科学前沿纵览

2021 年　第 4 期（总第 28 期）

中国科学院数学与系统科学研究院系统科学研究所　　2021 年 4 月 1 日

微分算子的近似最大右公因子

冯如勇

在现代计算机代数系统如 Maple 与 Mathematica 中，计算线性微分算子的最大右公因子是十分重要的。它在线性微分系统的闭形式解、微分伽罗华群的计算以及微分模的形式构造等方面扮演着关键角色。计算最大右公因子的研究可追溯到上个世纪初。 Ore 在 1933 年发展了非交换多项式环上的欧几里得算法，由此可计算线性微分算子的最大右公因子。而更为高效的算法由 Li 与 Nemes 在 1997 年基于微分结式理论以及模算法给出。另一方面，当所考虑的是实数（或者浮点数）上的微分算子时，理解这些算法的数值稳定性在计算中具有重要意义的，同时近似计算拥有比符号计算更为高效的潜在优势。

近期，来自加拿大的 Giesbrecht、Haraldson 与来自美国的 Kaltofen 首次引入了非交换情形近似最大右公因子的概念并给出计算方法，他们利用由 Li 发展的微分子结式理论将问题转为为有理函数系数的线性代数问题，并进一步转化为连续非约束优化问题，他们证明了在合理的假设下近似最大右公因子问题是适定的，通过所给方法求得的数值解是鲁棒的。

这项工作开启了微分算子环上近似计算的研究，所得结果有望推广到更一般的非交换多项式环中。

(Foundations of Computational Mathematics 2020 年 第 20 卷)

基于单项式预测技术的代数次数评估方法

冯秀涛

对一个代数正规型未知的布尔函数，如何高效的评估其代数次数是许多密码分析中的关键技术，例如积分分析、立方分析、高阶差分分析等。2015 年 Todo 等人对积分属性(integral property)一般化，提出了除属性(division property)的概念，并借用混合整数线性规划(MILP)方法，逐步发展出一套探测布尔函数代数结构的强有力的工具。

最近，针对除属性，Hu Kai 等从纯代数视角出发，提出了一种被称之为单项式预测(monomial prediction)的技术。该技术通过计数复合布尔函数的多项式传播迹来确定某个单项式是否在最终的复合布尔函数中出现。 利用该技术，他们证明了当前公开文献中许多关于除属性的算法没有产生错误警报但是可能失效，并进一步给出了单项式预测和基于比特的三子集除属性之间的等价关系。结果表明这两种方法对代数次数评估而言都是精确的。

作为应用，Hu Kai 等人对流密码算法 Trivium 的输出密钥流的代数次数作了精确评估，首次得到了 834 轮以内各输出密钥流的精确代数次数。在 Cube 攻击环境中，利用分别征服思想，他们进一步给出了一些大尺寸 Cube 变元的超级多项式的代数正规型，例如，75 到 78 维的 Cube 变元。利用它们，可以给出针对 840，841 和 842 轮的 Trivium 算法的近似最优的代数攻击。

(ASIACRYPT 2020)

高维最大最小距离设计

何煦

最近，南开大学及 Simon Fraser University 的三位学者提出了一种新的空间填充实验设计方法。

高维度的最大最小距离设计是当前空间填充实验设计的一个热点问题。常用的搜索算法对于高维度的问题通常效果不佳，而理论构造方法需要特殊的数学技巧。新方法通过先生成两个小设计，再将两个设计进行复合来得到大设计。通常第一个小设计可以是一个强度 2 的正交表，第二个小设计可以是一个拉丁超方设计。最终得到的设计是一个 U 设计，即每个维度的每种取值对应的实验次数相等。新方法得到的设计的实验次数与维度的比值一般在 0.5 与 2 之间。比较结果显示，这些设计同时具有很好的 L1 分离距离及 L2 分离距离，一般显著优于已有方法。

新方法是当前最佳的高维度最大最小距离设计方法。

(Biometrika 2021 年)

高斯过程回归中稀疏变分推断的收敛性

牟必强

高斯过程因其编码未知回归函数先验知识的便利性和经验上的成功常用于贝叶斯建模中，其建立的模型可以给出灵活的均值预测以及估计不确定性的度量。当先验分布和似然函数均为高斯分布时，贝叶斯后验存在显示解。此外，在许多情况下，当核函数关于超参数可微，可以用基于梯度的优化方法极大化具有显示目标函数的边际似然（也称为经验贝叶斯或类型 II 似然），有效地学习超参数。然而，高斯过程回归模型的精确推断的存储复杂度为 $O(N^2)$，计算

复杂度为 $O(N^3)$，其中 N 是训练样本的数量。因此，高斯过程回归在存储和计算方面的高昂代价促使研究具有适应于大规模数据集的可扩展近似算法。

稀疏方法依赖于一组诱导变量来近似表示后验分布。尽管稀疏方法已在研究和应用领域中广泛采用，但目前对其近似的后验分布的预测质量以及用近似边际似然的超参数估计引入的偏差还缺乏理论理解。在这项工作中，作者旨在刻画稀疏近似的精确性，得到了以下理论结果：

