第十二届中国数学会计算机数学大会

2021 年 6 月 4 日-7 日, 广西桂林

会议手册
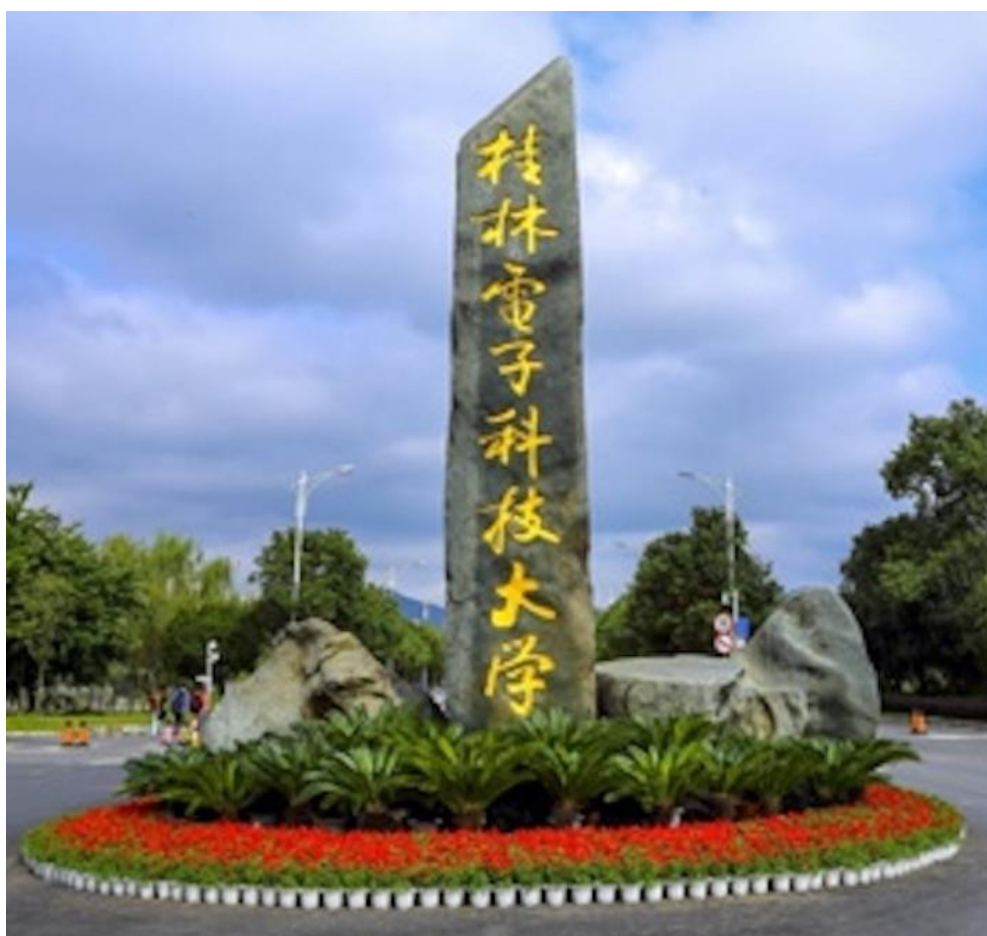
中国数学会计算机数学专业委员会主办

桂林电子科技大学与中国科学院数学机械化重点实验室承办

中国数学会协办

学院简介

桂林电子科技大学计算机与信息安全学院始建于 1980 年，是广西最早进行计算机专业人才培养的单位。1981 年开始招收本科生，1996 年开始招收硕士研究生，2018 年开始招收博士研究生。学院拥有网络空间安全一级学科博士点，计算机科学与技术、网络空间安全 2 个一级学科硕士点，计算机技术、软件工程 2 个工程硕士授权领域。网络空间安全是广西一流学科，位于"软科 2020 中国最好学科排名"第 18 位，广西第一。计算机科学与技术在 2017 年全国第四轮学科评估中成绩为 B-，位于"软科 2020 中国最好学科排名"第 87 位，广西第一。计算机科学学科 2021 年 5 月进入 ESI 全球排名前 1%。

经过 40 多年的努力建设，学院现有计算机科学与技术、软件工程、物联网工程、信息安全、智能科学与技术、信息对抗技术、网络空间安全 7 个本科专业。其中：

1. 计算机科学与技术专业通过工程教育专业认证，是国家级一流本科专业建设点国家级特色专业；国家级本科专业综合改革试点；教育部卓越工程师教育培养计划实施专业；广西本科高校特色专业；广西优势特色专业

2. 软件工程专业通过工程教育专业认证，是国家一流本科专业建设点；广西紧缺人才专业

3. 物联网工程专业是国家一流本科专业建设点；广西优势特色专业

4. 信息安全专业是国家一流本科专业建设点

5. 智能科学与技术专业是广西优势特色专业

学院现有教职工 133 人，其中专任教师 115 人，正高级职称教师 40 人，副高级职称教师 46 人，博士学位教师 74 人，博士生导师 21 人。拥有国家杰出青年基金获得者 1 名、国家第一批"万人计划"领军人才 1 名、国务院政府特殊津贴专家 2 名、广西八桂学者 2 名、广西教学名师 2 名、广西"新世纪十百千人才工程第二层次"人选 1 名，省级百人计划入选者 4 名、楚天学者 1 名。

学院拥有国家级教学团队 1 个、广西教学团队 1 个、广西人才小高地 1 个、广西创新研究团队 2 个。拥有教育部高等学校教学指导委员会委员 3 人，广西数字广西专家咨询委员会专家委员 1 名，广西数字基础设施专业委员会专家委员 1 名，广西中国-东盟信息港建设专业委员会专家委员 1 名，广西数字基础设施专业委员会专家委员 1 名。

学院建有国家级科研平台 1 个（卫星导航定位与位置服务国家地方联合工程研究中心），广西重点实验室 3 个（广西可信软件重点实验室、广西密码学与信息安全重点实验室、广西图像图形与智能处理重点实验室），广西工程技术研究中心 2 个（广西云安全与云服务工程技术研究中心、广西智慧工地工程技术研究中心），广西工程研究中心 1 个（中国-东盟信息港大数据应用工程研究中心），广西高校重点实验室 2 个（广西高校图像图形智能处理重点实验室、广西云计算与复杂系统重点实验室），校级研究院 2 个（人工智能交叉研究院、大数据技术研究院）。

学院建有国家级实验教学示范中心 1 个（计算机实验教学中心），国家级工程实践教育中心 1 个（桂电-中软工程实践教育中心），国家级工程专业学位研究生联合培养示范基地 1 个（桂电-桂林国家大学科技园研究生联培基地），3 门课程入选国家级一流本科课程（数据结构与算法、计算机科学导论、计算机思维的结构）。获国家级教学成果二等奖 2 项，广西区教学成果奖 5 项。

围绕学科前沿和国家、地方重大需求，形成了可信软件与大数据、密码学与信息安全、图像图形智能处理、物联网与位置服务等特色学科方向。"十三五"期间，学院新增国家自然科学基金项目 54 项，主持/参与国家自然科学基金重点项目 3 项、国家重点研发计划重点专项课题 1 项。横向和纵向到位科研经费 1.2 亿元。获广西自然科学奖二等奖 1 项，广西技术发明奖 3 项，广西科技进步奖 4 项，中国电子学科科学技术（自然科学类）奖 1 项。

学院坚守立德树人宗旨，围绕计算机、网络空间安全领域发展需求，全力推进一流学科建设和一流专业建设，持续提升人才培养质量，服务经济社会发展。

CM 2021

http://www.mmrc.iss.ac.cn/cscm/cm2021/

第十二届中国数学会计算机数学大会

2021年6月4－7日，中国 桂林

主办单位	**承办单位**	**协办单位**	**会议资助**
中国数学会计算机数学专业委员会	桂林电子科技大学 中国科学院数学机械化重点实验室	中国数学会	国家自然科学基金委员会 Maplesoft中国

大会主席　周娅　桂林电子科技大学

程序委员会

陈绍示　中科院数学与系统科学研究院（主席）
牟晨琪　北京航空航天大学（副主席）

■ "计算几何"专题程序委员会
李 新　中国科学技术大学
申立勇　中国科学院大学
朱春钢　大连理工大学
伍铁如　吉林大学
徐 岗　杭州电子科技大学
贾晓红　中科院数学与系统科学研究院

■ "密码数学"专题程序委员会
孙 兵　国防科技大学
王保仓　西安电子科技大学
林昌露　福建师范大学
龚 征　华南师范大学
崔 霆　信息工程大学
潘彦斌　中科院数学与系统科学研究院

■ "人工智能"专题程序委员会
雷 娜　大连理工大学
左旺孟　哈尔滨工业大学
刘世霞　清华大学
苏 航　清华大学
孟德宇　西安交通大学
郁文生　北京邮电大学

■ "组合数学"专题程序委员会
杨立波　南开大学
马 杰　中国科学技术大学
王光辉　山东大学
张华军　浙江师范大学
祝宝宣　江苏师范大学
鲁红亮　西安交通大学

■ "符号计算"专题程序委员会
陈长波　中科院重庆绿色智能技术研究院
孙 瑶　中科院信息工程研究院
李冬梅　湖南科技大学
李 伟　中科院数学与系统科学研究院
杨争峰　华东师范大学
杨 静　广西民族大学
程进三　中科院数学与系统科学研究院

■ "计算机数学及其应用"专题程序委员会
冯如勇　中科院数学与系统科学研究院
支丽红　中科院数学与系统科学研究院
冯 勇　中科院重庆绿色智能技术研究院
汤建良　深圳大学
李洪波　中科院数学与系统科学研究院
余志坤　北京航空航天大学
高小山　中科院数学与系统科学研究院
徐 鸣　华东师范大学
唐春明　广州大学
常 亮　桂林电子科技大学
夏璧灿　北京大学

大会邀请报告

江 松　北京应用物理与计算数学研究所
陈松灿　南京航空航天大学
林东岱　中科院信息工程研究所
侯庆虎　天津大学

青年邀请报告

刘日升　大连理工大学
张 江　密码科学技术国家重点实验室
郑大彬　湖北大学
林志聪　山东大学
秦小林　中科院成都计算机应用研究所
唐晓弦　北京航空航天大学
黄 劲　浙江大学
蓝如师　桂林电子科技大学

组织委员会

刘建明　桂林电子科技大学（主席）
陈光喜　桂林电子科技大学
唐 敏　桂林电子科技大学
李 佳　中科院数学与系统科学研究院
周代珍　中科院数学与系统科学研究院

大会联系人

陈绍示：schen@amss.ac.cn
牟晨琪：chenqi.mou@buaa.edu.cn

会议联系人：　陈光喜　桂林电子科技大学　　13977306429

唐敏　　桂林电子科技大学　　13978309010

周代珍　中科院数学与系统科学研究院　　13693282978

住宿与交通

会议地点: 广西桂林市桂林宾馆

详细地址：广西桂林市象山区榕湖南路 14 号

宾馆电话：0773-2898888

交通信息: 鉴于参会代表可能对桂林交通不熟悉，建议首选乘坐出租车。

- **桂林两江国际机场—桂林宾馆** (总路程：约 29 公里)
  乘机场大巴：约 1 小时 15 分钟；换乘公交：21 路公交（绢纺厂—公交东环车场）
  按照指示牌在机场大巴站乘坐大巴往市区方向在天鹅宾馆下车，步行 500 米在象山区政府公交站换成 21 路公交，在少年宫站下车，步行 250 米即可到达
  乘出租车：约 40 分钟

- **桂林火车站（桂林站）—桂林宾馆** (总路程：约 2.8 公里)

  乘公交车：约 20 分钟；乘坐公交线路：91 路（平桂西路北—文明路）

  出站后步行 200 米到桂林公交站台，乘 91 路，在文明路下车，步行 800 米即可到达

  乘出租车：约 12 分钟

- **桂林北站（高铁）—桂林宾馆** (总路程：约 8.15 公里)

  乘公交车：约 50 分钟；乘坐公交线路：100 路（桂林北站—和平村）

  出站后步行 200 米到桂林北公交站台，乘 100 路，在阳桥站下车，步行 870 米即可到达

  乘出租车：约 30 分钟

- **桂林西站（高铁）—桂林宾馆** (总路程：15 公里)

  乘公交车：约 1 小时；乘坐公交线路：22 路（桂林西站—天鹅塘）

  出站后到桂林西公交站台，乘 22 路，在少年宫站下车，步行 400 米即可到达

  乘出租车：约 40 分钟

第十二届中国数学会计算机数学大会 (CM2021)

2021 年 6 月 4 日 ~ 7 日

广西桂林

2020 年 6 月 5 日

开幕式与合影	6 月 5 日 8:30-9:00　宴会厅

S1　大会邀请报告 (1)	6 月 5 日 9:00-10:00　宴会厅

主持人：陈绍示

9:00-10:00　组合数学中的符号计算问题
　　　　　　侯庆虎（天津大学）

茶歇	6 月 5 日 10:00-10:20　None

Y1　青年邀请报告 (1)	6 月 5 日 10:20-10:50　宴会厅

主持人：刘建明

10:20-10:50　四元数代数在彩色图像处理中的应用研究
　　　　　　蓝如师（桂林电子科技大学）

Y2　青年邀请报告 (2)	6 月 5 日 10:20-10:50　榕湖厅

主持人：郁文生

10:20-10:50　最优化观点下的深度学习：从单层到多层最优化学习
　　　　　　刘日升（大连理工大学）

主持人：支丽红

10:55 - 11:10   用符号计算证明 Ramsey 定理的机械化方法(abstract)
鲁健 (上海大学数学系)

11:10 - 11:25   The convergence of an efficient Levenberg-Marquardt method for nonlinear equations under Holderian local error bound (abstract)
Liang Chen (Huaibei Normal University)

11:25 - 11:40   Isogeometric Analysis-based Topological Optimisation for Heterogeneous Parametric Porous Structures (abstract)
胡传丰 (浙江大学)

11:40 - 11:55   Lazy Hermite Reduction and Creative Telescoping for Algebraic Functions (abstract)
Du Lixin (School of Mathematical Sciences University of Chinese Academy of Sciences)

11:55 - 12:10   The subresultant of several univariate polynomials (abstract)
Yang Jing (Guangxi University for Nationalities)

分组报告 (2) "人工智能"专题   6 月 5 日 10:55-12:10 榕湖厅

主持人：蓝如师

10:55 - 11:10   Improve the Robustness and Accuracy of Deep Neural Network with $L_{2,\infty}$ Normalization (abstract)
于立佳 (中国科学院数学与系统研究院)

11:10 - 11:25   Analyzing the barren plateau phenomenon in training quantum neural networks with the ZX-calculus (abstract)
赵宸 (中国科学院数学与系统科学研究院)

11:25 - 11:40   基于超像素合并的超像素级高光谱图像分类(abstract)
李旭 (辽宁师范大学)

11:40 - 11:55   Attention-Based DenseNet for Pneumonia Classification (abstract)
王凯 (合肥工业大学数学学院)

11:55 - 12:10   Autotuning the Performance of Matrix Multiplication and Convolution for Deep Learning on CPU (abstract)
陈长波 (中国科学院重庆绿色智能技术研究院)

午餐   6 月 5 日 12:10-14:00 None

Y3 青年邀请报告 (3)   6 月 5 日 14:00-14:30 宴会厅

主持人：夏壁灿

14:00-14:30   Multistability of Small Reaction Networks
唐晓弦（北京航空航天大学）

Y4　青年邀请报告 (4)	6 月 5 日 14:00-14:30　榕湖厅

主持人：杨争峰

14:00-14:30　New Constructions of Optimal Cyclic (r, δ) Locally Repairable Codes from Their Zeros
郑大彬（湖北大学）

