cyclotomic ring. In this paper, we make a comprehensive analysis of the structure of functions with period M. We give the constraint to be satisfied by the function which could be evaluated homomorphically by one BlindRotations procedure in three equivalent forms. The class of such functions is named by M-constraint functions in this paper. besides, we find that each function with period M can be decomposed into the sum of a sequence of d-constraint functions where d|M. We extend TFHE functional bootstrapping scheme to general cyclotomic rings based on the analysis above.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000049]

Fast, Lagre Scale Dimensionality Reduction Schemes Based on CKKS

* Yuan Haonan (Chongqing Key Laboratory of Secure Computing for Biology, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences) Wu Wenyuan (Chongqing Key Laboratory of Secure Computing for Biology, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences)

In the era of big data, there has been a significant surge in the volume of data generated from diverse sources such as social media platforms, e-commerce websites, and Internet of Things (IoT) devices. This increase has led to an uptick in the dimensionality of the data. High-dimensional data escalates the costs associated with storage and processing and presents formidable challenges for data analysis and machine learning model training. Concurrently, most data encompasses personal privacy and ethical considerations and is dispersed across various institutions. Consequently, devising efficient and secure methods for joint high-dimensional data dimension reduction has emerged as a pivotal technology for addressing these issues.

This paper proposes a novel CKKS-based homomorphic encryption dimensionality reduction scheme (HE-DR), which combines the Rank-Revealing(RR) method's computational efficiency and homomorphic encryption's security to achieve fast and secure dimension reduction for high dimensional data. Our proposed scheme circumvents the necessity for data matrix encryption and the computation and transmission of ciphertext matrices. Consequently, compared with recent dimension reduction schemes based on fully or partially homomorphic encryption, our approach demonstrates nearly 60–200 times faster computational efficiency and less than 1/3 of the communication overhead previously observed in similar schemes. Furthermore, we demonstrate that our scheme maintains its computational efficiency even when dealing with high-dimensional data, requiring only five times the plaintext calculation time.

– – –– o – – –– o – – –– o – – –– o – – ––

[P000055]

Leveled homomorphic encryption based on NTRU without relinearization

* 代小康 (中科院重庆绿色智能技术研究院) 王皓勇 (中科院重庆绿色智能技术研究院) 吴文渊 (中科院重庆绿色智能技术研究院) 冯勇 (中科院重庆绿色智能技术研究院)

One of the difficulties in designing homomorphic encryption is how to maintain the ciphertext structure. This is because the ciphertexts of current lattice-based encryption schemes are polynomial vectors or matrices. For example, in schemes such as CKKS and BGV, the ciphertext is a two-dimensional

polynomial vector. After homomorphic multiplication (tensor multiplication of vectors), the dimension of the ciphertext becomes the original square. Therefore, in order to maintain the original ciphertext structure after each homomorphic multiplication, an operation called relinearization is performed. There are currently two mainstream relinearization technologies, one based on bit decomposition and the other based on module exchange. In order to convert the ciphertext to the original dimension, these two techniques need to perform $4 + \log q$ and 6 polynomial multiplication respectively. This greatly slows down homomorphic evaluation.

Homomorphic encryption based on NTRU is in a very delicate state. This is mainly based on two points. First of all, since it was proposed, the security of the earliest scheme NTRU-prime [Hoffstein,Joseph & Silverman 97] and the homomorphic scheme [Bonte et al ASIACRYPT21] has not been strictly proven, unlike LWE or RLWE, which are both based on the hardness problem of lattice or ideal lattice. Therefore, some NTRU-based homomorphic encryption schemes are generally based on some heuristic assumptions. Such as the homomorphic scheme YASHE [Bos et al IMA13] and the multi-key homomorphic scheme [López-Alt, Tromer & Vaikuntanathan STOC13] both need to rely on an assumption called the decisional small polynomial ratio assumption (DSPR). However, the DSPR assumption that the key is taken from the $\{0, 1\}$ distribution and the discreted gaussian distribution with small variance does not hold. In particular, the work [Ducas & Woerden ASIACRYPT21] showd that when q exceeds $O(n^{2.48})$, the sub-lattice attack will be very effective on solving NTRU problem. On the plus side, because NTRU' s public key and ciphertext are both a single polynomial, the ciphertext structure does not change when performing homomorphic evaluation. This therefore seems to avoid ciphertext relinearization operations. Notice that the decryption key becomes the square of the original. This is because the degree of the public key in the ciphertext becomes 2 after a homomorphic multiplication. Therefore, for initial NTRU ciphertext , after performing multiplication operations, as long as the degree of public keys in the resulting ciphertext is recorded, the corresponding decryption key can be determined. In order to control the noise, a large scaling factor can be multiplied when encoding the plaintext.