1）推导了高斯过程模型中变分推理精度的界限。对于平方指数核和高斯或紧支持的输入，证明可以使用 $O((\log N)^D)$的诱导变量，以任意高的概率使变分近似后验逼近真实后验，其中 D 是输入的维数，相应的计算复杂度为 $O(N(\log N)^{2D}(\log\log N)^2)$。

2) 推导的界限度量了近似后验和精确后验之间的 KL 散度，同时也暗示近似后验的均值和方差的逐点收敛。

3）证明了稀疏核岭回归中用于选择回归变量的现有方法的矩阵近似精度的理论保证可以直接转化为变分稀疏高斯回归的理论保证。

4） 推导了确保 KL 散度保持较小所需的诱导变量个数的下界。对于平方指数核和高斯协变量分布，这些下限与数据集的大小与上限具有相同的依赖性。

5） 根据理论结果，提供了如何在实践中选择诱导变量的建议，并说明了从经验上的改进路径。

(JMLR 2021 年)

基于对手模型学习的滚动时域演化算法

穆义芬

格斗游戏(fighting game)是一种两人实时对抗游戏，其重要特征是博弈者存在不同的角色和能力属性、博弈实时性高即博弈者须在短时间内做出决策并击败对手。针对这一序贯的零和博弈，唐等人的论文通过对对手行为模式的建模学习建立了一种新的智能决策算法，该算法在游戏 AI 的公开比赛中夺得冠军。

作为对手的游戏 AI 是由人编写的程序，可能具有行为模式，这是论文可行的基础。论文所提出的新游戏 AI 的核心是对手模型以及相应的滚动时域演化算法。对手的行为模型通过神经网络以及历史数据来拟合。基于对手模型，可以预测对手未来若干步的动作；进而，己方未来若干步表现良好的行为序列可以得到，最后通过遗传算法得到己方未来的行为序列，并从中选择第一步作为当前决策。

基于双人格斗游戏 AI 实时对抗平台 FightingICE，论文对该算法进行了内部测试，针对五种不同类型的对手模型，该算法均表现良好，胜率较高。该算法对应的格斗 AI Bot（ERHEA_PI）在 2020 年 IEEE Conference on Games 的格斗游戏人工智能竞赛中夺得最终冠军。论文结果可用于其他双人实时零和博弈任务。

(IEEE Transactions on Games 2021 年)

交通出行轨迹数据与出行行为研究

吴添

关于交通出行特征的研究，以往研究基本采用宏观平均的参数，忽略了车辆真实使用规律的差异性，比如出行规律和充电规律，导致个体层面的出行行为分析存在不足。因此，研究人员开始日益重视通过采集大样本车辆真实出行数据加以完善。其中，湖南大学的科研人员基于大样本私家车出行轨迹数据集，研究了个体出行行为和出行特征。

该研究基于 25,564 辆私家车轨迹数据中的停止等待信息，利用 DBSCAN（Density-Based Spatial Clustering of Applications with Noise）密度聚类方法识别出频繁访问的地点，并使用马尔可夫链研究了私家车在频繁访问地点之间行驶时的时空转换特性，进而基于时空熵的概念对每辆私家车的运动规律进行定量研究。

该研究的结果将为解决诸如缓解交通拥堵和改善交通服务等城市问题提供有效解决方案，为出行活动、交通管理和城市规划的研究提供了新的视角。

作为本领域的相关研究，美国的国家家庭交通调研（National Household Travel Survey，NHTS）数据库采集了全国范围内大规模个体出行特征，已经被卡内基梅隆大学、加利福尼亚大学、中佛罗里达大学等高校的科研人员广泛用于电动汽车电力覆盖里程、能耗与排放特征的研究。

（IEEE Transactions on Intelligent Transportation Systems，2020 年第 21 卷）

中国邮轮旅游需求预测方法

谢刚

现有关于邮轮旅游需求预测的文献仅采用单变量时间序列模型，基于邮轮游客量的历史数据对邮轮旅游需求进行预测。这些方法通常基于预测期内保持一致的模式和稳定的经济结构的假设。一旦发生剧烈变化和一次性不规则事件，它们可能无法提供准确的预测。为了有效提高中国邮轮旅游需求预测精度，中国科学院数学与系统科学研究院谢刚、钱雅彤和汪寿阳等人提出了一种基于大数据和参数优化的机器学习方法。

该方法利用重力搜索算法对最小二乘支持向量回归模型中超参数进行优化，并利用搜索引擎百度中的搜索查询数据和一些经济指标作为解释变量。在确定变量时，关键词选择经过平稳性、协整和格兰杰因果检验来确定，经济指标通过相关系数来确定。该研究的独特之处在于首次将大数据应用于中国邮轮旅游需求预测，大数据可能是先行指标，可以在一定程度上提前反映不规则事件的影响。

邮轮旅游是全球旅游行业中变化最快、利润最高的部门。随着消费水平的提高，中国的邮轮需求不断加大。在经历了十多年高速增长之后，中国的邮轮游客量增长率正在下降。因此，对于邮轮母港、邮轮和营销活动的投资风险正在加大。预测中国邮轮旅游需求是进行这些投资活动的必要前提，准确的预测可以有效地支持相关决策，如适当的邮轮旅游政策和营销策略。

(Xie, Qian, & Wang, Tourism Management 2021 年)