分组报告 (3)　"符号计算"专题	6 月 5 日 14:35-15:50　宴会厅

主持人：杨静

14:35 - 14:50　Sparse Multiplication of Multivariate Linear Differential Operators　(abstract)
Huang Qiao-Long（山东大学数学与交叉科学研究中心)

14:50 - 15:05　A Companion Curve Tracing Method for Rank-Deficient Polynomial Systems　(abstract)
陈长波（中国科学院重庆绿色智能技术研究院)

15:05 - 15:20　有理数域上一类多项式可约性的一个判别法(abstract)
赵世忠（华东师范大学)

15:20 - 15:35　几类多元多项式矩阵等价问题的研究(abstract)
郑丽翠（湖南科技大学)

15:35 - 15:50　Smith form of triangular multivariate polynomial matrix　(abstract)
Li Dongmei（湖南科技大学)

分组报告 (4)　"密码数学"专题	6 月 5 日 14:35-15:50　榕湖厅

主持人：孙瑶

14:35 - 14:50　Ramp schemes based on CRT for polynomial ring over finite field　(abstract)
Ding Jian（福建师范大学)

14:50 - 15:05　An Optimal Quantum Error-Correcting Procedure Using Quantifier Elimination　(abstract)
Mei Jingyi（East China Normal University）

15:05 - 15:20　Dynamic contest model with bounded rationality　(abstract)
Zhang Ming（山东大学)

15:20 - 15:35　Computing [1,2] open locating domination number in some families of graphs　(abstract)
Raza Hassan（University of Shanghai for Science and Technology）

15:35 - 15:50　高维多项式微分系统 Zero-Hopf 分岔分析及算法推导(abstract)
黄博（北京航空航天大学)

茶歇	6 月 5 日 15:50-16:15　None

分组报告 (5)　"符号计算"专题	6 月 5 日 16:15-17:30　宴会厅

<div align="right">主持人：李冬梅</div>

16:15 - 16:30　New results on the equivalence of bivariate polynomial matrices　(abstract)
Zheng Xiaopeng　(中国科学院数学与系统科学研究院)

16:30 - 16:45　The Invertibility of Rational Univariate Representations　(abstract)
肖水晶 (南昌大学)

16:45 - 17:00　Asymptotic normality in t-stack sortable permutations　(abstract)
陈曦 (大连理工大学)

17:00 - 17:15　稀疏三角分解在生物动力系统平衡点计算中的应用(abstract)
巨雯雯 (北京航空航天大学)

17:15 - 17:30　Efficient Algorithms for Determining Constant Residues　(abstract)
高艺漫 (中国科学院数学与系统科学研究院)

分组报告 (6)　"计算机数学及其应用"专题	6 月 5 日 16:15-17:30　榕湖厅

<div align="right">主持人：徐鸣</div>

16:15 - 16:30　Evolutionary behavior and novel collision of abundant wave solutions to a novel KP-like equation　(abstract)
Feng Yueyang　(Inner Mongolia University of Technology)

16:30 - 16:45　On the probability of generating a primitive matrix　(abstract)
Chen Jingwei　(CIGIT, CAS)

16:45 - 17:00　Verifying the positivity of a function over a finite set　(abstract)
杨剑霆 (中国科学院数学与系统科学研究院)

17:00 - 17:15　基于 Isabelle/HOL 程序规范的 C++ 代码生成(abstract)
许博 (北京林业大学信息学院)

17:15 - 17:30　1884-2016 年香港气候变化特征及其分析(abstract)
孙翔 (上海大学数学系)

晚餐	6 月 5 日 17:30-20:00　金桂厅

计算机数学专业委员会会议	6 月 5 日 20:00-22:00　榕湖厅

<div align="right">主持人：贾晓红</div>

2020 年 6 月 6 日

S2　大会邀请报告 (2)	6 月 6 日 9:00-10:00　宴会厅

主持人:　雷娜

9:00-10:00　机器学习中的一种高效和有效的模型选择策略–Leave Zero Out
陈松灿（南京航空航天大学）

茶歇	6 月 6 日 10:00-10:20　None

Y5　青年邀请报告 (5)	6 月 6 日 10:20-10:50　宴会厅

主持人:　侯庆虎

10:20-10:50　Pattern avoidance and lattice walks
林志聪（山东大学）

Y6　青年邀请报告 (6)	6 月 6 日 10:20-10:50　榕湖厅

主持人:　申立勇

10:20-10:50　方向场驱动的六面体网格剖分
黄劲（浙江大学）

分组报告 (7)　"组合数学"专题	6 月 6 日 10:55-12:10　宴会厅

主持人:　汪荣华

10:55 - 11:10　A note on the Turán number of non-bipartite graphs　(abstract)
Yuan Long-Tu（华东师范大学）

11:10 - 11:25　The balanced edge cover decompositions of graphs　(abstract)
Yu Minghui（Shandong Normal University）

11:25 - 11:40　Efficient Rational Creative Telescoping　(abstract)
Huang Hui（Dalian University of Technology）

11:40 - 11:55　F-factors in quasi-random hypergraphs　(abstract)
孙淑敏（山东大学）

11:55 - 12:10　A Ramsey–Turán theory for tilings in graphs　(abstract)
杨东雷（山东大学）

| 分组报告 (8)　"计算几何"专题 | 6 月 6 日 10:55-12:10　榕湖厅 |

主持人：徐岗

10:55 - 11:10　Quasi-interpolation for data mining　(abstract)
Gao Wenwu（Anhui University）

11:10 - 11:25　Generation of Escher-like Rosette Drawings　(abstract)
欧阳培昌（广西科技大学）

11:25 - 11:40　Introduction of Continuous Collision Detection of Truncated Ellipsoids　(abstract)
Wu Chengran（中国科学院数学与系统科学研究院）

11:40 - 11:55　Isogeometric analysis with error-based local adaptivity for structural vibration　(abstract)
Yu Peng（Guangxi University）

11:55 - 12:10　逼近误差有界的重新网格化(abstract)
傅孝明（中国科学技术大学）

| 午餐 | 6 月 6 日 12:10-14:00　None |

| Y7　青年邀请报告 (7) | 6 月 6 日 14:00-14:30　宴会厅 |

主持人：陈长波

14:00-14:30　无人机集群代数优化协调控制及应用
秦小林（中科院成都计算机应用研究所）

| 分组报告 (09)　"组合数学"专题 | 6 月 6 日 14:35-15:50　金桂厅 |

主持人：杨立波

14:35 - 14:50　A new bijection between RNA secondary structures and plane trees and its consequences　(abstract)
陈小锋（合肥工业大学）

14:50 - 15:05　Non-linear Hamilton cycles in linear quasi-random hypergraphs　(abstract)
舒希超（山东大学）

15:05 - 15:20　On sequences associated to the invariant theory of rank two simple Lie algebras　(abstract)
Zhang Yi（Department of Applied Mathematics, School of Science, Xi'an Jiaotong-Liverpool University, China）

15:20 - 15:35　Integer colorings with forbidden rainbow sums　(abstract)
周文玲（山东大学）

15:35 - 15:50　Properly colored cycles in edge-colored complete graphs containing no monochromatic triangles: a vertex-pancyclic analogous result　(abstract)
李若楠（西北工业大学）

分组报告 (10) "计算几何"专题	6 月 6 日 14:35-15:50 榕湖厅

主持人：朱春钢

14:35 - 14:50　Curvature-based r-adaptive isogeometric analysis with injectivity-preserving multi-sided domain parameterization (abstract)
纪野 (大连理工大学数学科学学院)

14:50 - 15:05　Interactive Design of cubic IPH spline curves with Control Polygon (abstract)
Zhang Jingjing (安徽大学)

15:05 - 15:20　A Neural Network Solver for Knot Placement in B-spline Approximation (abstract)
康红梅 (苏州大学)

15:20 - 15:35　基于 B++ 样条和 Toric 曲面的非连续界面力学问题等几何分析(abstract)
祝雪峰 (大连理工大学)

15:35 - 15:50　Salience-Driven Image Mosaic Method by Edge-Weighted Centroidal Voronoi Tessellations (abstract)
Xiang Bingjin (Hangzhou Dianzi University)

茶歇	6 月 6 日 15:50-16:10 None

分组报告 (11) "组合数学"专题	6 月 6 日 16:10-16:55 金桂厅

主持人：林志聪

16:10 - 16:25　Factors in randomly perturbed hypergraphs (abstract)
Chang Yulin (Shandong University)

16:25 - 16:40　Largest family without a pair of posets on consecutive levels of the Boolean lattice (abstract)
肖继孟 (西北工业大学)

16:40 - 16:55　$Y_{k,b}$-tiling and Hamilton ℓ-cycles in k-uniform hypergraphs (abstract)
孙琳 (山东大学)

分组报告 (12) "符号计算"专题	6 月 6 日 16:10-16:55 榕湖厅

主持人：荆瑞娟

16:10 - 16:25　双变元 Bernstein 展开的逆问题(abstract)
姚勇 (中科院成都计算机应用研究所)

16:25 - 16:40　Computing Strong Regular Characteristic Pairs with Groebner Bases (abstract)
董日娜 (中国科学院重庆绿色智能技术研究院)

16:40 - 16:55　预知分母可能因子的有理函数恢复算法(abstract)
夏朋 (辽宁大学)

Maple 宣讲会	6 月 6 日 17:00-18:00 金桂厅

分组报告 (12') "符号计算"专题	6 月 6 日 17:00-18:00 榕湖厅

主持人: 李子佳

17:00 - 17:15 Gröbner Basis Restriction Theory for Normalization of Indexed Differentials (abstract)
刘姜 (上海理工大学)

17:15 - 17:30 Minimal Representation of a polyhedron and its projections (abstract)
荆瑞娟 (江苏大学)

17:30 - 17:45 整数分拆的符号计算初探(abstract)
李永彬 (电子科技大学)

晚餐	6 月 6 日 18:00-20:00 None

2020 年 6 月 7 日

S3 大会邀请报告 (3)	6 月 7 日 9:00-10:00 宴会厅

主持人: 牟晨琪

9:00-10:00 密码分析中的代数思想
林东岱 (中科院信息工程研究所)

茶歇	6 月 7 日 10:00-10:20 None

分组报告 (13) "组合数学"专题	6 月 7 日 10:20-11:35 宴会厅

主持人: 程民权

10:20 - 10:35 Rainbow spanning structures in graph and hypergraph 2 systems (abstract)
王斌 (山东大学)

10:35 - 10:50 Nonlinear inverse relations of the Bell polynomials via the Lagrange inversion formula (II) (abstract)
王瑾 (浙江师范大学数学与计算机科学学院)

10:50 - 11:05 The log-concavity of Kazhdan-Lusztig polynomials of uniform matroids (abstract)
解红叶 (天津理工大学)

11:05 - 11:20 The maximum size of an edge 2-neighborhood in P5-free graphs (abstract)
许伟伦 (山东师范大学)

11:20 - 11:35 Reverse gamma-expansion for Eulerian polynomials (abstract)
赵彤远 (中国石油大学（北京）)

主持人:　冯如勇

10:20 - 10:35　基于多样化技术的确定性稀疏插值算法(abstract)
　　　　　　　戚妞妞 (桂林电子科技大学数学与计算科学学院)

10:35 - 10:50　Heights of the points on a plane algebraic curve　(abstract)
　　　　　　　冯爽 (中国科学院大学)

10:50 - 11:05　Machine Checked Proof for Some Integral Inequalities　(abstract)
　　　　　　　方敬轩 (中国科学院数学与系统科学研究院)

11:05 - 11:20　有限集上偏序关系的符号计算(abstract)
　　　　　　　张升荣 (电子科技大学数学科学学院)

11:20 - 11:35　Sparse Interpolation With Errors in Chebyshev Basis Beyond Redundant-Block Decoding　(abstract)
　　　　　　　Zhi-Hong Yang　(Shenzhen University)

Abstract Book

第十二届中国数学会计算机数学大会 (CM2021)

广西桂林

大会邀请报告

题目待定

* 江松 (北京应用物理与计算数学研究所)

个人简历：江松，中国科学院院士，北京应用物理与计算数学研究所研究员。主要从事可压缩流体力学数学理论、计算方法及应用研究。在理论方面，对任何绝热指数 >1，与合作者证明了具有大外力的三维定常可压缩 Navier-Stokes (NS) 方程弱解的存在性，以及具有大初值的高维非定常 NS 方程球/轴对称解的整体存在性。在应用方面，针对武器物理数值模拟的多介质大变形、网格畸变等计算难点，与同事一起提出了若干实用的新算法（如整体 ALE 局部欧拉自然耦合方法），并研制完成重大武器型号数值模拟软件平台。曾获国家自然科学二等奖、军队科技进步一等奖、中国青年科技奖、求是杰出青年奖等。

―――――○―――――○―――――○―――――○――――

机器学习中的一种高效和有效的模型选择策略 – Leave Zero Out

* 陈松灿 (南京航空航天大学)

摘要：模型选择是机器学习的核心。交叉验证 (Cross-Validation-CV) 作为一种广泛采用的选择策略，面临多重数据划分验证导致算法效率低以及在少标记学习场景下难奏效等挑战。本报告尝试给出一种无需交叉验证 (Leave-Zero-Out) 的高效和有效的选择新策略，使之更趋于实用。

个人简历：陈松灿，南京航空航天大学计算机科学和技术学院/人工智能学院教授。政府特贴专家。国际模式识别学会会士 (IAPR Fellow) 和中国人工智能学会会士 (CAAI Fellow)。在包括 IEEE Transactions 等在内的国际主流学术期刊上已发表 170 多篇 SCIE 论文，其中 3 篇发表在国际著名期刊《Pattern Recognition》上的论文获 2 年一评的年度最佳论文提名奖 (Best Paper Awards: Honorable Mentions)。1 篇《计算机学报》论文获颁 2010-2014 年 5 年度的 3 篇优秀论文奖之一。1 篇论文获 2016 国际模式识别会议（ICPR2016）"模式识别和机器学习 track"的最佳论文奖. 3 篇论文获全国学术会议的最佳/优秀论文奖。所发论文据 Google Scholar 统计，被引 15000 多次，H-指数 55。2014-2019 连续 6 年入选 Elsevier 中国高引学者榜。现任中国人工智能学会机器学习专委会主任、江苏省计算机学会常务副理事长。分别于 2011 年和 2013 年获教育部自然科学 1 等奖和国家自然科学 2 等奖，排名均为 2。至今主持国家自然科学基金项目 11 项，其中重点项目 1 项。已培养毕业博士生 39 名，6 位获江苏省优博，其中的 2 位继获全国百篇优博论文提名奖。2018 年入选了江苏省第一届"十佳研究生导师团队"。

―――――○―――――○―――――○―――――○――――

密码分析中的代数思想

* 林东岱 (中科院信息工程研究所)

摘要：本报告将从代数的角度介绍几种密码分析方法，探讨其代数性质及其变种，包括数值映射理论、相关立方攻击、差分线性分析等，以及它们在著名密码算法分析中的应用，内容涵盖了我们近年来在 CRYPTO 密码学年会和 EUROCRYPT 密码学年会上发表和即将发表的最新研究成果。

