華中科技大學数学中心
Center for Mathematical Sciences

中国 武汉
Wuhan China

Newsletter, Spring 2023

- 数学中心冬令营
- 数学中心近期研究进展
- 后量子安全候选算法在计算机上一小时内被破解
- 不可辨别性混淆——密码学的下一个里程碑
- 人工智能将如何改变数学?
- 俄罗斯科学院斯捷克洛夫数学研究所简介

華中科技大學数学中心
Center for Mathematical Sciences

华中科技大学数学中心简介

在建设世界一流大学的征程中，数学学科的作用异常重要。华中科技大学高瞻远瞩，于2013年成立数学中心。华中科技大学数学中心一方面倡导数学不同分支之间的相互交叉，激发新的合作研究，催生新的研究领域和研究群体。另一方面引领数学与工科、理科，医科及其它学科之间的合作研究，实现交叉创新、 合作共赢。

作为我校国际交流与合作的平台，数学中心大力推动与发展“跨学科应用数学”合作研究。我们的跨学科合作研究领域包括数学与地球科学（物理海洋学和气候动力学）的交叉研究，以及数学与生命科学（计算和定量生物学）的交叉研究。

华中科技大学数学中心积极开展前瞻性研究，立足华中、辐射全国、影响海外。数学中心将国际先进的人才培养模式和研究机构运行机制有机融入到我国建设一流大学与一流学科的伟大事业之中，努力成为培养和聚集一流人才的平台， 国际交流与合作的平台，科教运行机制以及人事体制改革试点的平台。

数学中心成员包括院士，国家特聘专家，外专千人计划专家，长江学者，青年学术英才，楚天学者，洪堡学者和华中学者。还有一批海内外知名访问学者，博士后，博士生，以及来自多个国家的留学生。数学中心设有李国平讲座教授，东湖讲座教授，东湖数学论坛，和郭友中数理科学讲座。

希望重要的数学发现萌芽于此，

希望新的研究领域和研究群体产生于此，

希望著名数学家和科学家在此留下足迹，

希望科技界更深刻地感受到数学的作用：

数学强，则科技强；科技强，则国家强！

数学中心官网

数学中心微信公众号

地址：中国湖北武汉珞喻路1037号
华中科技大学创新研究院（恩明楼）8楼
邮编：430074
网页：mathcenter.hust.edu.cn
电邮：mathcenter@hust.edu.cn

Huazhong University of Science and Technology
1037 Luoyu Road, Wuhan, China
Postal Code：430074
Web：mathcenter.hust.edu.cn
E-mail：mathcenter@hust.edu.cn

目 录

News
新闻

数学中心冬令营 | 1 |
华中科技大学数学中心&哈步数据科技智能零售实验室顺利签约 | 4 |

Academic Achievement
学术成果

数学中心近期研究进展 | 5 |
2023 年 1 月—3 月已发表或已接收文章列表 | 10 |

Qualifying Exams
资格考试

Advanced Probability Theory Qualifying Exam | 11 |
Test of English for Math Writing | 12 |
Stochastic Analysis Qualifying Exam | 16 |

Popular Mathematics
数学热门话题

美国国家标准与技术研究院（NIST）发布首批四种抗量子加密算法 | 18 |
后量子安全候选算法在计算机上一小时内被破解 | 22 |
用来破解美国政府加密算法的数学定理 | 25 |
林蕙佳：不可辨别性混淆——密码学的下一个里程碑 | 28 |
数学家开发了试图连接微观和宏观领域的方程式 | 31 |
p-Laplacian Allen-Cahn 方程动力学的进一步研究 | 34 |
人工智能将如何改变数学？ | 36 |
俄罗斯科学院斯捷克洛夫数学研究所简介 | 40 |

News 新闻

数学中心冬令营

华中科技大学数学中心于 2023 年 1 月 5 日至 2023 年 2 月 7 日顺利举办数学中心冬令营活动。课程安排如下：

课程主题：**Differential Topology**

授课老师：胡晓文老师

时间：2023 年 1 月 5 日起，每周二、四、六 14:00-16:30

腾讯会议：359-6853-4671

课程安排：

日　期	时　间	日　期	时　间
2023 年 1 月 5 日 周四	14:00-16:30	2023 年 1 月 19 日 周四	14:00-16:30
2023 年 1 月 7 日 周六	14:00-16:30	2023 年 1 月 28 日 周六	14:00-16:30
2023 年 1 月 10 日 周二	14:00-16:30	2023 年 1 月 31 日 周二	14:00-16:30
2023 年 1 月 12 日 周四	14:00-16:30	2023 年 2 月 2 日 周四	14:00-16:30
2023 年 1 月 14 日 周六	14:00-16:30	2023 年 2 月 4 日 周六	14:00-16:30
2023 年 1 月 17 日 周二	14:00-16:30	2023 年 2 月 7 日 周二	14:00-16:30

参考资料：

Dundas “A short course in differential topology-Cambridge University Press”

报告人简介：

- 胡晓文，现就职于大湾区大学

课程主题：**Stochastic Analysis**

授课老师：段金桥老师及团队内研究生

时间：2023 年 1 月 5 日起，每周二、四晚上 18：30-21：30

腾讯会议：440-1408-5085

课程安排：

日　期	时　间	授课老师	内　容
2023 年 1 月 5 日 周四	晚上 6:30-9:30	段金桥老师、肖望	Chapter1
2023 年 1 月 10 日 周二	晚上 6:30-9:30	段金桥老师、丁以恒	Chapter2
2023 年 1 月 12 日 周四	晚上 6:30-9:30	张燕杰	Chapter3
2023 年 1 月 17 日 周二	晚上 6:30-9:30	李鹏博	Chapter4
2023 年 1 月 26 日 周四	晚上 6:30-9:30	张鹏	Chapter5
2023 年 1 月 31 日 周二	晚上 6:30-9:30	郭瑾	Chapter6
2023 年 2 月 2 日 周四	晚上 6:30-9:30	杨璐璇	Chapter7
2023 年 2 月 7 日 周二	晚上 6:30-9:30	黄慧芳	Chapter8

参考资料：

J-F. Le Gall “Brownian Motion, Martingales, and Stochastic Calculus”

课程主题：Stochastic Flows and Jump-Diffusions

授课老师：乔会杰老师（东南大学）；张华老师（江西财经大学）

时间：2023 年 1 月 9 日起，每周一、三、五 19:30-22:30

腾讯会议：856-9792-4082

课程安排：

日　期	时　间	授课老师	内　容
2023 年 1 月 9 日 周一	19:30-22:30	乔会杰老师	Lecture 1
2023 年 1 月 11 日 周三	19:30-22:30	乔会杰老师	Lecture 2
2023 年 1 月 13 日 周五	19:30-22:30	乔会杰老师	Lecture 3
2023 年 1 月 16 日 周一	19:30-22:30	张华老师	Lecture 4
2023 年 1 月 18 日 周三	19:30-22:30	张华老师	Lecture 5
2023 年 1 月 20 日 周五	19:30-22:30	张华老师	Lecture 6

参考资料：

Hiroshi Kunita “Stochastic Flows and Jump-Diffusions”

报告人简介：

- 乔会杰，现为东南大学副教授，硕、博士生导师，主要从事随机分析及其相关领域的研究工作。
- 张华，现为江西财经大学副教授，硕士生导师，主要从事随机分析及随机偏微分方程方面的研究。

*更多课程回放内容，关注哔哩哔哩官方账号：**华中大数学中心***

华中科技大学数学中心&哈步数据科技智能零售实验室顺利签约

为深入贯彻落实数字经济时代、创新驱动数字化发展。2023 年 3 月 1 日，华中科技大学数学中心联合哈步数据在学科建设、人才培养以及产学研持续合作发展的若干领域达成共识并展开深度合作，当天顺利举行智能零售实验室签约发布仪式！

哈步数据在数学中心设立创新人才中心，通过校企合作支持数学中心开展课程开发、教学、创新实践及学生竞赛等活动，吸引优秀的学生到哈步数据实习。双方将针对如下内容进行深度合作：

（1）智能零售平台；

（2）消费数据商业化；

（3）零售隐私计算平台；

（4）跨境电商智能运营等零售数字化智能专业建设。

哈步数据提供基于全球消费零售智能化平台的国内及国际相关合作方落地资源，开展针对高校的商业零售智能化生态建设。

双方将充分发挥哈步数据在零售经验、稀缺数据能力和大数据算法的能力，华中科技大学数学中心在基础科学、信息科学、智能制造、大数据工程等科研成果和人才高度集中的优势，通过强强联合，提升哈步数据自主创新能力和核心竞争力，促进相关学科发展、人才培养、成果转化和拥有自主核心技术的国家智能产业建设，实现双方共同发展。

未来华中科技大学数学中学与哈步数据将秉承“长期合作、相互促进、平等协商、互利共赢”的原则，围绕“十四五”总体发展规划，围绕国家宏观产业政策和区域发展政策，且符合双方发展规划，调动和发挥共同资源优势，实现共赢发展，驱动数字化发展蓝图。

Academic Achievement 学术成果

■ 数学中心近期研究进展

1. Neural network stochastic differential equation models with applications to financial data forecasting

——Luxuan Yang, Ting Gao, Yubin Lu, Jinqiao Duan, Tao Liu

Applied Mathematical Modelling
https://doi.org/10.1016/j.apm.2022.11.001

- In this article, we employ a collection of stochastic differential equations with drift and diffusion coefficients approximated by neural networks to predict the trend of chaotic time series which has big jump properties. Our contributions are, first, we propose a model called Lévy induced stochastic differential equation network, which explores compounded stochastic differential equations with α-stable Lévy motion to model complex time series data and solve the problem through neural network approximation. Second, we theoretically prove that the numerical solution through our algorithm converges in probability to the solution of corresponding stochastic differential equation, without curse of dimensionality. Finally, we illustrate our method by applying it to real financial time series data and find the accuracy increases through the use of non-Gaussian Lévy processes. We also present detailed comparisons in terms of data patterns, various models, different shapes of Lévy motion and the prediction lengths.