Based on the above observations, we construct a homomorphic encryption scheme based on NTRU that does not require linearization. Complexity analysis and experimental results show that at the same level of homomorphic evaluation capabilities, the homomorphic multiplication speed of our scheme is $5-6$ times faster than CKKS and BFV.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000065]

Classification of a class of planar quadrinomials

* Chan Chin Hei (香港科技大学) Xiong Maosheng (香港科技大学)

Let p be an odd prime, k, l be positive integers, $q = p^k, Q = p^l$. In this work we study planar functions of the form $f_c(X) = c_0X^{qQ+q} + c_1X^{qQ+1} + c_2X^{Q+q} + c_3X^{Q+1}$ over F_{q^2} for any $= (c_0, c_1, c_2, c_3) \in F_{q^2}^4$. It

turns out that if $f_c(X)$ is planar, then $f_c(X)$ is linear equivalent to one of the functions below

1. X^{Q+1};
2. X^{Q+q};
3. $P_2(x, y,) = (x^Q y, x^{Q+1} + y^{Q+1})$ for some $\in F_q^*$;
4. $P_3(x, y) = (x^{Q+1} - x^Q y, xy^Q + y^{Q+1})$ for some $\in F_q^* \setminus \{-1\}$;
5. $X^{Q+q} + X^{Q+1}$ for some $\in F_{q^2}^* \setminus \mu_{q+1}$.

This work is analogous to the classification of APN functions from this family $f_c(X)$ for $p = 2$ obtained recently by Gölouglu.

It was well-known that properties of $f_c(X)$ are closely related to that of the rational function $g(X) = \frac{c_3^q X^{Q+1} + c_2^q X^Q + c_1^q X + c_0}{c_0 X^{Q+1} + c_1 X^Q + c_2 X + c_3}$. Recently Ding and Zieve used a powerful geometric method to study permutation properties of $f_c(X)$ for $p = 2$. The main technique of this work is to adopt their method and give a detailed study of the geometry properties of $g(X)$ for odd p from which the linear equivalence follows directly.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000066]

基于全同态加密的高效隐私保护聚类算法

* 杨晨 (中国科学院重庆绿色智能技术研究院)　陈经纬 (中国科学院重庆绿色智能技术研究院)　吴文渊 (中国科学院重庆绿色智能技术研究院)　冯勇 (中国科学院重庆绿色智能技术研究院)

聚类是一种重要的无监督机器学习方法，可以揭示隐藏在数据中的内在模式和特征，在数据分析领域有广泛的应用。为了分析大规模数据，外包计算 (outsourced computation) 是一种有效的解决方法。但是如果涉及到敏感数据，外包计算可能会存在隐私泄漏的问题。全同态加密 (fully homomorphic encryption) 可以在密文上进行操作而不需要解密，非常适合于外包计算的场景。目前，已经有许多基于全同态加密的隐私保护聚类算法的研究，但是目前的研究结果要么受限于全同态加密所带来的额外开销而非常耗时，要么经过一两次聚类算法的计算迭代后就要求解密再加密，才能继续进行计算。在此项工作中，我们提出了一种高效的找出一列数据中最小值或最大值的方法，充分利用了全同态加密的单指令多数据 (single-instruction-multiple-data) 加速计算的天然属性。将这种方法和同态加密的自举 (bootstrap) 相结合，我们的此项工作实现了一种实用的基于全同态加密的聚类算法协议，数据方和计算方之间只需要进行一轮交互即可完成聚类。我们实现的此聚类协议是基于 CKKS 这一全同态加密方案。实验结果表明我们的协议相比于其他已有的相关工作有显著的性能提升。我们在许多公开测试集上测试了我们的协议，在密文上的结果达到了和明文上结果几乎一样的精度。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000091]