个人简历：林东岱，现任中国科学院信息工程研究所学术委员会主任、研究员、博士生导师，中国密码学会和中国保密协会常务理事、中国电子学会理事，中国密码学会密码数学专业委员会和中国保密协

会隐私保护专业委员会主任委员。主要从事密码学、安全协议、网络与系统安全、分布式密码计算等方面的研究工作，在《IEEE Transaction on Information Theory》、《Designs, Codes and Cryptography》、EUROCRYPT 和 ASIACRYPT 等国内外学术刊物和学术会议上发表论文 200 余篇。先后参加或承担八五攀登计划、九五攀登计划预选项目，国家重大基础研究规划（973）、国家高科技发展计划（863）、国家自然科学基金与中国科学院战略性先导专项等项目。担任《Science China：Information sciences》、《密码学报》、《计算机研究与发展》及《信息安全学报》、《保密科学技术》等杂志编委，《Cybersecurity》和《网络空间安全》杂志副主编以及数十个国际会议大会主席、程序委员会主席或程序委员会委员，曾获 2006 年国家密码科技进步一等奖，2009 年中国科学院"朱李月华优秀教师"奖、2011 年国家科技进步二等奖和 2014 年中国科学院优秀指导教师奖。

————◦————◦————◦————◦————

组合数学中的符号计算问题

* 侯庆虎 (天津大学)

摘要：符号计算已经渗透到组合数学的多个领域，在其中发挥着重要作用。我们将通过一些例子展示符号计算方法在组合中的一些应用。我们首先关注符号求和问题。我们将从经典的 Gosper 算法和 Zeilberger 算法出发，介绍该符号求和的基本思想和方法。然后我们介绍该领域的一些新进展，包括多项式递归序列的求和问题、多重和问题等。其次，我们将介绍分拆等式的机器证明。我们将以 Ramanujan 同余式为例，给出它的 Gröbner 基证明。我们也将给出其基于模形式理论的证明，并介绍该方向的一项新进展。最后，我们将展示吴方法在组合计数问题中的一个应用以及柱形代数分解在组合不等式证明中的应用。

个人简历：侯庆虎，天津大学数学学院教授，副院长。研究方向为组合数学及其应用，相关成果发表在 J. Combin. Theory Ser. A, Adv. in Appl. Math. 等杂志。在组合恒等式的机器证明领域取得系列成果并参与多项应用项目，长期与社科院合作进行城市竞争力研究，获得"孙冶方"经济学奖。国家"优秀青年科学基金"获得者。先后主持和承担了国家 863 计划"生物大数据关键技术"项目，科技部重点研发计划"生物安全专项"，国家自然科学基金重点项目和国家 973 计划多项，国家自然科学基金创新群体项目 1 项，国家自然科学基金天元基金平台建设项目 2 项。出版专著中国城市竞争力报告 No. 14-17（2016-2019 年，每年一册），被社科院评为优秀对策一等奖（2012 年）。现任天津市公共安全大数据中心工程中心技术专家，中国数学会计算机数学专业委员会副主任，天津市数学会副理事长。

————◦————◦————◦————◦————

青年邀请报告

最优化观点下的深度学习：从单层到多层最优化学习

* 刘日升 (大连理工大学)

摘要：In this talk, I will first introduce some fundamental issues of bi-level optimization and connect this optimization tool with a variety of modern learning and vision application problems. Then I try to construct a unified framework to reformulate and understand different categories of existing gradient-based bi-level optimization algorithms. Finally, I would like to introduce our recent works on bi-level optimization and its applications in learning and vision fields.

个人简历：刘日升，教授（破格），博导，大连理工大学几何计算与智能媒体技术研究所所长。主要研究方向为机器学习、优化方法、计算机视觉等，发表 CCF/CAA 推荐期刊和会议论文 70 余篇，其中 A 类 30 余篇。成果获得教育部自然科学二等奖 1 项，辽宁省自然科学二等奖 1 项，多媒体旗舰会议 ICME Best Student Paper 奖 2 篇（2014、2015 连续两届），ICME 2017 Best Paper Finalist 奖 2 篇（TOP 3 %），图像处理知名会议 ICIP 2015 TOP 10% Paper 奖 1 篇，VALSE 2018 最受关注 Poster 奖 1 篇。担任 Journal of Electronic Imaging 资深编委（Senior Editor），The Visual Computer 和 IET Image Processing 编委，ICPR 和 ACCV 领域主席（Area Chair），AAAI 和 IJCAI 高级程序委员（Senior PC），CV/ML 领域全部 CCF 推荐 A 类会议（NIPS、ICML、CVPR、ICCV、AAAI、IJCAI、ACM MM 等）程序委员（PC），VALSE 执行 AC 委员会副主席。获得国家"优秀青年科学基金"，辽宁省兴辽英才计划"青年拔尖人才"，辽宁省"百千万人才工程"（千层次），香港-内地"香江学者"等。

—————◦—————◦—————◦—————◦—————

New Constructions of Optimal Cyclic (r,δ) Locally Repairable Codes from Their Zeros

* 郑大彬 (湖北大学)

摘要：An (r,δ)-locally repairable code ((r,δ)-LRC for short) was introduced by Prakash et al. for tolerating multiple failed nodes in distributed storage systems, which was a generalization of the concept of r-LRCs produced by Gopalan et al.. An (r,δ)-LRC is said to be optimal if it achieves the Singleton-like bound. Recently, Chen et al.[1] generalized the construction of cyclic r-LRCs proposed by Tamo et al.[3,4] and constructed several classes of optimal (r,δ)-LRCs of length n for $n|(q-1)$ or $n|(q+1)$, respectively in terms of a union of the set of zeros controlling the minimum distance and the set of zeros ensuring the locality. Following the work of [1,2], this paper first characterizes (r,δ)-locality of a cyclic code via its zeros. Then we construct several classes of optimal cyclic (r,δ)-LRCs of length n for $n|(q-1)$ or $n|(q+1)$, respectively from the product of two sets of zeros. Our constructions include all optimal cyclic (r,δ)-LRCs proposed in [1, 2], and our method seems more convenient to obtain optimal cyclic (r,δ)-LRCs with flexible parameters. Moreover, many optimal cyclic (r,δ)-LRCs of length n for $n|(q-1)$ or $n|(q+1)$, respectively such that $(r+\delta-1)\nmid n$ can be obtained from our method.

个人简历：郑大彬，男，1977 年 4 月生，理学博士。现为湖北大学数学与统计学学院教授、博士生导师、副院长，中国数学会理事、中国数学会计算机数学专业委员会委员、湖北省数学会理事。2006 年于中科院数学与系统科学研究院获博士学位，2009 年 6 月至 2012 年 4 月在中科院研究生院信息安全国家重点实验室从事博士后研究工作，2015 年 3 月至 2016 年 2 月在美国特拉华大学访问、学习。研究方向为编码密码学，主持国家自然科学基金项目 3 项和省部级项目多项。在《IEEE Transactoins on Information Theory》、《Design, Codes and Cryptography》、《Finite Fields and Their Applications》、《Discrete

Mathematics》、《Cryptography and Communications》、《SCIENCE CHINA Mathematics》等国内外学术刊物和会议上发表文章 30 余篇。曾获得第 31 届国际符号与代数计算 (ISSAC2006) 年会杰出论文奖。

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

Pattern avoidance and lattice walks

* 林志聪 (山东大学)

摘要：I will present some intriguting connections between pattern avoiding permutations and lattice walks.

个人简历：山东大学数学与交叉科学研究中心教授、博士生导师。2014 年博士毕业于法国里昂第一大学，2015 年-2018 年在韩国数理科学研究所和维也纳大学从事博士后研究工作。研究的主要兴趣是计数和代数组合，尤其是排列统计量和图同态的计数。

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

无人机集群代数优化协调控制及应用

* 秦小林 (中科院成都计算机应用研究所)

摘要：本报告简要介绍了无人机集群智能的前世今生，目前集群智能的典型应用场景，和主要关键技术与面临的一些挑战。最后，介绍了面向无人机集群智能的代数优化协调控制方法，包括编队构型代数优化控制和自主避障代数优化算法等。

个人简历：博士，研究员，中国科学院成都计算机应用研究所自动推理实验室主任，中国科学院大学教授，博士生导师，四川省"天府万人计划"专家。成都市科青联副主席、中国电子学会生物计算与生物信息处理专委会副理事长、中国数学会计算机数学专业委员会委员，四川省青年联合会第十四届委员。主持国家自然科学基金、四川省人工智能重大专项、省部级科研项目等 10 余项；参与军委科技委重大专项、创新特区课题、国家 973 项目、国家自然科学基金（重点项目）、中国科学院知识创新工程、中国科学院西部之光等 10 余项。在国内外重要期刊、会议发表论文 50 多篇（其中 SCI/EI 检索 40 余篇），申请国家发明专利 10 余项。获中国科学院院长优秀奖、中国科学院"西部青年学者"、四川省海外高层次留学人才、中国科学院"西部之光"人才培养计划、中国科学院"青年创新促进会"会员等。

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

Multistability of Small Reaction Networks

* 唐晓弦 (北京航空航天大学)

摘要：The multistability problem of biochemical reaction systems is crucial for understanding basic phenomena such as decision-making process in cellular signaling. Mathematically, it is a challenging real quantifier elimination problem. We present some recent progress on multistability of small reaction

networks. 1) For reaction networks with two reactions (possibly reversible), we find the multistable networks those have the minimum numbers of reactants and species. 2) For reaction networks with one-dimensional stoichiometric subspaces, we give the relation between the maximum numbers of stable steady states and steady states.

个人简历：唐晓弦 2014 年毕业于北京大学数学科学学院并取得博士学位。博士就读期间曾在美国北卡州立大学进行联合培养。取得博士学位之后，她先后在韩国国家数学研究所，德国不来梅大学以及美国德州农工大学从事博士后研究，博后期间曾到布朗大学计算与实验数学中心进行学期访问。她于 2019 年获得北京航空航天大学卓越百人计划的支持。主要研究方向是符号计算，生物数学及代数统计，研究兴趣为计算代数几何在生物与统计中的应用。在 Biometrika, Journal of Mathematical Biology, Bulletin of Mathematical Biology, SIAM Journal on Discrete Mathematics, 及 Journal of Symbolic Computation 等国际高水平期刊上发表论文。曾组织或参与 SIAM Conference on Applied Algebraic Geometry, SIAM Conference on Life Science, ISSAC, 及 ICMS 等国际前沿会议并作学术报告。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

方向场驱动的六面体网格剖分

* 黄劲 (浙江大学)

摘要：Hex mesh is attractive for many applications, but automatic and robust generation of high quality hex mesh is an open problem. Quadrangulation methods based on multi-chart parameterization achieve great success in these years. As a consequence, applying similar strategy for hex remeshing is a natural and promising idea.

This talk will introduce our attempts about this problem. First, we proposed spherical harmonic representation for general topology, analyzed and fixed all the local topological conflict. Second, to bypass the challenge of global conflict, we aimed at the hex meshes without any internal singularity, started from the ones associated with exact form, and then extended the technique to the superset of exact form, i.e. closed form. One of our latest work shows that the "smoothness" is indeed defined by integrability under metric instead of heuristically defined from aesthetic consideration. This talk will summarize our works: In global topology, we build the nested topological structure from the general topology, closed form and exact form; in local integrability, from locally Euclidean assumption to locally flat metric assumption.

个人简历：黄劲博士、教授，主要研究计算机图形学中几何计算以及物理模拟方面的课题。为在计算机离散计算的模式下，高效准确地再现连续的数学和物理行为，黄劲课题组在重网格化、弹性问题和流体问题的线性化降维、异质异构问题的均质化等方面开展了一系列的研究，发表二十余篇顶级学术论文，并获得多项发明专利授权，其中包括关于六面体网格自动生成的美国专利。2013-2014 加州理工学院访问学者，2015 年获国家优秀青年基金资助。研究受国家自然科学基金、美国通用汽车公司、上海核工程研究设计院等项目的资助。曾担任包括 ACM SIGGRAPH 在内的一些著名国际学术会议的程序委员会委员，Geometric Modeling and Processing、Symposium on Computer Animation 等几何、模拟方向的国际学术会议程序共同主席，著名学术期刊 CAGD，CGF 的副主编。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

四元数代数在彩色图像处理中的应用研究

* 蓝如师 (桂林电子科技大学)

摘要: Quaternionic representation (QR) of the color image encodes a color pixel using a quaternion. In this way, we can handle all color channels directly in the quaternionic domain and include their relations simultaneously. QR gives a new perspective for color image processing. In this talk, I will introduce some applications using QR of the color images in recent years, including image denoising, local feature extraction, dimension reduction, and QR-based deep neural network.

个人简历：蓝如师，桂林电子科技大学校聘教授，硕士生导师，广西图像图形与智能处理重点实验室副主任，中山大学国家数字家庭工程技术研究中心客座研究员。主要研究领域为图像处理、模式分类、医学信息处理。主持 2 项国家自然科学基金，并作为核心人员参与多项国家级及省部级项目。以第一作者在包括 IEEE TIP、IEEE TCYB、IEEE TCSVT、ICME、ICIP 等国内外重要期刊与学术会议上发表论文 30 余篇。入选广西高校引进海外高层次人才"百人计划"、广西第一批高层次人才（E 层次）及桂林电子科技大学"英才计划"，获广西杰出青年科学基金资助。

$$- - - - \circ - - - - \circ - - - - \circ - - - - \circ - - - -$$

分组报告

[P000002]

用符号计算证明 Ramsey 定理的机械化方法

* 鲁健 (上海大学数学系)　曾振柄 (上海大学数学系)

论文给出了 Ramsey 定理自动证明的代数化方法，并使用符号计算软件实现了 R(3,3)=6 和 R(3,4)=9 的自动证明，并讨论了处理更复杂情况，包括 R(3,5)=14 和 R(3,3,3)=17 等情形的分治法. 不同于以往的计算机辅助计算方法，本文通过将 Ramsey 问题转化为有限域上的多项式的展开合并过程，得到了 Ramsey 定理的机械化证明. （论文申请投稿《系统科学与数学》）

————∘————∘————∘————∘————

[P000003]

The convergence of an efficient Levenberg-Marquardt method for nonlinear equations under Holderian local error bound

* Liang Chen (Huaibei Normal University)　Yanfang Ma (Huaibei Normal University)

The Levenberg-Marquardt method is a famous numerical method for solving system of nonlinear equations and nonlinear least-squares problems. By using trust region technology, the Levenberg-Marquardt method with a new choice of the LM parameter is presented in this paper. The new choice of the LM parameter can be considered as a generalization of some other choices. By using the Hölderian local error bound of function and Hölderian continuity of its Jacobian instead of the commonly used local error bound and Lipschitz continuity of Jacobian respectively, the sequence generated by the Levenberg-Marquardt method has been shown to have global convergence, and to converge to a solution of nonlinear equations superlinearly and even quadratically for some special parameters. Numerical results show that the method performs well for singular problems.

————∘————∘————∘————∘————

[P000004]

Sparse Multiplication of Multivariate Linear Differential Operators

Giesbrecht Mark (David R. Cheriton School of Computer Science, University of Waterloo)　*
Huang Qiao-Long (山东大学数学与交叉科学研究中心)　Schost Eric (David R. Cheriton School of Computer Science, University of Waterloo)

We propose a new randomized algorithm for multiplication in the ring of non-commutative polynomials $K[x_1, \ldots, x_n] < \delta_1, \ldots, \delta_n >$, where $\delta_i = x_i(\frac{\partial}{\partial x_i})$, dedicated to sparse inputs. The complexity of our algorithm is polynomial in the input size and on an a priori sparsity bound for the output.