2. Detecting the Most Probable High Dimensional Transition Pathway Based on Optimal Control Theory

——Jianyu Chen, Ting Gao, Yang Li, Jinqiao Duan

Physica D，已投稿
https://arxiv.org/abs/2303.00385

- 基于最大值原理求高维迁移轨道。

3. Learning reduced effective dynamics from data-driven stochastic dynamcial systems

——Lingyu Feng, Ting Gao, Min Dai, Jinqiao Duan

Chaos，返稿修改已完成

https://arxiv.org/abs/2205.04151

➢ 短时数据预测长程，应用于快慢系统的慢流形逼近。

4. Model Based Reinforcement Learning with Non-Gaussian Environment Dynamics and its Application to Portfolio Optimization

——Huifang Huang, Ting Gao, Pengbo Li, Jin Guo, Peng Zhang, Nan Du

Applied Mathematical Modelling，已投稿

https://arxiv.org/abs/2301.09297v3

➢ 强化学习，发现复杂非高斯环境更适合股票市场，并得到投资回报的大幅提升。

5. Meta contrastive label correction for financial time series

——Luxuan Yang, Ting Gao, Min Dai, Yubin Lu, Wei Wei,

Cheng Fang, Yufu Lan, Jinqiao Duan

已投稿

https://arxiv.org/abs/2303.08103

➢ 少量金标准数据对于大量噪声数据的标签自动校正。

6. Approximations of Levy processes by integrated fast oscillating Ornstein-Uhlenbeck processes

——L. Feng, T. Gao, T. Li, Z. Lin, X. Liu

stochastics and dynamics，已投稿

➢ 建立了 Skorokhod M_1-拓扑下 Lévy 过程的一种光滑逼近方法。

7. Level structures on p-divisible groups from the Morava E-theory of abelian groups

——Zhen Huan, Nathaniel Stapleton

Mathematische Zeitschrift

https://doi.org/10.1007/s00209-023-03216-7

- The close relationship between the scheme of level structures on the universal deformation of a formal group and the Morava E-cohomology of finite abelian groups has played an important role in the study of power operations for Morava E-theory. The goal of this paper is to explore the relationship between level structures on the p-divisible group given by the trivial extension of the universal deformation by a constant p-divisible group and the Morava E-cohomology of the iterated free loop space of the classifying space of a finite abelian group.

郇真在今年第一季度继续对 2-向量丛研究，通过代数几何方法建立之前构造的 2-向量丛和椭圆上同调之间的联系。另外，郇真在和纽约大学阿布扎比分校的 Sati 教授和 Schreiber 教授合作，共同证明他们提出的猜想：（郇真之前构造的）twisted 拟椭圆上同调理论在 4 维球面上的取值在膜物理中至关重要。目前郇真已经完成关于 twisted 拟椭圆上同调的大部分计算。

8. Blowups and longtime developments with near-boundary mass accretions of irregularly- shaped Euler- Poisson dominated molecular clouds in astrophysics

——Chao Liu

SIAM Journal on Mathematical Analysis，已接收

- Motivated by the astrophysical problems of star formations from molecular clouds, we make the first step on the possible long time behaviors of certain irregularly-shaped molecular clouds. We emphasis the main difficulty of the blowups of the irregular-shaped fluids with vacuum (molecular clouds) comes from the initial irregular configurations of its density (multiple centers of gravity). This inevitably causes far more complicated movements during the evolution than the one with spherical symmetry. The spherical symmetric case has been well studied. However, for the non-spherical symmetric case with the gravity, it is very rare in the references due to a very complicate nonlinear interaction between the gravity and the fluids. This article concludes, under the admissible data (i.e., large scale, irregularly-shaped, expanding and rotational molecular clouds), the developments of the solution (molecular clouds)

are either global (the first class) with near-boundary mass accretions (leads to star formations), or blowup at finite time. In addition, certain singularities can be removed from the boundary if the data is strongly admissible. This paper partially answers Makino's conjecture [37] in 1992 on the finite time blowup of any tame solution without symmetries for some data and the model of the molecular clouds and the local wellposedness have been established in the companion article [30].

新研究成果：两篇正在写的文章关于膨胀的牛顿宇宙下完全非线性球对称非均匀引力不稳定性的证明。同时要求近抛物面型的压强分布和熵分布。

9. Geometric dynamics ofanchored filamentous networks subject to viscous flow

——Congping Lin, Peter Ashwin

Communications in Nonlinear Science and Numerical Simulation

https://www.sciencedirect.com/science/article/pii/S1007570422004993

- The Endoplasmic Reticulum (ER) is an organelle that can form a complex dynamic network of filaments embedded in the viscous flowing cytoplasm of plant cells, anchored to points in the cell membrane. We consider an idealized dynamical model of the ER network as constant tension filaments subject to viscous forces from cytoplasmic flow. We show that simple configurations lead to the creation of a filamentous network that is analogous to a 2D foam, but with different physical mechanisms. We consider a fixed set of anchor points and propose an adaptive algorithm to track the network in the presence of the flow. We find that minimal (Steiner) networks joining these anchor points can support filamentous network of varying geometries with and without an imposed flow. We demonstrate that, after the flow has ceased, the filamentous network can retain memory of previous flow direction and intensity.

我们考虑一个理想的动态模型的 ER 网络作为恒定张力丝受到粘性力从细胞质流动。我们表明，简单的配置导致了类似于 2D 泡沫的丝状网络的创建，但具有不同的物理机制。

10. Emergence of purely nonlinear localized states with frequencies exited from spectral bands

——Huajie Song, Haitao Xu

已投稿

https://arxiv.org/abs/2303.05247

- 对非线性格点（或晶格）系统中一种局部态的出现机制进行了讨论，考虑晶格大小的有限性并引入大晶格极限，描述了频率从谱带离开时对应的解的局部聚集效应，这是非线性格点系统数学研究中的一个常见现象，同时此问题也具有拓扑绝缘体的非线性边缘态的应用背景。

11. Three-dimensional numerical study on wrinkling of vesicles in elongation flow based on the immersed boundary method

——Wang Xiao, Kai Liu, John Lowengrub, Shuwang Li, and Meng Zhao

Physical Review E

https://journals.aps.org/pre/abstract/10.1103/PhysRevE.107.035103

- We study the wrinkling dynamics of three-dimensional vesicles in a time-dependent elongation flow by utilizing an immersed boundary method. For a quasispherical vesicle, our numerical results well match the predictions of perturbation analysis, where similar exponential relationships between wrinkles' characteristic wavelength and the flow strength are observed. Using the same parameters as in the experiments by Kantsler *et al*. [V. Kantsler *et al*., Phys. Rev. Lett. 99, 178102 (2007)], our simulations of an elongated vesicle are in good agreement with their results. In addition, we get rich three-dimensional morphological details, which are favorable to comprehend the two-dimensional snapshots. This morphological information helps identify wrinkle patterns. We analyze the morphological evolution of wrinkles using spherical harmonics. We find discrepancies in elongated vesicle dynamics between simulations and perturbation analysis, highlighting the importance of the nonlinear effects. Finally, we investigate the unevenly distributed local surface tension, which largely determines the position of wrinkles excited on the vesicle membrane.

研究了移动界面自相似演化的非线性分析，联系线性分析和数值模拟的结果，为研究界面长时间动力学提供了新的研究思路。

■ 2023 年 1 月—3 月已发表或已接收文章列表

1. Yang L, Gao T, Lu Y, et al. Neural network stochastic differential equation models with applications to financial data forecasting[J]. Applied Mathematical Modelling, 2023, 115: 279-299.

2. Huan Z, Stapleton N. Level structures on p-divisible groups from the Morava E-theory of abelian groups[J]. Mathematische Zeitschrift, 2023, 303(3): 64.

3. Liu C. Blowups and longtime developments with near-boundary mass accretions of irregularly-shaped Euler--Poisson dominated molecular clouds in astrophysics[J]. SIAM Journal on Mathematical Analysis. Accepted.

4. Lin C, Ashwin P. Geometric dynamics of anchored filamentous networks subject to viscous flow[J]. Communications in Nonlinear Science and Numerical Simulation, 2023, 118: 107012.

5. Xiao W, Liu K, Lowengrub J, et al. Three-dimensional numerical study on wrinkling of vesicles in elongation flow based on the immersed boundary method[J]. Physical Review E, 2023, 107(3): 035103.

Qualifying Exams 资格考试

Advanced Probability Theory Qualifying Exam

Center for Mathematical Sciences Huazhong University of Science and Technology
Spring 2023

Note: This exam covers Part I and Part II of Le Gall: Measure Theory, Probability, and Stochastic Processes.

1. Let $(E,\mathcal{A},\mu)$ be a measure space, and let $(A_n)_{n\in\mathbb{N}}$ be a sequence in $\mathcal{A}$. Show that the condition
$$\sum_{n=1}^{\infty}\mu(A_n)<\infty$$
implies $\mu(\limsup A_n)=0$

2. We assume that $\mu(E)<\infty$. Let $(f_n)_{n\in\mathbb{N}}$ and f be real measurable functions on E, and let $p\in[1,\infty)$. Show that the conditions
(i) $f_n\to f,\mu\ a.\ e.$,
(ii) there exists a real $r>p$, such that $\sup_{n\in\mathbb{N}}\int|f_n|^r\,d\mu<\infty$, imply that $f_n\to f$ in L^p.