基于可解正交阵列的 Ramp 密钥共享方案

王秀丽 (中国民航大学)　* 邓扬眉 (中国民航大学)

密钥共享方案是密码学领域的重要研究内容。本文给出了利用可解正交阵列构造理想的密钥共享方案的方法。在正交阵列的构造部分，首先，通过有限域上的差阵构造了强度为 2 的完全可解正交阵列. 之后利用有限域上的多项式构造了强度大于等于 2 的可解正交阵列，并且通过多个可解正交阵列得到了水平更大的可解正交阵列。在密钥共享方案的构造部分，证明了若存在可解正交阵列，则存在理想的 Ramp 密钥共享方案，给出了理想的密钥共享方案和几类理想的 Ramp 密钥共享方案的构造方法。最后通过实例验证了方案构造的合理性。

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000026]

A Basis-preserving Algorithm for Computing the Bézout Matrix of Newton Polynomials

Yang Jing (Guangxi Minzu University)　* Yang Wei (Guangxi Minzu University)

This paper tackles the problem of constructing Bézout matrices for Newton polynomials in a basis-preserving approach that operates directly with the given Newton basis, thus avoiding the need for transformation from Newton basis to monomial basis. This approach significantly reduces the computational cost and also mitigates numerical instability caused by basis transformation. For this purpose, we investigate the internal structure of Bézout matrices in Newton basis and design a basis-preserving algorithm that generates the Bézout matrix in the specified basis used to formulate the input polynomials. Furthermore, we show an application of the proposed algorithm on constructing confederate resultant matrices for Newton polynomials. Experimental results demonstrate that the proposed methods perform superior to the basis-transformation-based ones.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000028]

Affine geodesic convex polynomials are rare

* 王愚 (中国科学院数学与系统科学研究院机械化实验室)　叶科 (中国科学院数学与系统科学研究院机械化实验室)

本报告主要介绍多项式函数的测地凸性的一些研究成果.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000047]

A Generalization of Habicht's Theorem for Subresultants of Several Univariate Polynomials

Hong Hoon (North Carolina State University)　* 蒙嘉奇 (广西民族大学)　杨静 (广西民族大学)

The Habicht' s theorem contains two results: the relationship between a single subresultant polynomial of two univariate polynomials and the pseudo-remainder of its adjacent ones, and the relationship between a single subresultant polynomial and the subresultant polynomial of its adjacent ones. Following up the previous work on the generalization of the first result by Hong and Yang, this paper generalizes the second result to several polynomials and revealed that a subresultant polynomial of several univariate polynomials with higher order can be reduced to that of subresultant polynomials with lower orders.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000052]

Extensions of S-Lemma for Noncommutative Polynomials

* 闫斯卓 (中国科学院数学与系统科学研究院)　郭峰 (大连理工大学)　支丽红 (中国科学院数学与系统科学研究院)

We consider the problem of extending the classical S-lemma from the commutative case to noncommutative cases. Precisely, we extend the S-lemma to three kinds of noncommutative polynomials: noncommutative polynomials whose coefficients are real numbers, noncommutative matrix-valued polynomials, and hereditary noncommutative matrix-valued polynomials. Different from the commutative case, the S-lemma for noncommutative polynomials can be extended to the case involving multiple quadratic constraints. Some examples are given to demonstrate the relations between these newly derived conditions.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000058]

基于强弦图的 F_2 上三角分解的复杂度分析

* 齐朝星 (北京航空航天大学)　牟晨琪 (北京航空航天大学)