————∘————∘————∘————∘————

A note on the Turán number of non-bipartite graphs

Peng Xing (安徽大学)   * Yuan Long-Tu (华东师范大学)

Given a family of graphs $\mathcal{L}$, the Turán number $\mathrm{ex}(n, \mathcal{L})$ is the maximum possible number of edges in an n-vertex $\mathcal{L}$-free graph. The famous Erdős-Stone-Simonovits Theorem gives us the asymptotic value of $\mathrm{ex}(n, \mathcal{L})$.

The famous Erdős-Stone-Simonovits Theorem asserts the following:

$$\mathrm{ex}(n, \mathcal{L}) = t_p(n) + o(n^2) = \left(1 - \frac{1}{p}\right)\binom{n}{2} + o(n^2),$$

where $p = \min\{\chi(\mathcal{L}) : L \in \mathcal{L}\} - 1$ and $t_p(n)$ is the number of edges in a p-partite Turán graph. Therefore, if $p(\mathcal{L}) \geq 2$, i. e., $\mathcal{L}$ does not contain bipartite graphs, then the Erdős-Stone-Simonovits Theorem tells us the asymptotic value of $\mathrm{ex}(n, \mathcal{L})$. For $p(\mathcal{L}) \geq 2$, in order to determine the exact value of $\mathrm{ex}(n, \mathcal{L})$, Simonovits introduced the notion of the decomposition family $\mathcal{M}(\mathcal{L})$ of $\mathcal{L}$.

In this paper, we study the Turán number of those families of graphs such that their decomposition families $,\mathcal{M}(\mathcal{L})$ contain a matching and a star. To be precisely, we prove tight bounds on the Turán number of such families of graphs. We note that the upper bound proved in this paper improving upon the following result by Bollobás for such families of graphs. For sufficiently large n, we have

$$t_p(n) + \mathrm{ex}(\lceil n/p \rceil, \mathcal{M}(\mathcal{L})) \leq \mathrm{ex}(n, \mathcal{L}) \leq t_p(n) + (1 + o(1))p \cdot \mathrm{ex}(n/p, \mathcal{M}(\mathcal{L})) + cn,$$

In addition, we show the product conjecture by Simonovites is true for special families of graphs.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — — —

无需 Clifford 门分解与实表示的量子全同态加密方案

* 马光胜 (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)

本文提出了一种新的量子全同态加密（QFHE）方案，该方案允许实现控制旋转门，其中控制比特处于加密形式。在我们的方案中，可以直接对一般量子线路进行同态估计，而无需事先计算待估线路的 Clifford 门分解或实表示。在同态估计量子傅里叶变换时，一定条件下，我们的 QFHE 方案对比前人具有多项式提速。

我们 QFHE 方案的安全性基于底层经典 FHE 方案，而后者的安全性基于误差学习问题（LWE）和循环安全性假设。

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — — —

Improve the Robustness and Accuracy of Deep Neural Network with $L_{2,\infty}$ Normalization

高小山 (中国科学院数学与系统研究院) * 于立佳 (中国科学院数学与系统研究院)

In this paper, we enhance the robustness and accuracy of deep neural network (DNN) by introducing the $L_{2,\infty}$ normalization of the weight matrices of DNN with Relu as the activation function. It is proved that the $L_{2,\infty}$ normalization leads to large dihedral angles between two adjacent faces of the DNN function graph and hence smoother DNN functions, which reduces over-fitting of the DNN. A measure is proposed for the robustness of a classification DNN, which is the union of the volumes of the maximal robust spheres with the sample points as centers. A lower bound for the robustness measure in terms of the $L_{2,\infty}$ norm is given. Finally, an upper bound for the Rademacher complexity of DNN with $L_{2,\infty}$ normalization is given. An algorithm is given to train a DNN with the $L_{2,\infty}$ normalization and experimental results are used to show that the $L_{2,\infty}$ normalization is effective in terms of improving the robustness and accuracy.

$- - - - \circ - - - - \circ - - - - \circ - - - - \circ - - - -$

Quasi-interpolation for data mining

* Gao Wenwu (Anhui University)

Quasi-interpolation has been a useful scheme for data mining. In this talk, I will introduce some developments of quasi-interpolaiton and our recent works on quasi-interpolation including constructing quasi-interpolation, studying properties of quasi-interpolation and discussing its applications.

$- - - - \circ - - - - \circ - - - - \circ - - - - \circ - - - -$

Generation of Escher-like Rosette Drawings

* 欧阳培昌 (广西科技大学)   Gdawiec Krzysztof (Institute of Computer Science, University of Silesia)   Fathauer Rober (Tessellations Company)   Nicolas Alain (Nicolas Tessellation)   Kwok Wai Chung (Department of Mathematics, City University of Hong Kong)

"Smaller and Smaller" and "Sphere Surface with Fish" are two artworks by the Dutch artist M.C. Escher. Their whole idea and layout are exceptionally complex and beautiful. This paper proposes an easy method to generate drawings similar to "Smaller and Smaller" and "Sphere Surface with Fish". To this end, the geometrical structure of rosette tilings is first considered from the viewpoint of symmetry group in detail. This gives a simple way to construct rosette tilings. Then, to embed a pre-designed template into kite-shaped tiles of rosette tilings, a one-to-one mapping between kite-shaped and square regions is presented. Finally, some detailed implements of producing rosette and spherical drawings are specified. The presented examples show that by using the existing rich wallpaper templates, the method proposed in the paper can generate a variety of Escher-like rosette drawings.

————∘————∘————∘————∘————

基于多样化技术的确定性稀疏插值算法

* 戚妞妞 (桂林电子科技大学数学与计算科学学院)　唐敏 (桂林电子科技大学数学与计算科学学院)
邓国强 (桂林电子科学大学数学与计算科学学院)

稀疏多元多项式插值用于构造黑盒函数, 是求解多项式代数问题的一种有效策略, 具有多项式时间复杂度的多元稀疏插值算法已得到广泛研究和使用. 近期 Huang 提出了一个基于多样化技术的稀疏多项式插值算法, 计算复杂度为 $O(nT \log^2 q + nT\sqrt{D} \log q)$, 是有限域上首个关于变元个数 n 和项数界 T 的线性函数, 关于次数界 D 的分数次幂的高效算法. 然而, Huang 的算法是概率性的, 准确恢复黑盒多项式的成功率为 3/4. 本文分析了 Huang 算法失效的三种情形, 给出了相应的修正方案, 基于此设计了一个确定性的稀疏多项式插值算法, 并用大量的随机数值实验证实了该算法的有效性.

————∘————∘————∘————∘————

Analyzing the barren plateau phenomenon in training quantum neural networks with the ZX-calculus

* 赵宸 (中国科学院数学与系统科学研究院)　高小山 (中国科学院数学与系统科学研究院)

We propose a general scheme to analyze the gradient vanishing phenomenon, also known as the barren plateau phenomenon, in training quantum neural networks with the ZX-calculus. More precisely, we extend the barren plateaus theorem from unitary 2-design circuits to any parameterized quantum circuits under certain reasonable assumptions. The main technical contribution of this work is representing certain integrations as ZX-diagrams and computing them with the ZX-calculus. The method is used to analyze four concrete quantum neural networks with different structures. It is shown that, for the hardware efficient ansatz and the MPS-inspired ansatz, there exist barren plateaus, while for the QCNN ansatz and the tree tensor network ansatz, there exists no barren plateau.

————∘————∘————∘————∘————

Introduction of Continuous Collision Detection of Truncated Ellipsoids

* Wu Chengran (中国科学院数学与系统科学研究院)　Li Hongbo (中国科学院数学与系统科学研究院)

Collision detection is an important research subject in motion analysis. Now that ellipsoid is the primitive to fit moving objects, the study of continuous collision detection of ellipsoids is important. Previous researches always use complete ellipsoids to fit objects, however, in many cases this is not satisfactory. In this paper, we use truncated quadratic surface to fit objects, and solve the problem of continuous collision detection of truncated ellipsoids.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

The maximum size of an edge 2-neighborhood in P5-free graphs

* 许伟伦 (山东师范大学)　张霞 (山东师范大学)

For a graph $G = (V, E)$ and an edge $uv \in E(G)$, the 2-neighborhood of uv is the set of all edges having at least one endvertex in $N(u) \cup N(v)$. A graph is called P_5-free if it contains no induced subgraphs isomorphic to a path with 5 vertices. For P_5-free graphs, we show that the maximum cardinality of an edge 2-neighborhood is at most $\frac{5\Delta^2}{4}$, where Δ is the maximum degree of graphs. When Δ is even, this bound is tight and we confirms the strong edge-coloring conjecture posed by Erdős and Nešetřil for P_5-free graphs.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Asymptotic normality in t-stack sortable permutations

* 陈曦 (大连理工大学)

The problem of stack sorting was introduced by Knuth in 1960s and many variations have been considered since then. Let $W_t(n, k)$ be the number of t-stack sortable n-permutations with $k - 1$ descents. Then $W_1(n, k)$ and $W_{n-1}(n, k)$ correspond to the Narayana numbers and the Eulerian numbers, respectively. In this talk, we show that the numbers $W_t(n, k)$ satisfy central and local limit theorems for $t = 1, 2, n - 1$ and $n - 2$. This result, in particular, gives an affirmative answer to Lou Shapiro's question about the asymptotic normality of the Narayana numbers. As a generalization, we also show the asymptotic normality of Callan's m-th order Narayana numbers. This talk is based on joint work with Jianxi Mao, Yi Wang, Arthur L.B. Yang, and James J.Y. Zhao.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

有理数域上一类多项式可约性的一个判别法

* 赵世忠 (华东师范大学)

任给一个 m 次的整系数多项式 $\sum\limits_{i=0}^{m} a_i x^i$, 本文给出一种不动点迭代算法:

$$\begin{cases} u_1 = \tilde{u}_1, \\ u_2 = \tilde{u}_2, \\ \qquad \vdots \\ u_{m-1} = \tilde{u}_{m-1}, \\ u_n = -\dfrac{1}{a_m}\left(a_{m-1} + \dfrac{a_{m-2}}{u_{n-1}} + \dfrac{a_{m-3}}{u_{n-1}u_{n-2}} + \cdots + \dfrac{a_0}{u_{n-1}u_{n-2}\cdots u_{n-(m-1)}}\right) \ (n \geq m). \end{cases}$$

不难看出, 若该迭代具有一个有理数极限值, 则该值为多项式的一个零点, 从而多项式在有理数域上可约. 值得注意的是, 该迭代具有 "勿需选择初始点" 的特征: (1) 若多项式有 m 个绝对值互不相同的有理数零点, 那么任意取 $m-1$ 个非零有理初始点 $\tilde{u}_i (1 \leq i \leq m-1)$, 迭代均趋近于其中一个零点, 因此, 多项式可约. (2) 实验表明, 若多项式有一个有理数零点, 并且其绝对值大于复数域上其余 $m-1$ 个零点的模, 则任取 $m-1$ 个初始点, 多数情形下, 迭代均会收敛于该零点. (3) 进一步, 在前两种情形中, 若极限值零点的绝对值 $|u|$ 远大于 "模小于该 $|u|$" 的零点的模, 则由极少次 (比如 2 次) 迭代, 就可获得零点许多位的有效数字.

— — —— ∘ — — —— ∘ — — —— ∘ — — —— ∘ — — ——

A Companion Curve Tracing Method for Rank-Deficient Polynomial Systems

吴文渊 (中国科学院重庆绿色智能技术研究院)   * 陈长波 (中国科学院重庆绿色智能技术研究院)

We propose a method for tracing implicit real algebraic curves defined by polynomials with rank-deficient Jacobians. For a given curve $f^{-1}(0)$, it first utilizes a regularization technique to compute at least one witness point per connected component of the curve. We improve this step by establishing a sufficient condition for testing the emptiness of $f^{-1}(0)$. We also analyze the convergence rate and carry out an error analysis for refining the witness points. The witness points are obtained by computing the minimum distance of a random point to a smooth manifold embedding the curve while at the same time penalizing the residual of f at the local minima. To trace the curve starting from these witness points, we prove that if one drags the random point along a trajectory inside a tubular neighborhood of the embedded manifold of the curve, the projection of the trajectory on the manifold is unique and can be computed by numerical continuation. We then show how to choose such a trajectory to approximate the curve by computing eigenvectors of certain matrices. Effectiveness of the method is illustrated by examples.

— — —— ∘ — — —— ∘ — — —— ∘ — — —— ∘ — — ——

基于超像素合并的超像素级高光谱图像分类

谢福鼎 (辽宁师范大学)　＊李旭 (辽宁师范大学)　黄丹 (辽宁师范大学)　金翠 (辽宁师范大学)

超像素级的高光谱图像分类是一类有代表性的谱-空分类方法. 与像素级分类方法相比, 超像素级的分类方法在分类精度和分类效率方面都有明显的优势. 然而, 超像素级分类算法的主要缺点是分类结果严重依赖于超像素的分割尺度. 已有的文献表明, 最优超像素分割尺度的获得往往是一个实验结果, 很难预先确定. 为了削弱这种依赖性, 本文提出了一种基于超像素合并的超像素级高光谱分类算法. 该方法首先采用局部模块度函数对所构造的稀疏加权超像素图进行合并; 然后通过新定义的映射将每一个超像素块表示为一个样本点, 使用流行的 KNN 方法对合并后的超像素图像进行超像素级分类. 超像素的合并增强了空间信息在分类中的作用, 有效地削弱了分类结果对超像素分割尺度的依赖性, 并提高了分类精度. 为了评价该方法的有效性, 在两个公开的基准高光谱数据集上, 将所提出的方法与一些先进的高光谱图像分类方法进行了实验和对比. 实验结果和比较结果表明, 该方法不仅有效削弱了超像素分割尺度对分类结果的影响, 且在分类精度和计算效率方面都有十分明显的优势.

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

Heights of the points on a plane algebraic curve

＊ 冯爽 (中国科学院大学)　冯如勇 (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)

Let $\overline{K}$ be an algebraic closed field of characteristic zero, and $\mathfrak{h}$ be an absolute height on $\overline{K}$. Suppose that $f(x,y)$ is an irreducible polynomial in $\overline{K}[x,y]$ and $a,b \in \overline{K}$ satisfies $f(a,b) = 0$. We explicitly describe the relation between $\mathfrak{h}(a)$ and $\mathfrak{h}(b)$ by $\mathrm{tdeg}(f)$ and $\mathfrak{h}(f)$.