3. Let X be a real random variable. Assume that X is integrable $(E[|X|]<\infty)$. Prove that
$$\lim_{x\to+\infty}\mathbb{E}\left[|X|1_{\{|X|\geq x\}}\right]=0$$

4. Let $(X_n)_{n\in\mathbb{N}}$ be a sequence of real random variables. Assume that there exists a constant C such that $\mathbb{E}\left[(X_n)^2\right]\leq C$ for every $n\in\mathbb{N}$, and that $\operatorname{cov}(X_n,X_m)=0$ if $n\neq m$.
(i) Verify that
$$\frac{S_{n^2}-\mathbb{E}\left[S_{n^2}\right]}{n^2}\xrightarrow[n\to\infty]{}0,\ a.\ s.$$
(ii) Deduce from question (1) that we have also
$$\frac{S_n-\mathbb{E}[S_n]}{n}\xrightarrow[n\to\infty]{}0,\ a.\ s.$$

5. Let $(\mathcal{A}_n)_{n\in\mathbb{N}}$ be a sequence of sub-σ-fields of $\mathcal{A}$, and let $(X_n)_{n\in\mathbb{N}}$ be a sequence of nonnegative random variables.
(i) Prove that the condition "$\mathbb{E}\left[X_n|\mathcal{A}_n\right]$ converges in probability to 0" implies that X_n converges in probability to 0.
(ii) Show that the converseis false.

Test of English for Math Writing

Center for Mathematical Sciences Huazhong University of Science and Technology

mathcenter.hust.edu.cn

March 3, 2023

Total: 100 +5=105 points.

Part I:

For each statement, please provide a better version, by correcting grammar mistakes and/ or improving the writing style. (Two points for each problem. No partial credits.)

1. Let A is a number.
2. ...., where $A > 0$ is a number.
3. Section 1. Transition phenomena in stochastic dynamical systems and its application.
4. Suppose that $A > 0$ is a number.
5. f is a function and K is a constant.
6. J. Duan, An introduction To Stochastic dynamics. Cam University Press, 2015.
7. This is a SDE. It is useful in studying chemical reacting system.
8. We first prove A, then prove B. Furthermore, C is presented.
9. In this paper, inspired by Yan Wei's works and motivated by a paper in 1989, a stability result is proved.
10. For smooth function f, this functional is positive.
11. We consider following system.
12. This is dynamical system. We study dynamical behavior of this dynamical system.

13. This is locally Lipschitz condition. That is local Lipschitz condition. This is a local Lipschitz continuous function.

14. Stochastic dynamical system (including various stochastic differential equations) is an appropriate mathematical model of complex system.

15. Stochastic dynamical systems, which have been widely used to describe complex phenomena in physical, biological, and engineering systems, and which are interesting subject that is hot topic and also very interesting, are good mathematical models.

16. This is a good result, see [88].

17. Suppose $A = 9$ and $B = 0$, we obtain $C = 888$.

18. Assume that $A = 8$, then $B = 0.888$.

19. For $-9 < A^2 - B < 88$, we conclude $C = 6$.

20. Consider the following system:

$$A = 0.8$$
$$B = 888.$$

21. We first show a result A, then we proved a result B, and finally a result C has been demonstrated.

22. Suppose $A > 0$, $B < 9$, let $C = 0.9$, then $f > 0$.

23. The aim of this review paper is mainly considered nonlocal dynamics for non-Gaussian systems arising in gene regulatory network. The mean exit time, escape probability and maximal likely trajectory are utilized to quantify dynamical behaviors of stochastic differential equations with non-Gaussian α-stable type Lévy motions. This review paper is mainly considered how non-Gaussianity index and noise intensity affect the gene network.

24. Stochastic dynamical systems driven by noise have attracted a lot of attention

recently. It is widely used in physics.

25. We will introduce the connections between stochastic dynamics and nonlocal partial differential equation.

26. We will analysis how non-Gaussianity index and noise intensity affect the MeKS network.

27. P_{comK} denotes the promoter of gene *comK*.

28. Figure 1a is from [1] and Fig. 1b is from [2].

29. We will use the mean exit time, escape probability and Maximal likely trajectory to help quantify stochastic dynamics.

30. We adopt shooting method in [58] to solve two-point boundary value problem (7)-(8).

31. Random fluctuations have been extensively considered in the modeling and analysis of genetic regulatory systems [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20].

32. There exists powerful evidences indicating that gene expression with small diffusion and large bursting resembles the composition of systems with Lévy noise.

33. We consider orbit from x to y.

34. I have read paper about Onsager-Machlup action functional.

35. This is trajectory for a dynamical system.

36. Section 4. These are trajectories for dynamical system.

37. $f(x)$ is also equal to the gradient of potential function.

38. The most probable transition pathways are computed by numerically solving two

point boundary value problem.

39. This theorem holds if A or B is true.

40. This is a path connects A and B.

41. We call $S(x)$ is the action at x.

42. So to find the most probable transition path u_t, one is supposed to find it satisfies the following condition.

43. Note that f is a strict increase function.

44. There may be several paths satisfy (1) and (2).

45. It is true for every $T_0 < t^* \leq T_f$.

46. Let $A > 0$, it is easy to show this theorem.

47. It is clear from the Theorem 1.

48. Consider the equation (8), with r is a constant.

49. Let $U_t = Y_t - (\zeta + \int_{|z|<r} \{z - (e^z - 1)\} \nu(dz))t$ is a symmetric α-stable Lévy process.

50. This is a n-dimensional linear space.

Part II:

1. Translate this English paragraph into Chinese. (Three points. No partial credits.)

Paul R. Halmos: The heart of mathematics consists of concrete examples and concrete problems. Big general theories are usually afterthoughts based on small but profound insights; the insights themselves come from concrete special examples.

2. List three math books written by Paul R. Halmos. (Two points. No partial credits.)

Stochastic Analysis Qualifying Exam

Center for Mathematical Sciences Huazhong University of Science and Technology

January 2023

Note: This exam covers Jean-Francois Le Gall: Brownian Motion, Martingales, and Stochastic Calculus Chapters 1 - 7.

1. (20 points) (i). Show that the process $(W_t)_{t\geq 0}$ defined by $W_0 = 0$ and $W_t = tB_{1/t}$ for $t > 0$ is (indistinguishable of) a real Brownian motion started from 0. (Hint: First verify that W is pre-Brownian motion)
   (ii). Infer that $\lim_{t\to\infty} \frac{B_t}{t} = 0$ a. s.

2. (20 points) (i) Let M be a martingale with continuous sample paths such that $M_0 = x \in \mathbb{R}_+$. We assume that $M_t \geq 0$ for every $t \geq 0$, and that $M_t \to 0$ when $t \to \infty$, a. s. Show that, for every $y > x$,
   $$\mathbb{P}(\sup_{t\geq 0} M_t \geq y) = \frac{x}{y}. \tag{1}$$
   (ii) Assume now that B is a Brownian motion stared from 0, and let $\mu \geq 0$. Using an appropriate exponential martingale, show that
   $$\sup_{t\geq 0}(B_t - \mu t) \tag{2}$$
   is exponential distributed with parameter 2μ.

3. (20 points) (i) Let M be a (true) martingale with continuous sample paths, such that $M_0 = 0$. We assume that $(M_t)_{t\geq 0}$ is also a Gaussian process. Show that, for every that $t \geq 0$ and every $s > 0$, the random variable $M_{t+s} - M_t$ is independent of $\sigma(M_r, 0 \leq r \leq t)$.
   (ii) Under the assumptions of questions (i), show that there exists a continuous monotone nondecreasing function $f : \mathbb{R}_+ \to \mathbb{R}_+$ such that $\langle M, M\rangle_t = f(t)$ for every $t \geq 0$.

4. (20 points) Let $(X_t)_{t\geq 0}$ be a semimartingale. We assume that there exists an $(\mathcal{F}_t)$- Brownian motion $(B_t)_{t\geq 0}$ started from 0 and a continuous function b: $\mathbb{R} \to \mathbb{R}$, such that
   $$X_t = B_t + \int_0^t b(X_s)ds. \tag{3}$$
   (i) Let $F : \mathbb{R} \to \mathbb{R}$ be a twice continuously differentiable function on $\mathbb{R}$. Show that, for $F(X_t)$ to be a continuous local martingale, it suffices that F satisfies a second-order differential equation to be determined.

(ii) Give the solution of this differential equation which is such that $F(0)=0$ and $F'(0)=1$. In what follows, F stands for this particular solution, which can be written in the form $F(x)=\int_0^x \exp(-2\beta(y))dy$, with a function β that will be determined in terms of b.

5. (20 points) Let υ be a nonnegative function in $C_0(E)$, For every $x\in\mathbb{E}$ and every $t\geq 0$, we set, for every $\varphi\in\mathbb{B}(E)$,

$$Q_t^*\varphi(x)=\mathbb{E}_x\left[\varphi(X_t)\exp(-\int_0^t \upsilon(X_s)ds)\right]. \tag{4}$$

(i) Show that, for every $\varphi\in\mathbb{B}(E)$ and $s,t\geq 0$, $Q_{t+s}^*\varphi=Q_t^*(Q_s^*\varphi)$.

(ii) Let $\varphi\in C_0(\mathbb{R}^d)$ and set $u_t(x)=Q_t^*\varphi(x)$ for every $t>0$ and $x\in\mathbb{R}^d$. Prove that, for every $x\in\mathbb{R}^d$, the function $t\mapsto u_t(x)$ is continuously differentiable on $(0,\infty)$, and

$$\frac{\partial u_t}{\partial t}=\frac{1}{2}\Delta u_t-\upsilon u_t. \tag{5}$$

Popular Mathematics 数学热门话题

NIST 公布了 4 种抗量子加密算法，为抵御未来可能受到的量子计算机破解攻击提前布局。首批 4 种抗量子加密算法包括用于通用加密的 CRYSTALS-Kyber 算法，以及用于数字签名的 CRYSTALS-Dilithium、FALCON 和 SPHINCS+算法。以上 4 种加密算法基于结构化格和哈希函数，这两类数学问题可以抵抗量子计算机的攻击，从而保护数据免受密码分析的攻击。

马里兰州盖瑟斯堡的 NIST 中子研究中心（来源：NIST）

但是没过多久，比利时鲁汶大学的研究人员利用纯数学成功破解了 SIKE（Supersingular Isogeny Key Encapsulation）后量子加密算法。对于后量子密码学，研究人员还需要大量的工作，这在密码和数学上的探索是至关重要的。

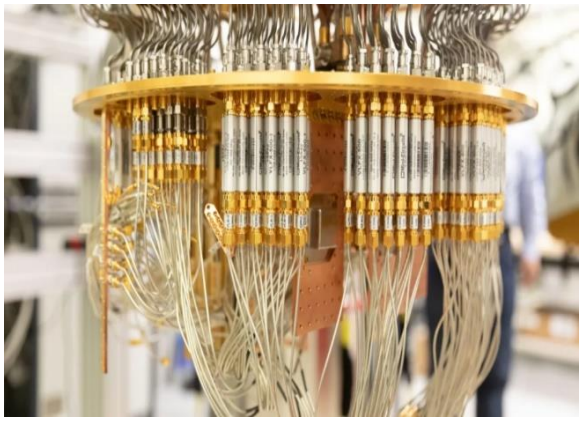
NIST Announces First Four Quantum Resistant Cryptographic Algorithms

美国国家标准与技术研究院（NIST）发布首批四种抗量子加密算法

GAITHERSBURG, Md. — The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day — such as online banking and email software. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years.

"Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project.



谷歌量子计算机（来源：CNET）

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools. As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm for each use case in the event one proves vulnerable.

"Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information." —NIST Director Laurie E. Locascio

Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send. Widely used public-key encryption systems, which rely on math problems that even the fastest conventional computers find intractable, ensure these websites and messages are inaccessible to unwelcome third parties.

However, a sufficiently capable quantum computer, which would be based on different technology than the conventional computers we have today, could solve these math problems quickly, defeating encryption systems. To counter this threat, the four quantum-resistant algorithms rely on math problems that both conventional and quantum computers should have difficulty solving, thereby defending privacy both now and down the road.

The algorithms are designed for two main tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ (read as "Sphincs plus"). Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

To prepare, users can inventory their systems for applications that use public-key cryptography, which will need to be replaced before cryptographically relevant quantum computers appear. They can also alert their IT departments and vendors about the upcoming change. To get involved in developing guidance for migrating to post-quantum cryptography, see NIST's National Cybersecurity Center of Excellence project page.

Post-Quantum Safe Algorithm Candidate Cracked in an Hour on a PC

后量子安全候选算法在计算机上一小时内被破解

By Matt Swayne

Well, that decrypted quickly…

A team of scientists report they were able to defeat one of the post-quantum safe algorithms that is still under consideration as part of the National Institute of Standards and Technology's (NIST) PQC program — and it only took one computational core on a PC working for about an hour.

The team, from Computer Security and Industrial Cryptography group (CSIS) at KU Leuven, were able to crack the algorithm SIKE — or Supersingular Isogeny Key Encapsulation (SIKE) — using a mathematical approach to understand SIKE's encryption and then predict and steal its encryption keys.

In the study, the researchers write: "We present a new and powerful key recovery attack on

the Supersingular Isogeny Diffie–Hellman key exchange protocol and its instantiation SIKE that recently advanced to the fourth round of NIST's ongoing Post-Quantum Cryptography standardization process. It is based on a "glue-and-split" theorem from 1997 due to Ernst Kani and heavily outperforms previous attack strategies…"

Startingly, the hack was performed on a classical computer — and took about an hour to complete.

They write: "A run on the SIKEp434 parameters, previously believed to meet NIST's quantum security level 1, took about 62 minutes, again on a single core. We also ran the code on random instances of SIKEp503 (level 2), SIKEp610 (level 3) and SIKEp751 (level 5), which took about 2h19m, 8h15m and 20h37m, respectively."

SIKE was among several algorithms that passed a NIST competition to identify and define standardized post-quantum algorithms. Because quantum computers represent a threat to current measures for securing information and data, the organization wanted to pinpoint algorithms that stood the best chance of withstanding attacks from quantum computers.

In a blog post, Steven Galbraith, a University of Auckland mathematics professor and a leading cryptographic expert, explains how they accomplished the hack: "The attack exploits the fact that SIDH has auxiliary points and that the degree of the secret isogeny is known. The auxiliary points in SIDH have always been an annoyance and a potential weakness, and they have been exploited for fault attacks, the GPST adaptive attack, torsion point attacks, etc."

It's not the end for SIKE. There may be ways to modify the algorithm to withstand these specific types of attacks. However, in an Ars Technica story, Jonathan Katz, professor in the department of computer science at the University of Maryland, said the news that a classical computer could crack an encryption scheme meant to be safe from quantum devices is troubling.

Katz wrote: "It is perhaps a bit concerning that this is the second example in the past six months of a scheme that made it to the 3rd round of the NIST review process before being completely broken using a classical algorithm. (The earlier example was Rainbow, which

was broken in February.) Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward."

Based on the achievement, the team — Wouter Castryck and Thomas Decru — should be in line to win $50,000 from Microsoft's SIKE Cryptographic Challenge.

Mathematical theorem used to crack US government encryption algorithm

用来破解美国政府加密算法的数学定理

By Catarina Chagas, Queen's University

In the digital era and moving towards quantum computing, protecting data against hack attacks is one of our biggest challenges—and one that experts, governments, and industries worldwide work hard to address. While this is an effort to build a more connected and safe future, it can certainly learn from the past.

In July, the US National Institute of Standards and Technology (NIST) selected four encryption algorithms and posed some challenge problems to test their security, offering a $50,000 reward for whomever managed to break them. It happened in less than an hour: one of the promising algorithm candidates, named SIKE, was hacked with a single personal computer. The attack did not rely on a powerful machine, but on powerful mathematics based on a theorem developed by a Queen's professor decades ago.

Ernst Kani has been researching and teaching since the late 1970s—first at the University of Heidelberg, in Germany, and then at Queen's, where he joined the Department of Mathematics and Statistics in 1986. His main research focus is arithmetic geometry, an area

of mathematics that uses the techniques of algebraic geometry to solve problems in number theory.

The problems Dr. Kani works to solve stretch back to ancient times. His specific field of research was pioneered by Diophantus of Alexandria around 1,800 years ago and is a set of problems known as Diophantine questions. One of the most famous questions in the field is Fermat's Last Theorem, posed by Pierre Fermat in 1637 and which took the math community 350 years to prove—an accomplishment by Princeton professor Andrew Wiles in 1994. Wiles received many prizes and honors for this work, including an honorary doctorate from Queen's in 1997.

Neither Diophantus nor Fermat dreamt of quantum computers, but Dr.Kani's work on Diophantine questions resurfaced during the NIST round of tests. The successful hackers—Wouter Castryck and Thomas Decru, both researchers at the Katholieke Universiteit Leuven, in Belgium—based their work on the "glue and split" theorem developed by the Queen's mathematician in 1997.

As a matter of fact, Dr. Kani was not concerned about cryptographic algorithms when he developed the theorem. That work kicked-off in the 1980s, in collaboration with another German mathematician, Gerhard Frey—whose work was crucial in solving Fermat's last theorem. Drs. Kani and Frey wanted to advance research on elliptic curves, a particular kind of equation that would later be used for cryptographic purposes.

Both researchers' goals at that time were purely theoretical. They were interested in manipulating mathematical objects to learn more about their own properties. "Doing pure mathematics is an end by itself, so we don't think of real-world applications," Dr. Kani explains. "But, later, many of those studies are useful for different purposes. When Fermat proposed his theorem hundreds of years ago, his intent was to be able to factor certain large numbers. The application to cryptography came only much later in 1978. Basically, all the methods we use today for data encryption are based on mathematics."

Doughnuts and curves

Mathematicians often refer to mathematics as a beautiful thing. For those who don't work in

the field, it might be challenging to see this beauty, or even to have a high-level understanding of what these research projects are all about—it requires some imagination.

Imagine an object shaped like a doughnut, with a hole in the middle: that's a visual model of an elliptic curve, also known as a genus one curve. Drs. Kani and Frey wanted to combine two genus one curves to form a new object—a genus two curve, something we can imagine like two doughnuts stuck solidly together side by side. They aimed to use some properties of the constructed genus two curve to deduce certain properties of the two original genus one curves, which were "glued" together.

In his 1997 paper, Dr. Kani generalized the original construction by gluing together an arbitrary pair of elliptic curves. But in that case the construction sometimes fails—it might construct an object in which the two doughnuts only touch each other in a single point. The paper analyzes the precise conditions for when this happens (i.e., when the construction fails or "splits"). Castryck and Decru used this characterization of the failure in their method of attacking the proposed encryption scheme SIKE.

"Our problem had nothing to do with cryptography, which is why I was surprised when I heard of the algorithm attack. It was quite ingenious, what they did there!" says Dr. Kani. "One of the co-authors of the SIKE algorithm expressed surprise in the fact that genus two curves could be used to gain information about elliptic curves. But this was precisely our original strategy in the 1980's and 1990's (and afterwards)."

Although cryptographers and computing engineers are not always wellversed in all the high-powered techniques of mathematics, many different skills and forms of knowledge can be combined to advance the way we store and transmit data.

"Cryptography uses a lot of sophisticated mathematics, especially arithmetic geometry. Computing experts and math experts have to work together to advance this field," says Dr. Kani, who continues to teach undergraduate and graduate courses and to work in arithmetic geometry—particularly on problems involving genus two curves and elliptic curves.

Huijia Lin proved that a new tool – iO, is the Next Milestone in Cryptography

林蕙佳：不可辨别性混淆——密码学的下一个里程碑

By Elizabeth Quill

A long-sought "holy grail" in cryptography is poised to change the way we protect sensitive information.

Today's standard encryption schemes take an all-or-nothing approach. Once scrambled, your data become inaccessible to anyone without the secret key.

This has allowed for secure e-mail communication, the proliferation of online transactions and digital signatures. It allows tax and medical records with sensitive personal information to be passed more safely across the internet. But if you give someone the secret key to access any of the data, all of the data become vulnerable.

What if instead you could assign specific people access to do very specific things with your data? Someone could get the information they need (the info you want them to have) without unlocking all of the original data. Bank details, credit card numbers, account passwords – all would remain hidden. That wholly different approach could also allow Netflix to make show recommendations without seeing your full viewing history, for example. Google could sort your e-mails without knowing what's in them. And medical researchers could analyze data to identify risk factors for a disease without accessing any individual's health information.