在本文中, 我们首先基于图的极大团引入了一种名为次强消除序的图的顶点序, 并证明了它可以完全刻画强弦图. 基于这种顶点序, 我们提出了一种新的多项式选取策略, 用于算法中的多项式计算. 然后, 我们证明了当这种顶点序被用作三角分解的变元序时, 其关联图为强弦图的多项式集合在分解中出现的任何多项式的变元都包含在某些极大团中, 这给出了有界树宽下的分解中变元的结构变化的统一描述. 因此, 我们证明了当输入多项式集合满足具有 n 个变元和 l 个多项式且其关联图是树宽为 m 的强弦图时, 使用新多项式选取策略进行三角分解的复杂度为 $O(4^m ln(ml/n-1)^{(n-1)})$. 当 $m << n$ 时, 这比原 $O(l^n)$ 更小.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000090]

Monotonic optimization with application to the selection of parameters for LWE-based encryption schemes

* 徐娟 (中国科学院重庆绿色智能技术研究院)　吴文渊 (中国科学院重庆绿色智能技术研究院)　冯勇 (中国科学院重庆绿色智能技术研究院)　董日娜 (中国科学院重庆绿色智能技术研究院)

The selection of parameters for LWE-based schemes is a challenging problem and becomes more important as lattice-based cryptography attracts increasing attention. In this paper, different from the conventional routine of selecting parameters by experience or deduction, we focus on the mathematical theory behind the problem, and address the problem of selecting optimal parameters for LWE-based schemes, which is even harder than selecting good parameters. This problem can be modeled as a global optimization problem, in which a certain constraint may not be expressed in closed form. Fortunately, through analysis we discover that the objective and the functions in all the constraints of this problem are monotone with respect to each of the variables. We provide a framework to address such problems; and for optimization problems in a special form, we are able to design a complete global optimization algorithm that is guaranteed to terminate in finitely many steps. This algorithm enables us to search for optimal parameters for the encryption schemes, while guaranteeing security and correctness specified by the user. As an example, we investigate the problem of choosing optimal parameters for the state-of-the-art BGV scheme, in the context of minimizing the communication overhead, without considering homomorphic operations, and present optimal parameters for it under specified security levels and correctness probability. In addition, we analyze the security level of the LWE instances in detail and empirically derive a closed formula to estimate the security level in terms of the parameters, which may be useful for future work.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000053]

A Positivstellensatz on the Matrix Algebra of Finitely Generated Free Group

* Liang Hao (Academy of Mathematics and Systems Science)

Let m and n be two positive integers. For the free group F_n generated by n letters, and a symmetric polynomial b with variables in F_n and with n-by-n complex matrices coeffitients, we use real algebraic geometry to give a new proof showing that b is a sum of Hermitian squares if and only if b is mapped to a positive semidefintie matrix under any finitely dimensional unitary representation of F_n.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000060]

An algorithm for computing comprehensive order basis systems of parametric polynomial matrices

* 杨润河 (中国科学院信息工程所)　孙瑶 (中国科学院信息工程所)　王定康 (中国科学院数学与系统科学院)　肖方慧 (湖南师范大学)　郑晓鹏 (中国科学院数学与系统科学院)

An algorithm for computing parametric order bases for univariate polynomial matrices with parameters is first presented in this paper. Starting from the non-parametric univariate polynomial matrix, our key idea is to construct a special module and module order. Then based on basis theory for modules, we present that the order basis can be obtained by computing a minimal basis for this module under this order. Further, we extend the definition of the order basis to the parametric polynomial matrix, and give the concept of comprehensive order basis systems. More importantly, the method based on bases for modules can be naturally generalized to the parametric case by means of comprehensive systems for modules. As a consequence, we design a new algorithm for computing comprehensive order basis systems.The proposed algorithm has been implemented on the computer algebra system Singular and Maple.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000062]