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

分布式存储编码研究进展

＊ 侯韩旭 (东莞理工学院)

纠删码被广泛的应用于分布式存储系统中以达到数据的高可靠性和低存储冗余。MDS 码是一类满足 MDS 特性的纠删码, 可以达到数据可靠性与存储冗余的最优折中。然而, 传统 MDS 码的修复带宽 (定义为修复一个失效节点需要从其它节点下载的数据量) 太大。再生码 (Regenerating Codes) 是满足 MDS 特性且达到存储冗余与修复带宽的最优折中曲线的一类存储编码。精确修复再生码的构造方法已被学术界广泛研究, 然而并没有大规模的应用在分布式存储系统中。本文分析了现有再生码在商用存储系统中应用的缺陷：(i) 再生码没有考虑商用存储系统的机架结构, 商用存储系统一般有多个机架通过核心网络连接, 而每个机架中可以插入多个存储节点, 机架间的网络带宽远小于机架内的网络带宽, 而再生码的跨机架修复带宽 (定义为修复一个失效节点需要在机架间下载的数据量) 不是最优的；(ii) 现有高码率再生码均具有分包数大和有限域大的特点, 分包数大会导致修复性能降低, 而有限域大会导致计算复杂度高。针对以上再生码的两大缺陷, 本文将从不同的角度分别介绍现有的研究进展并提出可行的研究方向。

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — —

[P000025]

Dynamic contest model with bounded rationality

* Zhang Ming (山东大学)   Xu Jin (山东大学)

This paper is devoted to exploring the complex dynamics of contest model, where two agents compete for some object with asymmetric valuations by simultaneously choosing efforts at each step. We build the nonlinear discrete system to describe the dynamic contest with bounded rationality, and discuss the stability conditions of the Nash equilibrium theoretically. Meanwhile, our numerical simulation experiments also reveal that the model can exhibit very complex dynamical behaviors. In particular, there exist two different routes to chaos for the system: the period-doubling (flip) bifurcation which leads to periodic cycles and chaos, and the Neimark-Sacker bifurcation which derives an attractive invariant closed curve. These two routes are significantly different for economic views. In addition, the stability of Nash equilibrium point is badly affected by the system parameters, such as the adjustment speeds, the values of the object, and so on. Therefore, the parameter adjustment method could be properly applied to make the system return to its stable state.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — —

[P000026]

几类多元多项式矩阵等价问题的研究

李冬梅 (湖南科技大学)   桂盈盈 (湖南科技大学)   * 郑丽翠 (湖南科技大学)

多维系统常用多项式矩阵来描述，系统理论中的多维系统等价问题也常被转化为多项式矩阵等价问题进行研究。本文主要研究两类多元多项式矩阵的等价问题，得到这些矩阵分别与其 Smith 型等价的判别条件。这些条件的检验是比较容易实现的，文中也通过等价实例进行说明。

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — —

Computing [1,2] open locating domination number in some families of graphs

* Raza Hassan (University of Shanghai for Science and Technology)

The problem of location detection is investigated for many scenarios, such as pointing out the flaws in the multiprocessors, invaders in buildings and facilities, and utilizing wireless sensors networks for the environmental monitoring process. The system or structure can be illustrated as a graph in each of these applications, and sensors strategically placed at a subset of vertices can determine and identify irregularities within the network. The (OLD-set) that is open locating dominating set is a subset of vertices in a graph, such that every vertex within the graph is distinct and non-empty. Let $G = (V, E)$, be the graph, a set $S \subseteq V(G)$ is a $[1, 2]$-OLD set if $N(i) \cap S \neq \emptyset$, for some $i \in V(G)$, and $1 \leq |N(i) \cap S| \leq 2$, as well as $N(i) \cap S \neq N(j) \cap S$, for every pair of distinct vertices $i, j \in V(G) \backslash S$. The minimum cardinality of $[1, 2]$-OLD set in a graph G is called $[1, 2]$-open locating domination number and is denoted by $\gamma_{[1,2]}^{old}$. In this paper, we compute the $[1, 2]$-open locating domination number of some families of graphs.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — —

F-factors in quasi-random hypergraphs

丁来浩 (华中师范大学)   韩杰 (罗德岛大学)   * 孙淑敏 (山东大学)   王光辉 (山东大学)   周文玲 (山东大学)

Given $k \geq 2$ and two k-graphs (k-uniform hypergraphs) F and H, an F-factor in H is a set of vertex disjoint copies of F that together covers the vertex set of H. Lenz and Mubayi [J. Combin. Theory Ser. B, 2016] studied the F-factor problem in quasi-random k-graphs with minimum degree $\Omega(n^{k-1})$. They posed the problem of characterizing the k-graphs F such that every sufficiently large quasi-random k-graph with constant edge density and minimum degree $\Omega(n^{k-1})$ contains an F-factor, and in particular, they showed that all linear k-graphs satisfy this property.

In this paper we prove a general theorem on F-factors which reduces the F-factor problem of Lenz and Mubayi to a natural sub-problem, that is, the F-cover problem.

By using this result, we answer the question of Lenz and Mubayi for those F which are k-partite k-graphs, and for all 3-graphs F, separately. Our characterization result on 3-graphs is motivated by the recent work of Reiher, Rödl and Schacht [J. Lond. Math. Soc., 2018] that classifies the 3-graphs with vanishing Turán density in quasi-random k-graphs.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — —

Gröbner Basis Restriction Theory for Normalization of Indexed Differentials

* 刘姜 (上海理工大学)

It is a fundamental problem to determine the equivalence of indexed differential polynomials in both computer algebra and differential geometry. However, in the literature, there are no general computational theories for this problem. The main reasons are that the ideal generated by the basic syzygies cannot be finitely generated, and it involves eliminations of dummy indices and functions. This paper solves the problem by extending Gröbner basis theory. We first present a division of the set of elementary indexed differential monomials $\mathbf{E}_\partial$ into disjoint subsets, by defining an equivalence relation on $\mathbf{E}_\partial$ based on Leibniz expansions of monomials. The equivalence relation on $\mathbf{E}_\partial$ also induces a division of a Gröbner basis of basic syzygies into disjoint subsets. Furthermore, we prove that the dummy index numbers of the sim-monomials of the elements in each equivalence class of $\mathbf{E}_\partial$ have upper bounds, and use the upper bounds to construct fundamental restricted rings. Finally, the canonical form of an indexed differential polynomial proves to be the normal form with respect to a subset of the Gröbner basis in the fundamental restricted ring. In further work, the results of this paper will be used to develop computational theories for more general indexed polynomials, and for similar-indexed polynomials, which can be applied to mechanical theorem-proving in differential geometry and to solving some basic problems in graph theory, including finding the canonical labeling of multi-weighted directed graphs, and the problem of how to add the least edges to turn a directed graph into a Hamiltonian graph.

——— ◦ ———— ◦ ———— ◦ ———— ◦ ————

New results on the equivalence of bivariate polynomial matrices

* Zheng Xiaopeng (中国科学院数学与系统科学研究院)   Lu Dong (北京航空航天大学)   Wang Dingkang (中国科学院数学与系统科学研究院)   Xiao Fanghui (湖南师范大学)

This paper investigates the equivalence problem of bivariate polynomial matrices. A necessary and sufficient condition for the equivalence of a square matrix with the determinant being some power of a univariate irreducible polynomial and its Smith form is proposed. Meanwhile, we present an algorithm that reduces this class of bivariate polynomial matrices to their Smith forms, and an example is given to illustrate the effectiveness of the algorithm. The results presented in the paper are also true for the non-square case.

——— ◦ ———— ◦ ———— ◦ ———— ◦ ————

[P000032]

The Invertibility of Rational Univariate Representations

* 肖水晶 (南昌大学)　曾广兴 (南昌大学)

In this paper, the so-called invertibility is introduced for rational univariate representations, and a characterization of the invertibility is given. It is shown that the rational univariate representations, obtained by both Rouillier's approach and Wu's method, are invertible. Moreover, the ideal created by a given rational univariate representation is defined. Some results on invertible rational univariate representations and created ideals are established. Based on these results, a new approach is presented for decomposing the radical of a zero-dimensional polynomial ideal into an intersection of maximal ideals.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

[P000033]

A Neural Network Solver for Knot Placement in B-spline Approximation

* 康红梅 (苏州大学)

Automatically determining knot number and positions is a fundamental and challenging problem in B-spline approximation. In this talk, the knot placement is abstracted as a mapping from initial knots to the optimal knots. We innovatively introduce a deep neural network solver to approximate the mapping. The neural network is composed of several subnetworks. Each subnetwork is designed to approximate the optimal knot positions in the case of fixed knot number. All the subnetworks are stacked together to find the optimal knots (including knot number and knot positions) within some given tolerance. Owing to the powerful approximation capabilities, as well as mature algorithms developed in deep learning, the proposed method can effectively and efficiently find the optimal knot number and knot positions.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

A Ramsey–Turán theory for tilings in graphs

* 杨东雷 (山东大学)

Given an integer $r \geq 2$ and a graph G, let $\alpha_r(G)$ be the maximum size of a K_r-free subset of vertices and write $\alpha(G) = \alpha_2(G)$. A central topic in Ramsey–Turán theory, initiated by Erdős and Sós, is to determine $RT_r(n; H; o(n))$, the minimum number of edges which guarantees that every n-vertex graph G with $\alpha_r(G) = o(n)$ contains a copy of H. For a k-vertex graph F and a graph G, an F-tiling is a collection of vertex-disjoint copies of F in G. We call an F-tiling perfect if it covers the vertex set of G. We will also refer to a perfect F-tiling as an F-factor, which is a fundamental object in graph theory with a wealth of results from various aspects. Motivated by Ramsey-Turán theory, a recent trend has focused on reducing the minimum degree condition forcing the existence of F-factors in graphs by adding an extra condition that provides pseudorandom properties.

In this talk, we mainly investigate the effect of imposing the condition that $\alpha_r(G) = o(n)$ by studying the minimum degree thresholds for K_k-tilings, and more generally, F-tilings. Similar questions for F-factors are considered where the condition $\alpha_r(G) = o(n)$ is replaced by $\alpha_r^*(G) = o(n)$ (r-partite hole number).

$$- - -- \circ - - -- \circ - - -- \circ - - -- \circ - - --$$

Efficient Rational Creative Telescoping

Giesbrecht Mark (University of Waterloo)   * Huang Hui (Dalian University of Technology)
Labahn George (University of Waterloo)   Zima Eugene (Wilfrid Laurier University)

In this talk, we describe a most recent algorithm developed by the authors to compute minimal telescopers for rational functions in two discrete variables. We will also discuss its extension to the q-rational case.

$$- - -- \circ - - -- \circ - - -- \circ - - -- \circ - - --$$

A new bijection between RNA secondary structures and plane trees and its consequences

* 陈小锋 (合肥工业大学)

In this paper, we first present a new bijection between RNA secondary structures and plane trees. Combined with the Schmitt-Waterman bijection between these objects, we then obtain a bijection on plane trees that relates the horizontal fiber decomposition associated to internal vertices to the degrees of odd-level vertices while the vertical path decomposition associated to leaves is related to the degrees of even-level vertices. To the best of our knowledge, only the former relation (i.e., horizontal vs odd-level) due to Deutsch is known. As a consequence, we obtain enumeration results for various classes of plane trees, e.g., refining the Narayana numbers and the enumeration involving young leaves due to Chen, Deutsch and Elizalde, and counting a newly introduced 'vertical' version of k-ary trees.

————○————○————○————○————

Non-linear Hamilton cycles in linear quasi-random hypergraphs

* 舒希超 (山东大学)　韩杰 (University of Rhode Island)　王光辉 (山东大学)

In this paper we show that for $\ell < k$ satisfying $(k - \ell) \nmid k$, (p, μ)-denseness plus a minimum $(\ell + 1)$-vertex-degree $\alpha n^{k-\ell-1}$ guarantees Hamilton ℓ-cycles, but requiring a minimum ℓ-vertex-degree $\Omega(n^{k-\ell})$ instead is not sufficient. This answers a question of Lenz–Mubayi–Mycroft and characterizes the triples (k, ℓ, d) such that degenerate choices of p and α force ℓ-Hamiltonicity. We actually prove a general result on ℓ-Hamiltonicity in quasi-random k-graphs, assuming a minimum vertex degree and essentially that every two ℓ-sets can be connected by a constant length ℓ-path. This result reduces the ℓ-Hamiltonicity problem to the study of the connection property.

————○————○————○————○————

稀疏三角分解在生物动力系统平衡点计算中的应用

* 巨雯雯 (北京航空航天大学)　牟晨琪 (北京航空航天大学)

生物动力系统通常以微分方程的形式描述系统中的反应变化, 变元规模通常很大且相互关系很稀疏. 无误差的符号计算方法和图论中的若干工具可分别用于研究微分生物系统的动态行为和稀疏性. 本文主要研究生物动力系统的变元稀疏度并利用稀疏三角分解计算此类系统的平衡点, 是之前文章成果的总结. 本文的主要贡献包括: (1) 分析了生物动力系统中多项式系统的关联图在弦完备化前后的变元稀疏性, (2) 利用稀疏三角分解算法计算了生物动力系统的平衡点, (3) 基于实验结果给出了生物动力系统弦完备化的推荐算法, 并证实了稀疏三角分解算法较普通算法在平衡点求解问题上更为有效.

————○————○————○————○————

On sequences associated to the invariant theory of rank two simple Lie algebras

Bostan Alin (Inria, Universite Paris-Saclay)   Tirrell Jordan (Department of Mathematics and Computer Science, Washington College, USA)   Westbury Bruce (Department of Mathematical Sciences, The Unversity of Texas at Dallas, USA)   * Zhang Yi (Department of Applied Mathematics, School of Science, Xi'an Jiaotong-Liverpool University, China)

以下是短摘要，长摘要见附件。

We study two families of sequences, listed in the On-Line Encyclopedia of Integer Sequences, which are associated to invariant theory of Lie algebras. For the first family, we prove combinatorially that the sequences A059710 and A108307 are related by a binomial transform. Based on this, we present two independent proofs of a recurrence equation for A059710, which was conjectured by Mihailovs. Besides, we also give a direct proof of Mihailovs' conjecture by the method of algebraic residues. As a consequence, closed formulae for the generating function of sequence A059710 are obtained in terms of classical Gaussian hypergeometric functions. Moreover, we show that sequences in the second family are also related by binomial transforms.

$$— — —— \circ — — —— \circ — — —— \circ — — —— \circ — — ——$$

Integer colorings with forbidden rainbow sums

* 周文玲 (山东大学)

For a set of positive integers $A \subseteq [n]$, an r-coloring of A is rainbow sum-free if it contains no rainbow Schur triple. In this paper we initiate the study of the rainbow Erdős-Rothchild problem in the context of sum-free sets, which asks for the subsets of $[n]$ with the maximum number of rainbow sum-free r-colorings. We show that for $r = 3$, the interval $[n]$ is optimal, while for $r \geq 8$, the set $[\lfloor n/2 \rfloor, n]$ is optimal. We also prove a stability theorem for $r \geq 4$. The proofs rely on the hypergraph container method, and some ad-hoc stability analysis.

$$— — —— \circ — — —— \circ — — —— \circ — — —— \circ — — ——$$

高维多项式微分系统 Zero-Hopf 分岔分析及算法推导

* 黄博 (北京航空航天大学)   韩德仁 (北京航空航天大学)

本文针对高维多项式微分系统的 Zero-Hopf 分岔进行分析. 首先, 我们将分岔分析问题约化为代数问题, 并基于半代数系统求解的符号算法给出微分系统存在 Zero-Hopf 分岔点的判定方法. 然后, 基于二阶平均方法推导出微分系统 Zero-Hopf 分岔分析的算法框架, 并利用符号计算方法通过具体算例开展极限环分岔研究. 最后提出几个相关的研究问题.

— — —— ∘ — — —— ∘ — — —— ∘ — — —— ∘ — — ——

[P000043]

Properly colored cycles in edge-colored complete graphs containing no monochromatic triangles: a vertex-pancyclic analogous result

* 李若楠 (西北工业大学)

A properly colored cycle (path) in an edge-colored graph is a cycle (path) with consecutive edges assigned distinct colors. A monochromatic triangle is a cycle of length 3 with the edges assigned a same color. It is known that every edge-colored complete graph without containing monochromatic triangles always contains a properly colored Hamilton path. In this paper, we investigate the existence of properly colored cycles in edge-colored complete graphs when monochromatic triangles are forbidden. We obtain a vertex-pancyclic analogous result combined with a characterization of all the exceptions.