This and other cryptographic wonders now appear possible through a master tool called indistinguishability obfuscation.

"It's a new tool – a very powerful tool," says cryptographer Huijia (Rachel) Lin of the University of Washington in Seattle who showed with colleagues in 2020 how to construct the tool. "Once you have this superstrong power, then a lot of the other tasks are either special cases of it, or you can easily use this to realize [those tasks]."

Vinod Vaikuntanathan, a computer scientist at MIT who has worked with Lin on previous research, compares indistinguishability obfuscation, or iO, to a grand theory in physics that would unite gravity and quantum mechanics. “iO gives you a way to do a grand unification of cryptography in the sense that you can explain much of what cryptography does in a very simple way.”

Standout research

Indistinguishability obfuscation is a form of program obfuscation, an approach that seeks to hide the inner workings of a computer program, not just the message or data itself. Though proposed in 1976 in a paper that set the foundation for modern cryptography, program obfuscation proved difficult to achieve. For many years, people thought it might not be possible.

And in 2001, researchers showed that complete program obfuscation — called black-box obfuscation, in which input and output data are known but nothing else about a program can be discovered — is impossible. Yet indistinguishability obfuscation, proposed at the same time and shown to be incredibly powerful, doesn’t demand that everything about a program remain hidden. It instead deals with two programs that perform the same function. If the inner workings of those two programs can be hidden enough that the two can’t be distinguished from each other, indistinguishability obfuscation has been achieved. By hiding the secret key within the program itself, iO enables the delegation of specific data and data tasks to specific people.

Still, proposal after proposal for making iO work proved breakable. Researchers couldn’t figure out how to keep it safe from an adversary’s attacks. Lin says the approaches being used didn’t appeal to her. Researchers were leaning on what appeared to be “good enough” ways of getting at the problem that weren’t backed by rigorous mathematical proofs.

Lin instead wanted to break the problem down so she could understand each component and how they worked together. She wanted to approach the problem like a clock, with gears and nuts and bolts, instead of tangled like “a bowl of spaghetti.”

Through this strategy, Lin, along with Amit Sahai of UCLA and Aayush Jain, a Ph.D.

student at UCLA at the time, demonstrated that iO is achievable. It would be secure based on standard assumptions in the field, the team proved, renewing hope in the tool.

"Of course, [Huijia] is brilliant," Vaikuntanathan says, adding that her persistence is what really sets her apart. "It takes some guts to continue with an approach when essentially all the rest of the world thinks that it is not going to work."

Backstory

Lin says she didn't grow up with computers or fall in love with computer programming at an early age. As a student, she was interested in physics and strived to be good at everything. She started with computer science in college; a class in cryptography as a Ph.D. student at Cornell University "was really mind-opening," she says. Her introduction to what are known as zero-knowledge proofs stands out in her memory.

A zero-knowledge proof says that a person can convince someone else that they know a secret without revealing the secret or any details about it. Say, for example, you knew that a number was the product of two prime numbers. Can you convince someone that fact is true without revealing what the primes are? How to prove that such a task is possible fascinated Lin.

Cryptography includes a lot of these seeming paradoxes that prove to be possible. Indistinguishability obfuscation is yet another example – and Lin works on others, including secure multiparty computation, which allows a computer task to run across multiple people's data without any person having to reveal their data to anyone in the group, or to a third party.

"I'm very attracted to these magical concepts," Lin says. "The fun of it is to make this concept come to realization."

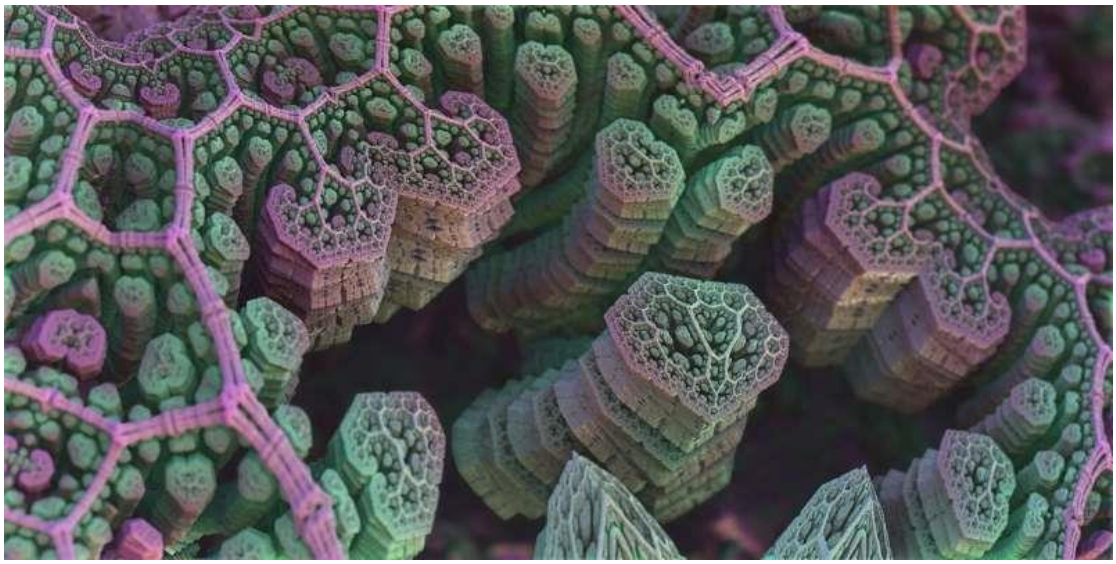
Indistinguishability obfuscation is still far from real-world implementation. But Vaikuntanathan says it's not unusual for first constructions of what will become important approaches to be impractical at first. "Wait for a decade," he says.

Mathematician develops equations that seek to bridge the micro and macro realms by Eindhoven University of Technology

数学家开发了试图连接微观和宏观领域的方程式

By Eindhoven University of Technology

一旦粒子数量多了，它们的行为往往会有所不同。由于数据的复杂性不断增加，描述它们行为的微观模型很快就变得非常难以计算，而且数据量巨大。这对那些对宏观系统（如自然、种群或肿瘤）的动力学感兴趣的研究人员提出了挑战。数学家 Jasper Hoeksma 通过将粒子数量设为无穷大，提出了一种可以在微观和宏观两个层面上都适用的数学方程。



If you look at the world with a microscope, or at the universe with a telescope, it turns out that many things can be described in terms of particles: particles that move, wiggle, hop or even pop in and out of existence. Particles can be molecules, bacteria, pixels, plants, planets, or sometimes even people.

In his thesis, mathematician Jasper Hoeksema has investigated the following question: what happens if you put many particles together, take a few steps back, and squint your eyes a bit?

"Instead of individual particles, you suddenly start to see vague colors or shades of gray.

These roughly correspond to how many particles there are at any given spot. The more particles there are, and the further you step back, how sharper this picture becomes. Just like a painting in a museum that only makes sense when you look at it from a distance," explains Hoeksema.

"Mathematically, you can even talk about what happens if you take the number of particles to infinity, which is precisely what I did."

From micro to macro

Answering this question does more than merely satisfy a mathematical curiosity, says Hoeksema.

"It serves to bridge two ways of looking at reality that are often worlds apart. While microscopic models track the state of all particles in a system individually, macroscopic models look at the world from a more abstract level, describing qualities like movement, density, velocity and temperature."

"Take the behavior of minute cracks in metal structures. It's relatively easy to describe the way these fissures attract and repel each other as a random (stochastic) process. But what if you want to explain how a metal beam bends? You can of course try to aggregate the insights you gained at the microscopic level, and deduce from that how things work at a macroscopic level. But these calculations very quickly become very costly.

"As an alternative, engineers have come up with alternative models that, although less rigorous, can be used for experimental observations. My question is: how can I bring these models together? How can we derive a mathematical equation that fits both realities and is also rigorous?"

Two scenarios

For this, Hoeksema looked at two scenarios: one where particles attract and repel each other (like metal cracks), and one where particles are being added and removed (like changes in population, ecology and tumors).

In both cases he was able to show that if the number of particles approaches infinity, the density of the particles more and more satisfies a particular mathematical equation. Moreover, he calculated the probabilities that the particles differ from this expected behavior, and show that these probabilities become smaller and smaller.

"All of this guarantees that in the end we can throw away the positions of all the particles, and only have to worry about the mathematical equation itself," says Hoeksema. "This equation will allow you to make accurate predictions about the behavior of dynamic systems at a macroscopic level, without requiring massive amounts of computing power."

Hoeksema is very happy with the results of his mathematical investigations, which are part of a broader research project led by his supervisor Oliver Tse. "It is not often that mathematics succeeds in catching up with the practical research of physicists and their models. This shows why mathematics at a theoretical level matters, even if the applications are ten to twenty years away."

A closer look at the dynamics of the p-Laplacian Allen–Cahn equation

p-Laplacian Allen-Cahn 方程动力学的进一步研究

By Incheon National University

来自韩国的研究人员使用带有p-Laplacian的Allen-Cahn方程分析了有界性和能量衰减性质的数值格式。研究揭示了 p-Laplacian 算子下 Allen-Cahn 方程的基本性质（相位分离、有界性和能量衰减性）。鉴于 Allen-Cahn 方程的广泛应用，这些结果有助于发展对复杂生物化学反应的数学理解。

In the past few decades, the use of phase field-modeling equations for mathematical modeling has progressed. Phase separation has been studied extensively in thermodynamics and materials engineering, but the biological field has also begun to take an interest in this phenomenon.

The Allen–Cahn equation (AC equation) is one such reaction-diffusion equation, used to study the evolution of the non-conserved phase-field interfaces separating different physical regions. Originally introduced to model the motion of anti-phase domain (crystallographic defect) formation in a binary alloy, it is now widely used from processing geometrical image segmentation to studying crystal growth.