Gröbner Basis of the Defining Ideal of Quaternionic Polynomial Ring in Symbolically Many Quaternionic Variables

刘越 (中国科学院数学与系统科学研究院数学机械化重点实验室)　李洪波 (中国科学院数学与系统科学研究院数学机械化重点实验室)　黄雷 (中国科学院数学与系统科学研究院数学机械化重点实验室)　邵长鹏 (中国科学院数学与系统科学研究院数学机械化重点实验室)　* 王正阳 (中国科学院数学与系统科学研究院数学机械化重点实验室)

In a non-commutative ring, to test whether a set of polynomials involving m variables, where m is symbolic instead of numeric, is a Gröbner basis of an ideal, the S-polynomial reduction test must be done inductively, which may be very complicated. The defining ideal of the quaternionic polynomial ring in m quaternionic variables is a typical example, where it is not difficult to predict a Gröbner basis based on the results from small values of m, but it is extremely difficult to make the verification by finishing all the S-polynomial reductions inductively.

In this paper, we present a computer-assisted inductive proof on a Gröbner basis of the defining ideal of quaternionic polynomial ring. We develop two techniques in the course of the proof: left-to-right decomposition, which provides a much weaker test for Gröbner basis, and subdivision and rewriting of interval variables, which preserves the leading term in rewriting monomials as new variables and successive reductions. Both techniques may be extended to more general non-commutative setting involving m variables. With the help of an improved computer-assisted proving program and a modern workstation, the entire Main Theorem can be proven in as fast as 42 minutes.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

[P000013]

Construction of three class of at most four-weight binary linear codes and their applications

* 张同慧 (福建师范大学)

Three classes of binary linear codes with at most four nonzero weights were constructed in this paper, in which two of them are projective three-weight codes. As applications, s-sum sets for any odd s $>$ 1 were constructed.

– – –– ○ – – –– ○ – – –– ○ – – –– ○ – – ––

Index for speakers

Bai Ziwei , 27
Chan Chin Hei , 59
Chen Hui , 48
Chen Shaoshi , 41
Du Hao , 55
Guo Wan-Ming , 27
Jing Yang , 39
Lan Lin , 49
Li Jie-Ying , 50
Liang Hao , 64
Liu Ye , 51
Qi Niuniu , 30
Song Jichao , 38
Wang Zhimin , 37
Xu Jia , 43
Yang Wei , 61
Yao Hongmei , 37
Yuan Haonan , 57
Zhai Ziqi , 35
Zhang Yi , 54
Zhao Yuegang , 46
Zuo Qian , 36
丁剑, 31
上官冲, 26
代小康, 58
代梓灏, 38
关剑成, 28
冯勇, 32
刘凯荣, 56
刘姜, 56
刘登发, 57
刘超, 25
刘静, 43
卫亚蓉, 42
吕龙杰, 45
吴弢 , 29
吴严生, 25
吴玉玲, 34
吴金明, 47
唐春明, 21
孟可欣, 52
宋秋叶, 23
张同慧, 65
张子扬, 53
张宇欣, 36
张英瑞, 28
徐仝友, 42
徐娟, 63
朱群喜, 49
李喆 , 52
李昊坤, 44
李真, 46
杨志红, 23
杨文强, 34
杨晨, 60
杨林翰, 26
杨润河, 64
杨立波, 32
林成青, 31
武斌, 29
熊贝贝, 31
王华雄, 20
王愚, 61
王文嵩, 54
王杰, 41
王正阳, 64
窦国威, 30
胡慧丹, 24
胡胜龙, 33
范更华, 20
蒙嘉奇, 62
蔡小敏, 35
薛白, 27
袁骁, 33
谢嘉诚, 50
谢岩峰, 39

邓扬眉, 61
邢朝平, 20
郑晓朋, 45
郭峰, 41
闫斯卓, 62
陆伟, 54
陆镜宇, 22
陈日增, 40
陈琦元, 22
霍雨欣, 47
马鸿宇, 48
高奕博, 21
高艺漫, 55
齐朝星, 62