— — —— ∘ — — —— ∘ — — —— ∘ — — —— ∘ — — ——

[P000045]

Factors in randomly perturbed hypergraphs

* Chang Yulin (Shandong University)   Han Jie (University of Rhode Island)   Kohayakawa Yoshiharu (Universidade de Sao Paulo)   Morris Patrick (Freie Universitat Berlin and Berlin Mathematical School)   Mota Guilherme Oliveira (Universidade de Sao Paulo)

We determine, up to a multiplicative constant, the optimal number of random edges that need to be added to a k-graph H with minimum vertex degree $\Omega(n^{k-1})$ to ensure an F-factor with high probability, for any F that belongs to a certain class $\mathcal{F}$ of k-graphs, which includes, e.g., all k-partite k-graphs, $K_4^{(3)-}$ and the Fano plane. In particular, taking F to be a single edge, this settles a problem of Krivelevich, Kwan and Sudakov [Combin. Probab. Comput. 25 (2016), 909-927]. We also address the case in which the host graph H is not dense, indicating that starting from certain such H is essentially the same as starting from an empty graph (namely, the purely random model). This is a joint work with Jie Han, Yoshiharu Kohayakawa, Patrick Morris and Guilherme Oliveira Mota.

— — —— ∘ — — —— ∘ — — —— ∘ — — —— ∘ — — ——

[P000046]

Efficient Algorithms for Determining Constant Residues

* 高艺漫 (中国科学院数学与系统科学研究院)　郭婧 (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)

In this extended abstract, we describe a modular algorithm for determining whether all the residues of a t-simple function are constant, and an algorithm for solving a parametric problem related to constant residues. Both of them help us develop efficient algorithms for integrating functions within elementary extensions via additive decompositions.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

[P000047]

Evolutionary behavior and novel collision of abundant wave solutions to a novel KP-like equation

* Feng Yueyang (Inner Mongolia University of Technology)　Bilige Sudao (Inner Mongolia University of Technology)　Wenbo Ma (Inner Mongolia University of Technology)　Leilei Cui (Inner Mongolia University of Technology)

In the present paper, various wave solutions of a novel KP-like equation were successfully derived, on the basis of Hirota bilinear method. First, multi-breather wave solutions including one-brather wave, two-breather wave, three-breather wave and hybrid solutions between breather waves and solitary waves have been constructed with their dynamic characters and physical structure via choosing the complex conjugate parameter values. Next, by combining the long wave limit method and choosing the complex conjugate parameter values in term of multi-kink solutions, multi-lump wave solutions including one-lump wave, two-lump wave and three-lump wave and two types of hybrid solutions between lump waves and solitary waves have been obtained. Additionally, the one-breather wave and one-lump wave have been studied in detail. Finally, several groups of images exhibited their trajectories and the fusion and fission process with physical interpretion via symbolic computation. Furthermore, the obtained results have immensely enriched the exact solutions of a novel KP-like equation on the available literature and enabled us to understand the nonlinear dynamic system deeply.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

On the probability of generating a primitive matrix

* Chen Jingwei (CIGIT, CAS)   Feng Yong (CIGIT, CAS)   Liu Yang (Chongqing Jiaotong University)   Wu Wenyuan (CIGIT, CAS)

Given a $k \times n$ integer *primitive* matrix A (i.e., a matrix can be extended to an $n \times n$ unimodular matrix over the integers) with size of entries bounded by λ, we study the probability that the $m \times n$ matrix extended from A by choosing other $m - k$ vectors uniformly at random from $\{0, 1, \cdots, \lambda - 1\}$ is still primitive. We present a complete and rigorous proof that the probability is at least a constant for the case of $m \leq n - 4$. Previously, only the limit case for $\lambda \to \infty$ with $k = 0$ was analysed in Maze *et al.* (2011), known as the natural density. Based on extensive computer simulations, we conjecture that a similar result holds as well for $n - 4 < m \leq n - 1$. If the conjecture is true, then there exists a Las Vegas algorithm that completes a $k \times n$ primitive matrix to an $n \times n$ unimodular matrix and runs in expected $\tilde{O}(n^\omega \log \|A\|)$ bit operations, where $\tilde{O}$ is big-O but without log factors, ω is the exponent on the arithmetic operations of matrix multiplication and $\|A\|$ is the maximal absolute value of entries of A.

— — —◦ — — —◦ — — —◦ — — —◦ — — —

Largest family without a pair of posets on consecutive levels of the Boolean lattice

* 肖继孟 (西北工业大学)

Let Y_k be the poset with elements $x_1, x_2, y_1, y_2, \ldots, y_{k-1}$ such that $y_1 < y_2 < \cdots < y_{k-1} < x_1, x_2$ and let Y_k' be the same poset but all relations reversed. We say that a family of subsets of $[n]$ contains a copy of Y_k on consecutive levels if it contains $k+1$ subsets $F_1, F_2, G_1, G_2, \ldots, G_{k-1}$ such that $G_1 \subset G_2 \subset \cdots \subset G_{k-1} \subset F_1, F_2$ and $|F_1| = |F_2| = |G_{k-1}| + 1 = |G_{k-2}| + 2 = \cdots = |G_1| + k - 1$. If both Y_k and Y_k' on consecutive levels are forbidden, the size of the largest such family is denoted by $\mathrm{La_c}(n, Y_k, Y_k')$. In this talk, we will determine the exact value of $\mathrm{La_c}(n, Y_k, Y_k')$.

— — —◦ — — —◦ — — —◦ — — —◦ — — —

基于 MLWE 低膨胀率的同态加密方案的隐私预测服务框架

* 白亚男 (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)

　　随着数据的大量涌入，在丰富的计算资源和先进算法的推动下，深度学习在解决许多复杂任务方面表现出了强大的能力，在医学诊断，风险评估和预警，面部识别等多个领域中有着广泛的应用。为了减轻使用模型的成本，云服务商（例如，亚马逊，谷歌，阿里巴巴）提供机器学习即服务（MLaaS），为用户提供模型训练和预测的 API。但是，这样的服务中存在隐私保护的问题：输入和分析结果被公开给云服务器，侵犯了敏感用户数据的隐私。以基于 IoT 的智能 eHealthcare 设备为例，用户使用智能穿戴设备（例如智能手表）将其身体图片或医用数据（例如心率，血压，体温等）上传到云医疗（例如由 Google 或 Microsoft 提供）的 API，希望了解自己的健康状况。服务器接收到用户的数据后，通过自带的深度学习模型做出决策，并将结果发送给用户。在这个场景下，深度学习的隐私预测需要完成两个安全目标：（1）用户的输入信息、中间计算结果和决策结果不应透露给服务器。（2）服务器的专有深度学习模型属于智力财产，不应泄露给用户。多种解决框架可用于解决上述问题，但都存在着通信开销大的缺点，假设以 46mm 的华为手表 GT 为智能终端设备，设备和边缘服务器使用 WiFi（802.11）通信，上传和下载数据速率为 16.2Mbps，手表的电池总容量为 420mAh，接收和发送数据的每秒耗电量是 0.347A[8]。在理想情况下，即手表电量全部用来完成隐私预测任务，使用 Gazelle 和 FALCON 框架只能支持查询 126 次。我们提出了 LeHE4SCNN，采用一种基于 MLWE 困难问题的低膨胀率的同态加密方案 LeHE，此方案与基于 RLWE 的同态加密方案相比，由于采用较小的参数设置即可达到较高的安全级别，因此加解密效率高，密文膨胀率低，且密文膨胀率独立于安全级别。针对卷积运算的特点——参与求内积计算的向量维数与明文多项式的次数相比较小，设计了新的输入打包和输出解包的方法，提高了同态计算的效率，并进一步降低了密文膨胀。CNN 的线性部分计算采用 LeHE 方案直接导致了较低的通信开销，非线性部分使用数据隐藏中的数据混乱技术，将密文顺序重排后发给用户，用户解密后分辨不出输入和输出的对应关系，无法得到模型的参数。我们采用实际的卷积神经网络和手写数据集 MNIST 实现了 LeHE4SCNN。在相同的实验环境和参数设置下，所提框架的通信开销为 12.39MB，与最新的框架 Gazelle 和 FALCON 需要 70MB 相比降低了 6 倍。在上述场景中，使用本框架的手表的总电量可供查询 713 次。所提的框架以用户能容忍的时间范围内，以低能耗、低成本、高精度完成隐私预测任务，具有广泛的行业应用前景。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

逼近误差有界的重新网格化

* 傅孝明 (中国科学技术大学)

　　重新网格化是计算机图形学与计算机辅助设计中的一个基础问题。为了控制输入与输出形状之间的相似性，它们之间的逼近误差被显式地控制。除了逼近误差有界的约束外，还期望更低的网格复杂度和更高的网格质量。但是，这些约束是相互矛盾的，需要插入更多的点来控制误差，而低复杂度要求点数尽量少。本报告将讨论满足这三个约束的重新网格化算法，并应用到三个问题中：相容性网格生成、高阶网格生成、模板三角化。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

Isogeometric Analysis-based Topological Optimisation for Heterogeneous Parametric Porous Structures

* 胡传丰 (浙江大学) 胡慧 (浙江大学) 蔺宏伟 (浙江大学)

Porous structures widely exist in nature and artifacts, which can be exploited to reduce structural weight and material usage or improve damage tolerance and energy absorption. In this study, we develop an approach to design optimised porous structures with Triply Periodic Minimal Surfaces (TPMSs) in the framework of isogeometric analysis (IGA)-based topological optimisation. In the developed method, the designed porous structures can achieve the optimal mechanical performance by controlling the density distribution under a fixed weight constraint. Firstly, the implicit functions of the TPMSs are adopted to design several types of porous elements with different densities. Secondly, an equivalent method is proposed to calculate the equivalent elastic modulus of porous elements on the basis of Energy Conservation Law. Subsequently, the functional relationships of different porous elements between the equivalent elastic modulus and the relative density are constructed. Thirdly, given the design domain represented by a trivariate B-spline solid, boundary conditions and the type of porous material, we can obtain an optimal density distribution from the IGA-based porous topological optimisation to minimise the compliance. Finally, an optimum porous structure is generated in the B-spline solid with TPMS on the basis of the optimised density distribution. Experimental results demonstrate the effectiveness and efficiency of the proposed method.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Curvature-based r-adaptive isogeometric analysis with injectivity-preserving multi-sided domain parameterization

* 纪野 (大连理工大学数学科学学院) 王梦云 (大连理工大学数学科学学院) 于滢滢 (大连理工大学数学科学学院) 朱春钢 (大连理工大学数学科学学院)

Inspired by the r-refinement method in isogeometric analysis, in this paper, we propose a curvature-based r-adaptive isogeometric method for planar multi-sided computational domains parameterized by toric surface patches. We construct three absolute curvature metrics of isogeometric solution surface to characterize its gradient information, which is more straightforward and effective. The proposed method takes the internal weights as optimization variables and the resulting parameterization is analysis-suitable and injectivity-preserving with a theoretical guarantee. Several PDEs are solved over multi-sided computational domains parameterized by toric surface patches to demonstrate the effectiveness and efficiency of the proposed method.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Interactive Design of cubic IPH spline curves with Control Polygon

* Zhang Jingjing (*安徽大学*)

Indirect Pythagorean hodographs (IPH) spline curves are a set of curves which have rational pythagorean hodographs after reparameterization by a fractional quadratic transformation. In this paper, we provide an algorithm to interactively design a cubic IPH spline curve from any given control polygon. The method has the same friendly interface and properties as those for B-splines and meanwhile facilitates intuitive and efficient construction of open and closed PH spline curves. The key idea is to solve the ratios of a set of auxiliary points associated with the edges and then construct a piecewise cubic IPH spline curve which has as higher as possible continuity, i.e., the absolute curvature value of the adjacent curve segments are same. A very interesting observation is that for any open control polygon, a quadratic B-spline curve can have continuity absolute curvature by carefully choosing the knots as the function of the control points.

———— ○ ———— ○ ———— ○ ———— ○ ————

双变元 Bernstein 展开的逆问题

徐嘉 (*西南民族大学数学学院*)   *姚勇 (*中科院成都计算机应用研究所*)

熟知多项式 $f \in \mathbb{R}[x_1, \cdots, x_n]$ 在盒子 $B \subset \mathbb{R}^n$ (盒子指区间的直积) 上可以用 Bernstein 基展开. 如果展开式的系数 (称为 Bernstein 系数) 都是非负的, 则多项式 f 在盒子 B 上取非负值. 这提供了证明多项式正性的一个方法. 但是上述结论的逆命题是不对的. 作为部分反方向的结论我们熟知, 如果 f 在盒子 $B \subset \mathbb{R}^n$ 上是严格正的, 则总可以通过剖分 B 到充分小的子盒子 $B_1, \cdots, B_s$, 使得 f 在每一个子盒子上的 Bernstein 系数都是非负的. 但是当 '严格正' 用 '非负' 替换之后, 问题变得困难. 本文研究了二元多项式在单位正方形 $I_2 = [0,1] \times [0,1]$ 上的相关问题. 我们找到了存在剖分 $\mathfrak{S}$, 使得 f 在每一个子盒子 $B_i \in \mathfrak{S}$ 上的 Bernstein 系数都是非负的充分必要条件.

———— ○ ———— ○ ———— ○ ———— ○ ————

Computing Strong Regular Characteristic Pairs with Groebner Bases

* 董日娜 (中国科学院重庆绿色智能技术研究院)

The W-characteristic set of a polynomial ideal is the minimal triangular set contained in the reduced lexicographical Groebner basis of the ideal. A pair (G, C) of polynomial sets is a strong regular characteristic pair if G is a reduced lexicographical Groebner basis, C is the W-characteristic set of the ideal $< G >$, the saturated ideal $sat(C)$ of C is equal to $< G >$, and C is regular. In this talk, we show that for any polynomial ideal I with given generators one can either detect that I is unit, or construct a strong regular characteristic pair (G, C) by computing Groebner bases such that $I \subseteq sat(C) = < G >$ and $sat(C)$ divides I, so the ideal I can be split into the saturated ideal $sat(C)$ and the quotient ideal $I : sat(C)$. Based on this strategy of splitting by means of quotient and ideal computations, a simple algorithm is presented to decompose an arbitrary polynomial set F into finitely many strong regular characteristic pairs, from which two representations for the zeros of F are obtained: one in terms of strong regular Groebner bases and the other in terms of regular triangular sets.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Attention-Based DenseNet for Pneumonia Classification

* 王凯 (合肥工业大学数学学院)　江平 (合肥工业大学数学学院)　蒋鑫宇 (合肥工业大学数学学院)
孟婧 (合肥工业大学数学学院)

Early detection and classification of pneumonia are helpful to reduce mortality. As the current algorithms are not particularly effective in pneumonia classification, and DenseNet has the advantages of solving gradient disappearance, reducing model parameters, and feature reusing in the deep networks, this paper proposes a method based on DenseNet to classify pneumonia in chest X-ray images. For highlighting the pneumonia information in the feature map, a feature channel attention block Squeeze and Excitation (SE) is added to DenseNet. To further focus on the lesion region, we replace the average pooling of the third transition layer in DenseNet with max-pooling. By comparing several activation functions, we choose PReLU to avoid neuron death in the process of model training ultimately. Moreover, we preprocess the chest X-ray2017 dataset with data augmentation and normalization. Experiments show that our model's Accuracy, Precision, Recall and F1-score can reach 92.8

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

$Y_{k,b}$ -tiling and Hamilton ℓ -cycles in k-uniform hypergraphs

* 孙琳 (山东大学)

In this lecture, I will give an edge condition for the existence of a $Y_{k,b}$-tiling with a fixed size which leads to some new results on d-degree Hamilton ℓ-cycle problem. For all $k \geq 3$, $1 \leq \ell < k/2$ and $\max\{k-\ell, \ell+1\} \leq d \leq k-1$, I will give an asymptotic bound on the minimum d-degree for the existence of Hamilton ℓ -cycles in k-graphs, where $k - \ell$ divides n. This asymptotic bound is the best possible for some cases.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

RAINBOW SPANNING STRUCTURES IN GRAPH AND HYPERGRAPH 2 SYSTEMS

程杨杨 (山东大学)   韩杰 (罗德岛大学)   * 王斌 (山东大学)   王光辉 (山东大学)

We study the following rainbow version of subgraph containment problems in a family of (hyper)graphs, which generalizes the classical subgraph containment problems in a single host graph. For a collection $\boldsymbol{G} = \{G_1, G_2, \ldots, G_m\}$ of not necessarily distinct graphs on the same vertex set $[n]$, a (sub)graph H on $[n]$ is rainbow if $E(H) \subseteq \bigcup_{i \in [m]} E(G_i)$ and $|E(H) \cap E(G_i)| \leq 1$ for $i \in [m]$. Note that if $|E(H)| = m$, then a rainbow H consists of exactly one edge from each G_i.