Concurrent with these developments, several new operators for the AC equation (such as fractional Laplacian and p-Laplacian) have also been proposed. The p-Laplacian, for example, appears in mathematical models of physical processes such as nonlinear diffusion. However, despite wide applicability, little is known about the influence of Laplacian operators, particularly p-Laplacian, on solutions of the Allen–Cahn equation.

Recently, a team of researchers from Korea, including Professor Dongsun Lee from Incheon National University, investigated the dynamics of the p-Laplacian AC (p-AC) equation. The study was specifically aimed at examining how the type of Laplacian influences a solution to the AC equation. This paper was published in Applied Mathematics and Computation.

Explaining the rationale of this study, Prof. Lee says, "We consider three criteria when we

model with phase-field equations. These include the evolution of phase separation, energy dissipation law, and the nonconservation of mass. Our numerical study was revolved around these basic properties of the AC equation."

The researchers first characterized the different morphological changes of numerical solutions under various numerical tests (like phase separation, equilibrium profile, boundedness, total energy dissipation, traveling wave solutions, geometric motions, and comparison of AC equations with different Laplacians). Next, computational tests were employed to analyze the interfacial dynamics of AC equations and p-Laplacian.

The experiments demonstrated that the solutions of the AC equation maintained the three criteria—phase separation, boundedness, and energy decay properties—with the p-Laplacian operator. The researchers also identified that the sharpness of an interface can be adjusted to the pvalues, revealing an advantage of p-AC equation over the classical Laplacian.

Discussing the long-term implications of this study, Prof. Lee says, "With phase modeling and the use of mathematical equations like p-AC, we can identify how cells organize complex biochemical reactions in distinct chemical environments, or in organelles where components diffuse for processes."

For Prof. Lee and his co-author on this study, Prof. Chaeyoung Lee of Korea University, the pursuit of these mathematical models is far from over. Building on these results, the researchers wish to advance the understanding of phase field models by studying biochemical reactions using p-AC equations in the future.

How will AI change mathematics?

人工智能将如何改变数学？

By Davide Castelvecchi

人工智能工具已经开始帮助研究者建立新的理论和解决难题。它们可能进一步撼动数学。

As interest in chatbots spreads like wildfire, mathematicians are beginning to explore how artificial intelligence (AI) could help them to do their work. Whether it's assisting with verifying human-written work or suggesting new ways to solve difficult problems, automation is changing the field in ways that go beyond mere calculation, researchers say.

"We're looking at a very specific question: will machines change math?" says Andrew Granville, a number theorist at the University of Montreal in Canada. A February workshop at the University of California, Los Angeles (UCLA), explored this question, aiming to build bridges between mathematicians and computer scientists. "Most mathematicians are completely unaware of these opportunities," says one of the event's organizers, Marijn Heule, a computer scientist at Carnegie Mellon University in Pittsburgh, Pennsylvania.

Akshay Venkatesh, a 2018 winner of the prestigious Fields Medal who is at the Institute for Advanced Study in Princeton, New Jersey, kick-started a conversation on how computers will change maths at a symposium in his honour last October. Two other recipients of the medal, Timothy Gowers at the Collège de France in Paris and Terence Tao at UCLA, have also taken leading roles in the debate.

"The fact that we have people like Fields medallists and other very famous big-shot mathematicians interested in the area now is an indication that it's 'hot' in a way that it didn't used to be," says Kevin Buzzard, a mathematician at Imperial College London.

AI approaches

Part of the discussion concerns what kind of automation tools will be most useful. AI comes in two major flavours. In 'symbolic' AI, programmers embed rules of logic or calculation

into their code. “It’s what people would call ‘good old-fashioned AI’,” says Leonardo de Moura, a computer scientist at Microsoft Research in Redmond, Washington.

The other approach, which has become extremely successful in the past decade or so, is based on artificial neural networks. In this type of AI, the computer starts more or less from a clean slate and learns patterns by digesting large amounts of data. This is called machine learning, and it is the basis of ‘large language models’ (including chatbots such as ChatGPT), as well as the systems that can beat human players at complex games or predict how proteins fold. Whereas symbolic AI is inherently rigorous, neural networks can only make statistical guesses, and their operations are often mysterious.

De Moura helped symbolic AI to score some early mathematical successes by creating a system called Lean. This interactive software tool forces researchers to write out each logical step of a problem, down to the most basic details, and ensures that the maths is correct. Two years ago, a team of mathematicians succeeded in translating an important but impenetrable proof — one so complicated that even its author was unsure of it — into Lean, thereby confirming that it was correct.

The researchers say the process helped them to understand the proof, and even to find ways to simplify it. “I think this is even more exciting than checking the correctness,” de Moura says.

As well as making solitary work easier, this sort of ‘proof assistant’ could change how mathematicians work together by eliminating what de Moura calls a “trust bottleneck”. “When we are collaborating, I may not trust what you are doing. But a proof assistant shows your collaborators that they can trust your part of the work.”

Sophisticated autocomplete

At the other extreme are chatbot-esque, neural-network-based large language models. At Google in Mountain View, California, former physicist Ethan Dyer and his team have developed a chatbot called Minerva, which specializes in solving maths problems. At heart, Minerva is a very sophisticated version of the autocomplete function on messaging apps: by training on maths papers in the arXiv repository, it has learnt to write down step-by-step

solutions to problems in the same way that some apps can predict words and phrases. Unlike Lean, which communicates using something similar to computer code, Minerva takes questions and writes answers in conversational English. “It is an achievement to solve some of these problems automatically,” says de Moura.

Minerva shows both the power and the possible limitations of this approach. For example, it can accurately factor integer numbers into primes — numbers that can’t be divided evenly into smaller ones. But it starts making mistakes once the numbers exceed a certain size, showing that it has not ‘understood’ the general procedure.

Still, Minerva’s neural network seems to be able to acquire some general techniques, as opposed to just statistical patterns, and the Google team is trying to understand how it does that. “Ultimately, we’d like a model that you can brainstorm with,” Dyer says. He says it could also be useful for non-mathematicians who need to extract information from the specialized literature. Further extensions will expand Minerva’s skills by studying textbooks and interfacing with dedicated maths software.

Dyer says the motivation behind the Minerva project was to see how far the machine-learning approach could be pushed; a powerful automated tool to help mathematicians might end up combining symbolic AI techniques with neural networks.

Maths v. machines

In the longer term, will programs remain part of the supporting cast, or will they be able to conduct mathematical research independently? AI might get better at producing correct mathematical statements and proofs, but some researchers worry that most of those would be uninteresting or impossible to understand. At the October symposium, Gowers said that there might be ways of teaching a computer some objective criteria for mathematical relevance, such as whether a small statement can embody many special cases or even form a bridge between different subfields of maths. “In order to get good at proving theorems, computers will have to judge what is interesting and worth proving,” he said. If they can do that, the future of humans in the field looks uncertain.

Computer scientist Erika Abraham at RWTH Aachen University in Germany is more

sanguine about the future of mathematicians. “An AI system is only as smart as we program it to be,” she says. “The intelligence is not in the computer; the intelligence is in the programmer or trainer.”

Melanie Mitchell, a computer scientist and cognitive scientist at the Santa Fe Institute in New Mexico, says that mathematicians’ jobs will be safe until a major shortcoming of AI is fixed — its inability to extract abstract concepts from concrete information. “While AI systems might be able to prove theorems, it’s much harder to come up with interesting mathematical abstractions that give rise to the theorems in the first place.”

The Steklov Mathematical Institute

俄罗斯科学院斯捷克洛夫数学研究所简介

By V. V. Kozlov（写于 2009 年）

斯捷克洛夫数学研究所于 1934 年 4 月 24 日列宁格勒的苏联科学院大会决议成立。研究所以弗拉基米尔·安德烈耶维奇·斯捷克洛夫命名。第一任所长为伊万·维诺格拉多夫。

1940 年研究所迁到莫斯科，但前建筑物作了它的列宁格勒分所，现在已经分离为俄罗斯科学院斯捷克洛夫数学研究所圣彼得堡分所，位于俄罗斯圣彼得堡。

When thinking out my talk, I could see again and again what a large-scale phenomenon the Steklov Mathematical Institute is. This is my belief, and I would like to share it with the readers.

Rephrasing Newton, we can boldly say that the Steklov Institute stands on the shoulders of giants. I would like to start my talk by recalling our great predecessors.

Studies in mathematics as such started in Russia the year after a decree by Peter I establishing the Academy of Sciences. Two Bernoulli brothers, Nicholas and Daniel, were offered positions in St. Petersburg. They were very young at the time: Nicholas, the elder, was 30 and Daniel was 25. The history of their invitation is as follows. Peter had been discussing details of his plan to organize an academy of sciences with Leibniz. Johann Bernoulli, the father of Nicholas and Daniel, was one of Leibniz's favourite disciples. He held a good position in Basel, so only representatives of the next generation of the Bernoulli family could be invited. A question went to St. Petersburg as to who it would be better to invite, Nicholas or Daniel. Finally, Lavrenty Blumentrost, the president of the Academy of Sciences, invited both.

In 1725 Nicholas Bernoulli took the chair of mathematics, and Daniel was offered the chair of physiology (although his brother Nicholas had educated him also as a professional mathematician). The Academy expenses on these outstanding researchers amounted to 4% of its total budget. By the way, mathematicians were the most highly paid at that time:

Nicholas the mathematician got 1000 rubles for a year, while Daniel, the physiologist, got 800 rubles. I think this a tradition to bear in mind.

In 1726 Nicholas Bernoulli passed away and Daniel took his chair. He worked 8 years at the Academy, after which he returned to Basel. During these 8 years Daniel Bernoulli published 47 research papers in periodicals of the St. Petersburg Academy, 6 papers a year — a good example for all of us. He prepared the first monograph on hydrodynamics, which became very famous when it was subsequently published. Among other things, one of his organizational accomplishments was also very important: he pressed for Leonhard Euler to be invited to the Academy.

Daniel Bernoulli was more a mathematical physicist than a 'pure' mathematician. (Incidentally, upon returning to Basel he took the chair of experimental physics.) In a letter to Euler he once wrote that it might be better for physics as such if there were no mathematics (in fact, this was his harsh reaction to d'Alembert's works in physics, which he did not think highly of).