Our main results are on rainbow clique-factors in (hyper)graph systems with minimum degree conditions on each individual graph. In particular,

1. we obtain a rainbow analogue of an asymptotical version of the Hajnal–Szemerédi theorem, namely, if $t \mid n$ and $\delta(G_i) \geq (1 - \frac{1}{t} + \varepsilon)n$ for each $i \in [\frac{n}{t}\binom{t}{2}]$, then $\boldsymbol{G}$ contains a rainbow K_t-factor;

2. we prove that for $1 \leq d \leq k-1$, essentially a minimum d-degree condition forcing a perfect matching in a k-graph also forces rainbow perfect matchings in k-graph systems.

The degree assumptions in both results are asymptotically best possible (although the minimum d-degree condition forcing a perfect matching in a k-graph is unknown in general). For (1) we also discuss directed versions, a multipartite version, and a hypergraph extension. Finally, to establish these results, we in fact provide a general framework to attack this type of problems, which reduces it to subproblems with *finitely many* colors.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Isogeometric analysis with error-based local adaptivity for structural vibration

* Yu Peng (Guangxi University)

This paper presents a new adaptive isogeometric method for structural vibration. Based on the newly introduced Geometry-Independent Field approximaTion (GIFT), generalized from Iso-Geometric Analysis (IGA), we exactly describe the geometry of the structure with NURBS (Non-Uniform Rational B-Splines), and independently employ PHT-splines (Polynomial splines over Hierarchical T-meshes) to achieve local refinement in the solution field. To deal with error estimation, we improve the MAC (Modal Assurance Criterion) method to locate unique, as well as multiple, modal correspondence between different meshes. Local adaptivity is carried out by sweeping modes from low to high frequency. Numerical examples show that a proper choice of the spline space in solution field (with GIFT) can deliver better accuracy than using NURBS solution field. In addition, for vibration of Reissner-Mindlin plates, our proposed method indicates that the adaptive local $h-$refinement achieves a better solution accuracy than the uniform h-refinement.

$$- - - - \circ - - - - - \circ - - - - - \circ - - - - - \circ - - - - -$$

预知分母可能因子的有理函数恢复算法

肖丽霞 (吉林大学)　* 夏朋 (辽宁大学)

令 $\mathbb{Z}$ 为整数环. 本文考虑预知分母可能因子的有理函数恢复问题: 假设待恢复的有理函数 $R(U) = \frac{P(U)}{Q(U)} \in \mathbb{Z}[U]$, 并且假定

(1) 对于任意选定的节点 U_i, 与之相应的有理函数值 $R(U_i)$ 容易计算;

(2) 已知分母 $Q(X)$ 的所有可能因子 $D_i(U), i = 1, \ldots, m$, 即

$$Q(U) = CD_1^{d_1} D_2^{d_2} \cdots D_m^{d_m},$$

其中 $0 \le d_1, d_2, \ldots, d_m$ 为未知的待定正整数, $C \in \mathbb{Z}$ 为待定系数, $P(U)$ 为未知多项式.

关心此类问题的原因是: 在正维多项式系统解的有理表示算法中, 令 U 为变元集 X 的极大无关变元集, $V = X/U$, I^e 是正维理想 I 在 $K(U)[V]$ 上的扩张理想, 解决 I^e 的解的有理表示集是求解正维理想 I 的有理表示的关键步骤. I^e 是 $K(U)[V]$ 上的零维理想, 理论上, 对 I^e 直接使用 Rouillier 建立的 RUR 算法, 可得其在有理函数域 $K(U)$ 中的有理表示 (RUR), 但由于在有理函数域 $K(U)$ 中运算, 计算代价非常大. 若先选择适当的节点 U_i, 即可得到零维理想 $I_{U_i} \subset K[V]$, 在一定条件下, I_{U_i} 的 RUR 中的系数等于 I^e 的 RUR 系数 $R_k(U) \in K(U)$ 在 U_i 点的赋值, 故有理函数值 $R_k(U_i)$ 已知. 于是可以通过数据 $\{U_i, R_k(U_i)\}$ 将 RUR 中的有理系数 $R(U)$ 恢复出来, 从而获得 I^e 在 $K(U)[V]$ 中的有理表示. 又因为谭畅、张树功已经证明这种 RUR 中所有多项式的系数的分母的最小公倍式的无平方部分整除某一已知多项式 F, 其中 F 为 I^e 的 Groebner 基的领项系数的最小公倍式. 由于 I^e 的 Groebner 基已知, 故 F 已知. 这表明以正维多项式系统解的有理表示为研究背景, 预知分母可能因子的有理函数恢复问题的 2 个基本假设是合理的.

对于这种有理函数恢复问题, 若这些 d_i 得以确定, 则该问题转化为多项式恢复问题, 利用多项式插值算法即可将有理函数恢复出来. 下面分析确定 d_i 的恢复方法.

选择适当的 U_i, 使得 $D_j(U_i)$ 与 $D_k(U_i)$ 互相不能整除, 因为

$$R(U_i) = \frac{M_i}{N_i} = \frac{P(U_i)}{Q(U_i)} = \frac{P(U_i)}{CD_1(U_i)^{d_1} D_2(U_i)^{d_2} \cdots D_m(U_i)^{d_m}},$$

由于 $P(U_i)$ 和 $Q(U_i)$ 可能存在公因子, $N_i \le Q(U_i)$, 所以将 N_i 分解成 $D_1(U_i), D_2(U_i), \ldots, D_m(U_i)$ 乘幂的乘积的形式时

$$N_i = c_i D_1(U_i)^{d_1^{(i)}} D_2(U_i)^{d_2^{(i)}} \cdots D_m(U_i)^{d_m^{(i)}},$$

其各因子的幂次 $d_j^{(i)} \le d_j$. 选择足够多的 U_i, 可得

c_1 , $d_1^{(1)}$, $d_2^{(1)}$, $\cdots$, $d_m^{(1)}$,

c_2 , $d_1^{(2)}$, $d_2^{(2)}$, $\cdots$, $d_m^{(2)}$,

$\vdots$, $\vdots$, $\vdots$, $\vdots$, $\vdots$

取 $d_1 = \max\{d_1^{(i)}\}$, $d_2 = \max\{d_2^{(i)}\}$, ..., $d_m = \max\{d_m^{(i)}\}$, $C = LCM\{c_i : i = 1, \ldots\}$, 则

$$Q(U) = C D_1^{d_1} D_2^{d_2} \cdots D_m^{d_m},$$

至此, 将有理函数恢复问题转化为多项式恢复问题, 即求多项式 $P(U)$, 使得 $P(U_i) = Q(U_i)R(U_i)$, $i = 1, \ldots$.

$$———— \circ ———— \circ ———— \circ ———— \circ ————$$

[P000064]

Nonlinear inverse relations of the Bell polynomials via the Lagrange inversion formula (II)

马欣荣 (苏州大学数学科学学院)　＊王瑾 (浙江师范大学数学与计算机科学学院)

In this paper, by means of the classical Lagrange inversion formula, we establish a general nonlinear inverse relation as the solution to the problem proposed in the paper [J. Wang, Nonlinear inverse relations for the Bell polynomials via the Lagrange inversion formula, J. Integer Seq., Vol. 22 (2019), Article 19.3.8]. As applications of this inverse relation, we not only find a short proof of another nonlinear inverse relation due to Birmajer et al., but also set up a few convolution identities concerning the Mina polynomials.

$$———— \circ ———— \circ ———— \circ ———— \circ ————$$

[P000065]

The log-concavity of Kazhdan-Lusztig polynomials of uniform matroids

＊解红叶 (天津理工大学)　张彪 (天津师范大学)

Elias, Proudfoot, and Wakefield conjectured that the Kazhdan-Lusztig polynomial of any matroid is log-concave. Inspired by a computer proof of Moll's log-concavity conjecture given by Kauers and Paule, we use the computer algebra system to prove the conjecture for arbitrary uniform matroid.

$$———— \circ ———— \circ ———— \circ ———— \circ ————$$

verifying the positivity of a function over a finite set

* 杨剑霆 (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)　支丽红 (中国科学院数学与系统科学研究院)

Given a finite set $S = \{s_0, s_1, s_2, ..., s_{N-1}\}$, we aim to verify that a map f from S to $\mathbb{R}$ is nonnegative, i.e. $f(s) \geq 0$ for each $s \in S$. We propose the following method:

(1) Choose a finite abelian group $G = \{g_0, g_1, g_2, ..., g_{N-1}\}$, define a bijection $\phi : G \mapsto S$, $s_i = \phi(g_i)$ for $0 \leq i \leq N - 1$;

(2) We verify that $f \circ \phi$ is a nonnegative function on G via computing its sparse sum-of-squares representation on abelian group G.

−−−−− ◦ −−−−− ◦ −−−−− ◦ −−−−− ◦ −−−−−

基于 B++ 样条和 Toric 曲面的非连续界面力学问题等几何分析

* 祝雪峰 (大连理工大学)　侯文彬 (大连理工大学)　朱春钢 (大连理工大学)　姜凯 (大连理工大学)
纪野 (大连理工大学)　胡平 (大连理工大学)　Ma Zheng-Dong (Michigan University)

非连续界面力学问题是非常重要一类力学问题，如碳纤维复合材料界面力学问题、材料损伤和断裂、流固耦合等。非连续力学问题中界面物理场函数或其导函数在界面处常不连续，这也是"非连续力学"的由来。如何精确高效求解非连续界面力学问题，特别是在界面处准确计算物理场函数是。在等几何分析中，由于 CAD 模型包含多个剪裁曲面，曲面界面之间几何不连续，导致基于剪裁曲面的场函数也不连续，这是一类特殊的非连续力学问题。此外在某些工程问题中，在不同材料界面处或者流固耦合处需要施加边界条件，然而现有的处理界面问题的仿真算法长无法满足这一要求。

针对上面问题，我们将简要介绍一下近期在非连续力学界面问题仿真方面所做的一些工作：工作 1：针对扩展有限元（XFEM）和扩展等几何分析（XIGA）在多材料界面无法直接施加边界条件问题，发展了 B++ 样条扩展等几何分析方法。该方法允许在界面处施加 Dirichlet 边界条件，解决了困扰 XFEM 和 XIGA 多年的边界条件施加问题。我们将这一方法拓展到三明治复合材料结构的等几何分析，并用于折叠屏手机屏幕的非线性问题的仿真。工作 2：求解断裂问题的 XIGA 或 XFEM 算法中位移场富集项无明确物理含义。此外在断裂界面处无法施加自然边界条件。针对这两个问题，我们发展了求解断裂问题的 B++ 样条扩展等几何分析方法。工作 3：针对剪裁曲面边界处几何不连续引起等几何分析场函数不连续的问题，我们和朱春刚教授团队合作发展了基于 Toric surface 的多片剪裁曲面等几何分析方法，并将之用于冲压成形仿真。

−−−−− ◦ −−−−− ◦ −−−−− ◦ −−−−− ◦ −−−−−

Smith form of triangular multivariate polynomial matrix

Liu Jinwang (湖南科技大学)   * Li Dongmei (湖南科技大学)   wu Tao (湖南科技大学)

The Smith form of a matrix plays an important role in the equivalence of matrices. We know that some multivariate polynomial matrices are not equivalent to their Smith forms. In this paper, we investigate mainly the Smith forms of triangular multivariate polynomial matrices and testify two classes upper triangular multivariate polynomial matrices are equivalent to their Smith forms respectively.

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

基于 Isabelle/HOL 程序规范的 C++ 代码生成

蒋东辰 (北京林业大学信息学院)   * 许博 (北京林业大学信息学院)

本文研究从 Isabelle 函数式规范到 C++ 代码的生成方法。Isabelle/HOL 支持函数式编程并提供交互式验证方法，可实现函数式程序的验证开发。但这与工业界广泛使用的 C++ 语言存在差异。本文将从类型转换和函数生成两个方面探讨从 Isabelle 函数式规范到 C++ 代码的转换方法。该工作完成了 Isabelle 预定义类型到 C++ 类型的映射，支持扩展自定义类型，能够将已被验证的函数规范转换自动转换为与其操作语义等价的 C++ 代码，实现 C++ 代码的可靠生成。

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

Autotuning the Performance of Matrix Multiplication and Convolution for Deep Learning on CPU

* 陈长波 (中国科学院重庆绿色智能技术研究院)   池昊宇 (中国科学院重庆绿色智能技术研究院)

Deep learning (DL) compilers have emerged with the aim of closing the gap between abundant, fast-growing DL models and the lag of high performance implementations of these models on diverse hardware devices. In this work, we introduce several strategies and integrate them into a unified autotuning framework, called AutoMCL, to improve the performance of DL compilers by combining human's expertise with machine's learned intelligence. The preliminary experiments conducted on different CPU platforms show that the proposed framework brings an average $29.07\times$ speedup compared to TensorFlow and an average $1.55\times$ speedup while consuming only $0.47\times$ optimization time compared to a state-of-art DL compiler AutoTVM for fully connected neural networks on an Intel CPU, and an average $1.36\times$ speedup compared to TensorFlow and an average $1.09\times$ speedup with similar compilation time compared to AutoTVM for several well-known convolutional neural networks on multiple CPUs.

— — — — ◦ — — — — ◦ — — — — ◦ — — — — ◦ — — — —

Sparse Interpolation With Errors in Chebyshev Basis Beyond Redundant-Block Decoding

Kaltofen Erich (North Carolina State University, Duke University)   * Zhi-Hong Yang (Shenzhen University)

We present sparse interpolation algorithms for recovering a polynomial with $\leq B$ terms from N evaluations at distinct values for the variable when $\leq E$ of the evaluations can be erroneous. Our algorithms perform exact arithmetic in the field of scalars K and the terms can be standard powers of the variable or Chebyshev polynomials, in which case the characteristic of K is $\neq 2$. Our algorithms return a list of valid sparse interpolants for the N support points and run in polynomial-time. For standard power basis our algorithms sample at $N = \lfloor \frac{4}{3}E + 2 \rfloor B$ points, which are fewer points than $N = 2(E+1)B - 1$ given by Kaltofen and Pernet in 2014. For Chebyshev basis our algorithms sample at $N = \lfloor \frac{3}{2}E + 2 \rfloor B$ points, which are also fewer than the number of points required by the algorithm given by Arnold and Kaltofen in 2015, which has $N = 74 \lfloor \frac{E}{13} + 1 \rfloor$ for $B = 3$ and $E \geq 222$. Our method shows how to correct 2 errors in a block of $4B$ points for standard basis and how to correct 1 error in a block of $3B$ points for Chebyshev Basis.