Euler arrived in St. Petersburg in 1727 (the same year when Newton died). He was then a young man of 19. For 14 years he worked at the St. Petersburg Academy and for 25 years after that at the Berlin Academy of Sciences. After long negotiations the St. Petersburg Academy was able to lure him back, and he worked there the last 17 years of his life (and was buried in St. Petersburg). Astonishingly, his productivity only grew with time: Euler published 50 papers in the first 14 years, while during the last 17 years, though almost blind, he dictated 400 research papers. For quite a few years after Euler's death, journals of the St. Petersburg Academy were overflowing with his posthumous publications. Euler's works gave an enormous impetus to the development of mathematics in general, and especially in Russia.

After Euler there were many outstanding mathematicians of world renown at the Academy of Sciences. For instance, we can remember Academicians M. V. Ostrogradskii and O. I. Somov. Ostrogradskii received his mathematical education in Europe, and it is worth mentioning that a considerable part of his work in mathematics involved developing and generalizing ideas of foreign authors. He put much effort into teaching at engineering and military schools. Among his students were I. A. Vyshnegradskii (a pioneer of control

systems engineering) and N.P. Petrov (the author of hydraulic lubrication theory).

However, the founding of the St. Petersburg school of mathematics is with good reason ascribed to Pafnutii L'vovich Chebyshev, who as a very young man (an adjunct professor of mathematics) took a very active part in editing and publishing Euler's works. I must say that this was a powerful incentive for his own investigations, especially in number theory. In particular, Chebyshev obtained an outstanding result on the limiting distribution of the number of primes not exceeding a fixed bound. His slightly odd aversion to complex numbers did not allow him to provide a formal proof of the existence of the desired asymptotic espression. He is the author of classical results in probability theory and the founder of the modern theory of polynomial approximation: it is sufficient to mention the Chebyshev polynomials of least deviation from zero. His theory of webs is well known in geometry. Its creation was prompted by the quite real-life problem of cutting out clothing. His contribution to the theory of machines and mechanisms was great. He himself designed many original mechanisms, some of which have survived to this day. It is worth mentioning that Chebyshev's theory of approximation by polynomials was developed in connection with the problem of an optimal choice of the parameters of approximate inversors which are four-rod mechanical linkages.

Chebyshev loved to teach and till the end of his life gave lectures at St. Petersburg University, which enabled him to found an outstanding school. Such renowned mathematicians as E. I. Zolotarev, A. N. Korkin, G. F. Voronoi, D. A. Grave, and many others were among his students. Two of them, Andrei Andreevich Markov and Aleksandr Mikhailovich Lyapunov, played a significant part in the development of mathematics within the Academy of Sciences,

Academician Markov was Chebyshev's immediate successor in mathematics. He brought glory to Russian mathematics by introducing so-called Markov processes. There are an enormous number of publications concerned with Markov processes. Such processes are very important for probability theory and mathematical statistics, but also for applications to physics, biology, and so on.

To say that Academician Lyapunov was a genius is not too strong an assertion. He worked all his life on a problem posed by Chebyshev (and did solve it eventually!): the problem of

the existence and stability of figures of equilibrium of a rotating fluid. In its complexity it is not in the least easier than the Millennium Prize Problems in the famous list of the Clay Institute. By the way, of the five volumes of Lyapunov's works published by the USSR Academy of Sciences in the 1960s, the bulky texts relating to the Chebyshev problem occupy three volumes. I think that only a few of Lyapunov's ideas and methods used in this problem have actually been assimilated and incorporated into the tool kit of contemporary mathematics. In the process of solving the Chebyshev problem Lyapunov made plenty of discoveries. In particular, he developed a general theory of stability of motion which is not only a cornerstone of theoretical mechanics, but also underlies the design of mechanisms and machines in engineering.

Lyapunov obtained fundamental results in potential theory and probability theory. In particular, he indicated very general conditions ensuring that the central limit theorem holds for sums of independent random variables. To this end he introduced the characteristic function of a probability distribution and developed a theory of such functions which has long been a classical part of probability theory. Markov was 'upset' by Lyapunov's unexpected success, since he himself had been working in this direction, striving to establish a result of this kind using the real-valued method of moments due to his great teacher. He thought about this question for almost 10 years and finally was able to prove the central limit theorem by the method of moments under the same assumptions as Lyapunov.

Lyapunov had only one disciple, Vladimir Andreevich Steklov. As a student at Kharkov University, Steklov attended lectures of the young private docent Lyapunov. He was only six years younger than his teacher. At first, Lyapunov focused him on theoretical problems of hydrodynamics, and in particular on the problem of the motion of a rigid body in a fluid. In trying to solve the problem (posed by Lyapunov) of classifying all the cases when the equations of motion admit an additional first integral in the form of a homogeneous quadratic form, Steklov found a new integrable case. This important result, which supplemented the classical investigations of Kirchhof and Clebsch, was the core of Steklov's Master's thesis. However, Lyapunov soon found a gap in Steklov's calculations and pointed out another integrable case. In fact, Steklov's and Lyapunov's cases are mutually dual: either of these two first integrals can be taken as the kinetic energy of the system 'body + fluid'; then the other quadratic form will be a first integral of the equations of motion.

After that, Steklov switched to more general problems connected with equations of mathematical physics, partial differential equations, and with the area now usually regarded as functional analysis. In 1902 he defended his doctoral thesis “General methods of solution of the main problems of mathematical physics” and the same year was elected a corresponding member of the St. Petersburg Academy of Sciences. In 1912 he became a full member, in 1916 was elected a member of the Governing Board of the Academy, and in 1919, at the height of the Civil War, was named a vice-president of the Academy. He was the only vice-president at that time and had to manage all the economic problems of the Academy, publishing, and many other issues.

I must say that Steklov was quite loyal to the Soviet government, which was noticed and valued. He met with V. I. Lenin on several occasions. The first meeting was arranged by Maxim Gorky. It should be mentioned that Steklov made a favourable impression on Lenin and used this very smartly for the good of the Academy. It was thanks to his efforts that the St. Petersburg Academy of Sciences was smoothly transformed into a new institution, the Academy of Sciences of the USSR.

In 1921, on the initiative of Academicians Steklov, A. F. Ioffe, and A. N. Krylov, the Physico-Mathematical Institute was created on the basis of the Mathematical Cabinet founded by Steklov in 1919 (which bore the names of Chebyshev and Lyapunov), the Laboratory of Physics established by Academician P.P. Lazarev in 1912, and the Seismic Station of the Academy. The mathematics division of the institute consisted of the eminent scholars S. N. Bernstein, I. M. Vinogradov, A. O. Gel’fond, N. E. Kochin, A. N. Krylov, M. A. Lavrent’ev, N. N. Luzin, L. A. Lyusternik, P. S. Novikov, S. L. Sobolev, D. K. Faddeev, V. A. Fock, and L. G. Schnirelmann.

Steklov died in 1926, and the Physico-Mathematical Institute was given his name. After him, the physicist A. F. Ioffe, the mechanician A. N. Krylov, and the mathematician I. M. Vinogradov were the directors. On 28 April 1934 the institute was divided into two parts, the Physical and the Mathematical Institutes, and Ivan Matveevich Vinogradov became the director of the Mathematical Institute. He headed it (with a break) for 45 years, a unique case in the history of the Academy of Sciences. Initially the institute was housed in the building of the Krzhizhanovskii Power Engineering Institute (the present address is 19

Leninskii Prospekt).

I shall now list some outstanding achievements of the Steklov Institute, grouping them according to areas of mathematics. But I must make two remarks. First, I include in the list works of our colleagues from the St. Petersburg Department of the Steklov Mathematical Institute. Second, some persons that I shall mention are occasionally associated with other institutions (most often, Moscow State University). This is hardly surprising, because these persons held several positions at the same time. For instance, A. N. Kolmogorov is usually associated with the Faculty of Mechanics and Mathematics of Moscow University. But in fact, before World War II and during the war he worked at the Steklov Institute. Later, when Khrushchev prohibited the practice of holding several positions, Kolmogorov decided for Moscow State University. In his memoirs he wrote that he had later thought about that decision many times and believed that he had made a mistake: by staying at the Mathematical Institute he could perhaps have exerted a much greater influence on the mathematical life in this country. Nevertheless, towards the end of his life Kolmogorov returned to a full-time position at the Steklov Institute while also holding a (part-time) position as head of a department at Moscow State University.

I now turn to the brightest achievements of our researchers.

In *number theory* results of Vinogradov and Yu. V. Linnik (Leningrad) are well known. They proved the so-called ternary Goldbach conjecture. This was a very difficult problem of additive number theory (each odd integer is a sum of three primes). Before that, L. G. Schnirelmann, using his concept of the density of sets of positive integers, had managed to prove a weaker version of this result: each positive integer is a sum of some bounded number of primes. Schnirelmann was a brilliant and many-sided mathematician; at the age of 28 he became a corresponding member of the Academy of Sciences of the USSR. He was only 33 when he committed suicide under (officially) undisclosed circumstances. The Department of Number Theory included also such well-known experts as A. A. Karatsuba, N. M. Korobov, S. M. Voronin, and A. G. Postnikov. A. O. Gel’fond solved Hilbert’s 7th problem on transcendental numbers. Recall that at the beginning of the 20th century Hilbert stated 23 problems which he regarded as key questions for the development of mathematics. Solving any of them is considered a great achievement. Anticipating slightly, I can say that six problems from Hilbert’s list were solved in the Mathematical Institute or its St.

Petersburg Department. I do not think any other research institution can boast of such a result.

On the other hand, I would like to say that although solving particular, perhaps very difficult, problems is certainly important for mathematics, it is my belief that its alliance with physics and mechanics means much more for its development.