$- - -- \circ - - -- \circ - - -- \circ - - -- \circ - - --$

The balanced edge cover decompositions of graphs

* Yu Minghui (Shandong Normal University)   Zhang Xia (Shandong Normal University)

For a graph $G = (V, E)$, a subset M of E is called an edge cover of G if M contains at least one incident edge of v for each $v \in V$. Let $cd(G)$ be the maximum number of disjoint edge covers in G. It is well known that every simple graph G has $\delta(G) - 1 \leq cd(G) \leq \delta(G)$, where $\delta(G)$ is the minimum degree of G. The problem to determine whether a simple graph G has $cd(G) = \delta(G)$ or not is NP-complete. In this paper, we consider balanced edge cover decompositions. For an integer $k \geq 2$, define that $V_k = \{v \in V : k | d(v)\}$. We show that if $G[V_k]$ is a union of disjoint unicycle graphs or forest, then G has a k-edge cover decomposition $E = \cup_{i=1}^{k} E_i$ such that E_i contains at least $\left\lfloor \frac{d(v)}{k} \right\rfloor$ incident edges of v for each $v \in V$ and each $i \in \{1, 2, \ldots, k\}$, with only exception that $G[V_k]$ is a union of disjoint cycles and each vertex $v \in V \setminus V_k$ has $d(v) = 1 \pmod{k}$ and $v \in N(V_k)$. This extends the previous results on $G[V_k]$ being a forest or G being peelable.

Joint work with Xia Zhang.

$- - -- \circ - - -- \circ - - -- \circ - - -- \circ - - --$

Minimal Representation of a polyhedron and its projections

* 荆瑞娟 (江苏大学)

In this paper, we propose a new method to give a minimal representation of a polyhedron and its projections. This method does not require the polyhedron to be full-dimensional, pointed or non-empty. It can detect the implicit equations of a polyhedron, if there was, and remove all the redundant inequalities in the representation of this polyhedron and its projections. Moreover, it can detect the emptiness of a polyhedron.

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

有限集上偏序关系的符号计算

* 张升荣 (电子科技大学数学科学学院)　资俊伟 (电子科技大学数学科学学院)　骆孟煜 (电子科技大学数学科学学院)　李永彬 (电子科技大学数学科学学院)

不同于序理论和拓扑理论中关于偏序关系和 T_0 拓扑的研究思路，本文给出一种通过解有限域 $\mathbb{F}_2$ 上多项式方程组求有限集 $[n]$ 上所有偏序关系和 T_0 拓扑的方法，并通过实例说明了方程组零点和偏序以及 T_0 拓扑的对应关系。运用 Gröbner 基理论，得到一种求有限集 $[n]$ 上偏序个数和 T_0 拓扑个数的符号计算方法，并给出 Maple 程序。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

整数分拆的符号计算初探

* 李永彬 (电子科技大学)

整数分拆是一个古老有趣的课题。本报告旨在汇报，作者在整数分拆的符号计算的初步尝试。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

基于 MLWE 的多密钥同态方案

* 代小康 (中科院重庆研究院)   吴文渊 (中科院重庆研究院)   冯勇 (中科院重庆研究院)

传统的全同态加密仅允许对使用单个密钥加密的数据进行计算，很好的解决了外包运算中的安全问题。当有多个数据提供方需要合作完成一些计算任务时，单密钥的同态方案需要在加密前协商共同的密钥，以保证运算能顺利进行 [1]。当参与方较多时，多方的密钥协商会带来较高的通信复杂度，如果能容忍较高的通信复杂度，那么传统的安全多方计算协议就能很好的解决问题。为了将同态加密引入到多方计算场景，Lopez-Alt, Tromer 和 Vaikuntanathan(LTV)[2] 提出了多密钥全同态加密的概念，多密钥全同态加密允许对在不同密钥下加密的密文进行同态计算，并提出一个基于 NTRU[3] 的多密钥同态方案。LTV[2] 基于 NTRU 加密系统构造了一个多密钥全同态方案，该方案的安全性基于多项式环上的非标准假设，不像 learning with error(LWE) 或者 ring variant(RLWE)，该假设没有 worst case to average case 的安全性规约。文献 [2] 同时构造了一个基于 RLWE 的多密钥同态方案，但是该方案只支持对数级别的密钥和电路深度。之后 Clear 和 McGoldrick[4] 基于 LWE，构造了一个 Gentry, Sahai 和 Waters(GSW)[5] 类型的多密钥同态方案，该方案支持任意多个密钥。随后 Mukherjee 和 Wichs[6] 对方案 [4] 进行改进，构造了一个两轮的 Multi-Party Computation(MPC) 协议。2016 年 Peikert 和 Shiehian[1], Brakerski 和 Perlman[7] 同时基于 LWE 构造了多密钥同态方案，与之前方案不同的是，方案 [1] 支持参与方的动态加入，方案 [7] 的构造引入 Bootstrapping 来实现密钥转换。2017 年 Chen long[8] 等人构造了 RLWE 类型的多密钥同态方案，该方案利用 R-GSW 方案的多密钥变体解决了密文乘法运算后的再线性化问题。2019 年，Chen hao[9] 等人基于类似的方法将 TFHE 方案改造为多密钥版本，并在 [10] 中提出一个新的方法将 RLWE 类型的同态方案改造为多密钥版本。不像整数格上的 Shortest Independent Vectors problems(SIVP) 问题，理想格上的 SIVP 问题还没有得到很好的研究，其困难性还值得考究 [11]。例如整数格上近似 GapSVP 问题是困难的，但是该问题在理想格上却是容易的。特别是对于次数为 2 的整数幂的多项式环中的理想格，大多数同态方案的困难性依赖该格上的困难问题。同时，由于 2 的整数幂为稀疏的，导致方案的安全强度级别的选取很不平滑。Module learning with error(MLWE) 也称为 general LWE，其困难性可以规约到模格上的某类困难问题，一般认为 MLWE 比 RLWE 更难，能解秩为 3 的 MLWE 问题也就能解 RLWE 问题 [11]，同时，对于不同的安全强度要求，可以选择不同的秩来满足要求，因此安全强度的选取更加平滑。基于 MLWE 构造的 Kyber 加密方案 [12] 也被 NIST 纳入了后量子密码标准。鉴于此，我们构造了第一个 MLWE 类型密文的多密钥方案。类似之前的方案，我们引入 Common reference string model(CRS)，参与方每个人的私钥拼接起来构成新的密钥，和 RLWE 类型的密文一样，MLWE 类型的密文做乘法后密文维度为之前的平方倍，相应的解密密钥为原密钥的张量积，该张量积中包含不同参与方密钥分量的乘积，方案 [8] 中利用了 GSW 类型的多密钥方案来构造分量乘积的密文。我们的主要贡献是提出了一种新的方法构造再线性密钥，简单来讲，我们引入循环安全假设，每个参与方首先在本地生成自己私钥的密文，在同态运算的再线性化操作中，利用私钥的密文和对应的公钥结合得到相应的密钥交叉项在新密钥下的密文，相较于方案 [8]，我们的方案更加高效，随着参与方人数的增长，我们方案的渐进复杂度更优，在安全性方面，我们可以设置 n 和 d 的大小来选取合适的安全强度，因此我们的方案更加灵活。此外，为了控制再线性化导致的噪声增长，我们引入模提升技术 [13, 14] 因此在相同的参数尺寸下，支持更多的乘法运算次数，此外所有针对 RLWE 类型密文的同态方案的优化技术，如明文打包技术 (SIMD)、自举技术（bootstrapping）都与 MLWE 类型的密文兼容。

———— ◦ ———— ◦ ———— ◦ ———— ◦ ————

Lazy Hermite Reduction and Creative Telescoping for Algebraic Functions

Chen Shaoshi (KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences)   * Du Lixin (School of Mathematical Sciences University of Chinese Academy of Sciences)   Kauers Manuel (Institute for Algebra, Johannes Kepler University)

Bronstein's lazy Hermite reduction is a symbolic integration technique that reduces algebraic functions to integrands with only simple poles without the prior computation of an integral basis. We sharpen the lazy Hermite reduction by combining it with the polynomial reduction to solve the decomposition problem of algebraic functions. The sharpened reduction is then used to design a reduction-based telescoping algorithm for algebraic functions in two variables.

— — —◦ — — —◦ — — —◦ — — —◦ — — —

Machine Checked Proof for Some Integral Inequalities

* 方敬轩 (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)

We give some examples of mathematical analysis and check the proof by a program we write in Maple and illustrate its method. The program module we write can automatically apply Cauchy's mean value theorem, triangle inequality, Holder's inequality, Schwartz inequality and Newton-Leibniz formula. Besides, this module can correct some wrong inequalities.

— — —◦ — — —◦ — — —◦ — — —◦ — — —

The subresultant of several univariate polynomials

Hong Hoon (North Carolina State University)   * Yang Jing (Guangxi University for Nationalities)

Subresultant of two univariate polynomials is a fundamental object in computational algebra and geometry. They are naturally defined by an expression in the roots. Sylvester et al. provided expressions for them in terms of coefficients. They are used in numerous applications. In this paper, we generalize the subresultants of two polynomials to arbitrary number of polynomials, resulting in the so-called multi-polynomial subresultants. Specifically,
  1. we propose a definition of multi-polynomial subresultants in terms of roots;
  2. we provide an expression for them in terms of coefficients;
  3. we show some applications:
  - parametric multi-polynomial GCD, and
  - parametric multiplicity.

— — —◦ — — —◦ — — —◦ — — —◦ — — —

[P000081]

An Optimal Quantum Error-Correcting Procedure Using Quantifier Elimination

Xu Ming (East China Normal University)   Deng Yuxin (East China Normal University)   Sun Yingji (East China Normal University)   * Mei Jingyi (East China Normal University)

Quantum communication channels suffer from various noises, which are mathematically modelled by error super-operators. To combat these errors, it is necessary to design recovery super-operators. We aim to construct the optimal recovery that maximizes the minimum fidelity through the noisy channel. It is typically a MAX-MIN problem, out of the scope of convex optimization. Compared to existing methods, our method is exact and complete by a reduction to quantifier elimination over real closed fields in a fragment of two alternative quantifier blocks. Finally, the complexity is shown to be in EXP.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

[P000082]

Salience-Driven Image Mosaic Method by Edge-Weighted Centroidal Voronoi Tessellations

Cui Lingling (Hangzhou Dianzi University)   * Xiang Bingjin (Hangzhou Dianzi University)   Jiang Peng (Hangzhou Dianzi University)   Renshu Gu (Hangzhou Dianzi University)   Jinlan Xu (Hangzhou Dianzi University)   Xu Gang (Hangzhou Dianzi University)

Traditional image mosaic method usually generates the mosaic visual effects for the whole input image. In this paper, we propose a general framework to automatically generate mosaic in the saliency region of the input image for the protection of privacy information. Firstly, a feature-preserving image mosaic method by edge-weighted centroidal voronoi tessellations (EWCVT) is proposed. Secondly, by combining the proposed feature-preserving image mosaic method and the saliency detection method, a salience-driven image mosaic framework is presented. Experimental results show the effectiveness of our algorithm, and the boundary of the mosaic area in the generated mosaic image captures the shape of salient regions. In particular, mosaic tessellations are neatly arranged thanks to edge-weighted centroidal Voronoi tessellation. The proposed framework can be used for the image privacy information protection and artistic applications.

— — —— ◦ — — —— ◦ — — —— ◦ — — —— ◦ — — ——

Ramp schemes based on CRT for polynomial ring over finite field

* Ding JIAN (福建师范大学)   Lin Changlu (福建师范大学)   Wang Huaxiong (Nanyang Technological University, Singapore)

Secret sharing schemes play fundamental roles in many cryptographic applications, and hence they have been constructed by using various mathematical tools. As we all know, the most famous Shamir scheme and Asmuth-Bloom scheme are based on polynomials over finite field and Chinese Reminder Theorem (CRT) for integers, respectively. Compared with Shamir scheme, Asmuth-Bloom scheme has a lower information rate, but it has a lower computational complexity in its secret reconstruction phase. In ASIACRYPT 2018, Ning et al. constructed a perfect (r,n)-threshold scheme based on CRT for polynomial ring over finite field, and the corresponding information rate is one which is the greatest information rate for a (r,n)-threshold scheme. However, perfect security is too much security for many practical purposes. In this work, we generalize the scheme of Ning et al. to a (t,r,n)-ramp scheme based on CRT for polynomial ring over finite field, which has the greatest information rate (r-t) for a (t,r,n)-ramp scheme. Moreover, for any give $r_1 < r_2 \leq n$, we will use our ramp scheme to construct a (r_1, n)-threshold scheme that is threshold changeable to (r',n)-threshold scheme for all $r' \in \{r_1 + 1, \ldots, r_2\}$ in the full version of this paper. We claim that our threshold changeable secret sharing (TCSS) scheme has a higher information rate than other existing TCSS schemes of this type.

$--—— \circ ——— \circ ——— \circ ——— \circ ———$

1884-2016 年香港气候变化特征及其分析

* 孙翔 (上海大学数学系)   曾振柄 (上海大学数学系)

根据香港 1884-2016 年长达百年的气候数据资料，利用 MannKendall 和滑动 t 检验，以及小波变换和交叉小波变换对香港气候进行分析。结果表明，在前半段 1884-1939 年香港年平均最低与最高气温增长速率基本一致，在后半段 1947-2016 年平均最低气温增长速率显著高于年平均最高气温增长速率；气温突变检验表明香港气温在 1958 年发生显著的均值突变；小波变换得到香港气温和降水存在多尺度周期变化，其中气温和降水的第一主周期分别为 52a 和 42a；交叉小波分析显示 ENSO 特征值 Nino3.4、SOI 与气温、降水在全时间段上相关性不显著，但存在局部相关性。关键词：气候变化；突变检测；ENSO；小波

$--—— \circ ——— \circ ——— \circ ——— \circ ———$

Reverse gamma-expansion for Eulerian polynomials

* 赵彤远 (中国石油大学（北京）)

The expansion coefficients of classical Eulerian polynomials $A_n(t)$ are nonnegative by the symmetric basis of $\{t^i(1+t)^{n-2i}\}$, which is called the gamma-nonnegativity proved by Foata-Schzenberger in 1970. In this paper, we investigate the interlacing nonnegativity of the inverse gamma-expansion, that is, the coefficients of $\{(1+t)^n\}$ expanded by the basis of $\{(-t)^i A_{n-2i}(t)\}$ are nonnegative. In addition, we also prove that the coefficients of $\{(1+t)^n\}$ in the inverse gamma-expansion of several famous combinatorial polynomials such as Narayana polynomials are interlacing nonnegativitive. It is an interesting open problem to look for combinatorial interpretations of these coefficients.

$$- - -- \circ - - -- \circ - - -- \circ - - -- \circ - - --$$