I now proceed to *algebra and algebraic geometry*. Academician I. R. Shafarefich founded the Moscow school of algebraic geometry. He himself discovered the general reciprocity law. Two of his students, corresponding members of the Russian Academy of Sciences (RAS) Yu. N. Manin and V. A. Iskovskikh, solved the Luroth problem on the non-rationality of threefold quadrics. In various periods the department of algebra included N. G. Chebotarev, A. I. Mal'tsev, D.K. Faddeev, A. N. Tyurin, A. G. Kurosh, and A. I. Kostrikin.

B. N. Delauney, P. S. Alexandroff, L. S. Pontryagin, L. V. Keldysh, A. D. Aleksandrov, V. A. Rokhlin, M. M. Postnikov, L. A. Lyusternik, and L. G. Schnirelmann worked in geometry and topology.

Academician S.P. Novikov is now the head of the Department of *Geometry and Topology* at the Mathematical Institute. As a young man, Novikov proved the topological invariance of rational Pontryagin classes. For this and several other results he became the first Russian mathematician to be awarded the Fields Medal, the highest international honour for mathematicians. Lyusternik and Schnirelmann solved the Poincar ́e problem on the existence of three closed disjoint geodesics on each Riemannian sphere. To this end they introduced a new topological invariant, the category of a topological space. Now the staff of this department also includes Academicians V. I. Arnold and V. A. Vassiliev, famous for their work in catastrophe theory.

A constellation of eminent experts in *differential equations* have been working at the Steklov Mathematical Institute. It suffices to recall Pontryagin's discovery of the maximum principle, the cornerstone of the mathematical theory of optimal control. E. F. Mishchenko, R. V. Gamkrelidze, and V. G. Boltyanskii participated in developing and substantiating this principle. Deep results in differential game theory and its applications are due to Yu. S. Osipov and A. V. Kurzhanskii. Academician D. V. Anosov is the creator of the hyperbolic

theory of dynamical systems, a mathematical theory of deterministic chaos very popular with physicists and chemists. Academician A. A. Bolibrukh solved one of Hilbert's problems, related to so-called Fuchsian equations. Incidentally, for a long time this problem had been regarded as solved in the affirmative, and Bolibrukh not only constructed a counterexample, but also found a criterion ensuring that Hilbert's conjecture nevertheless holds. S. L. Sobolev developed a theory of generalized functions (Sobolev spaces). O. A. Ladyzhenskaya (in conjunction with N. N. Ural'tseva) completed the solution of Hilbert's 19th and 20th problems on the analyticity of solutions of partial differential equations of elliptic type. Academician V. I. Smirnov worked fruitfully in differential equations and mathematical physics. By the way, he was a student of V. A. Steklov himself.

In *probability theory and mathematical statistics* the school of Academician Kolmogorov achieved world fame. It is now led by Academician Yu. V. Prokhorov. Among outstanding results we point out the modern axiomatics of probability theory constructed by Kolmogorov (Hilbert's 6th problem) and the law of the iterated logarithm discovered by A.Ya. Khintchine. For the development of mathematical statistics the work of N. V. Smirnov and L. N. Bol'shev, corresponding members of the Academy, was of great importance. The St. Petersburg school of probability theory and ergodic theory is led by Academician I. A. Ibragimov.

Many brilliant mathematicians have worked in the Department of Complex Analysis of the Mathematical Institute. One of them, S. N. Mergelyan, became a corresponding member of the RAS at the age of 25. I must point out that the theory of functions of complex variables is very important for mechanics, particularly in planar hydrodynamics and elasticity problems. It comes as little surprise therefore that M. V. Keldysh and M. A. Lavrent'ev, besides other areas, did much work on problems of mechanics. G. M. Goluzin and A. F. Leont'ev also worked in the Department of Complex Analysis. The current staff members of the department represent the schools of Academicians A. G. Vitushkin and A. A. Gonchar.

The *theory of functions* is an area where N. N. Luzin, one of the founders of the Moscow school of mathematics (also known as 'Luzitania'), worked very fruitfully. S. M. Nikol'skii, who turned 104 on 30 April 2009, has been working in the Department of the Theory of Functions for more than half a century. As an academician, he is a member of the institute's

Academic Council, and I know of no occasion when he has missed a meeting of the council. Outstanding results in the theory of functions are due to S. N. Bernstein, D. E. Men'shov, V. I. Smirnov, and S. B. Stechkin. And here we should not forget about Kolmogorov and Arnold, who solved Hilbert's 13th problem on superposition of continuous functions.

Functional analysis at the Mathematical Institute was developed by its pioneers I. M. Gelfand (now living in the US), M. A. Naimark, and A. I. Plesner.

As regards *mathematical logic*, our successes here are unquestionable. Academicians P. S. Novikov and S. I. Adian solved the famous Burnside problem, and Yu. V. Matiyasevich solved Hilbert's 10th problem on the algorithmic unsolvability of Diophantine equations. Results of A. A. Markov and N. A. Shanin on the theory of algorithms and constructive mathematics are well known.

An entire constellation of names in *applied mathematics* includes M. V. Keldysh, Ya. B. Zel'dovich, L. A. Lyusternik, L. V. Kantorovich (Nobel Prize in economics), A. A. Lyapunov (a pioneer of Russian cybernetics) K. A. Semendyaev, K. K. Mardzhanishvili, A. A. Dorodnitsyn, A. N. Tychonoff, S. K. Godunov, K. I. Babenko, and N. N. Yanenko. The story of their achievements would require a separate article.

In *theoretical and mathematical physics* a high level of research was set by Academician V. A. Fock, who was one of the founders of quantum field theory (Fock spaces). N. N. Bogolyubov, who worked in our institute for a long time, created the microscopic theory of superconductivity and superfluidity. L. D. Faddeev solved the inverse scattering problem for the three-dimensional Schr¨odinger equation. He is one of the pioneers of the quantum theory of gauge fields. The names of our famous scientists M. K. Polivanov, V. S. Vladimirov, D. V. Shirkov, and A. A. Slavnov are connected with this area.

Mechanics at the Mathematical Institute is represented by brilliant researchers: N. E. Kochin, P.Ya. Kochina, N. I. Muskhelishvili, S. A. Khristianovich, L. I. Sedov, D. E. Okhotsimskii, V.P. Korobeinikov, and A. G. Kulikovskii. M. V. Keldysh created a mathematical model of flutter. Kochin proposed a mathematical model for zonal circulation of the atmosphere, the existence of which had been in doubt before him. Sedov solved the important strong explosion problem.

During World War II the Mathematical Institute was evacuated to Kazan, though some researchers stayed in Moscow and Leningrad. At this time, Academician S. L. Sobolev became the director of the institute. Five of our colleagues, including Academicians V. S. Vladimirov and E. F. Mishchenko, took part in combat.

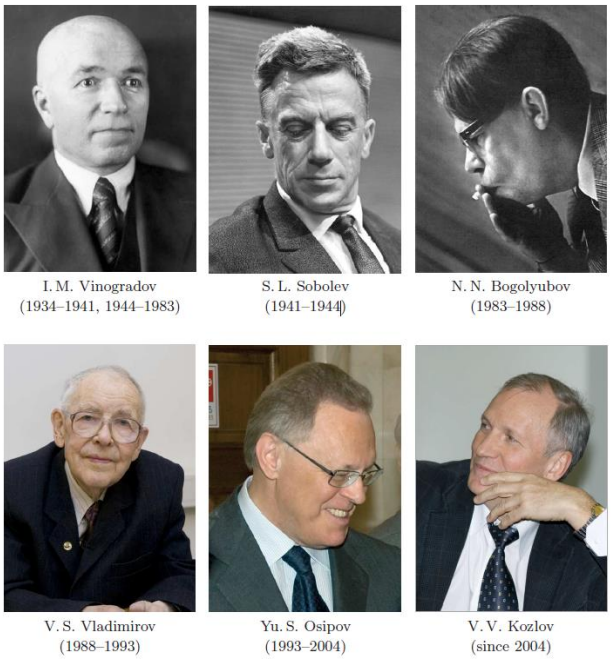
Not just during the war years but also before the war, researchers from the Mathematical Institute investigated subjects of defense value. A. N. Kolmogorov and N. V. Smirnov developed a theory of gunnery; S. L. Sobolev, M. V. Keldysh, and A. A. Markov carried out calculations on the motion of projectiles; I. M. Gelfand and L. A. Lyusternik designed tables for determining the parameters of aircraft flight; S. N. Bernstein developed a method for radio direction finding of ships. In particular, I should point out A. O. Gel'fond's work in cryptography, encoding and decoding secret messages. He worked at the Navy General Staff and did very much at a practical level. By the way, this subject is now also being developed at our institute, on a modern theoretical and practical foundation.

Many of our scientists took part at the Atomic Project. N. N. Bogolyubov, V. S. Vladimirov and Ya. B. Zel'dovich developed nuclear weaponry at Arzamas-16; S. L. Sobolev and S. A. Khristianovich solved the problem of gas diffusion separation of uranium isotopes at Laboratory no. 2, headed by I. K. Kikoin. I. M. Gelfand, A. A. Dorodnitsyn, A. N. Tychonoff, and N. N. Yanenko worked on some problems related to the Atomic Project in the Department of Applied Mathematics of the Mathematical Institute, headed by Academician M. V. Keldysh. M. A. Lavrent'ev, I. G. Petrovskii, L. I. Sedov, K. A. Semendyaev, and V. A. Fock also carried out research connected with the Atomic Project.

The Mathematical Institute has never been especially large; the total number of its researchers has not exceeded 150. However, quite a few research institutes have been organized by separating them off from our institute at one time or another. In 1939 the Institute of Mechanics of the USSR Academy of Sciences (now the Ishlinskii Institute of Problems of Mechanics of the RAS) was organized on the basis of the Department of Continuum Mechanics; in 1940 the Leningrad (now St. Petersburg) Department of the Steklov Mathematical Institute was formed; in 1948 the Institute of Precision Mechanics and Computer Engineering of the USSR Academy of Sciences was organized on the basis of the Department of Approximate Calculations (subsequently, the present Dorodnitsyn

Computing Centre of the RAS was split off from that institute); in 1956 the Sverdlovsk Department of the Steklov Mathematical Institute was founded, initially headed by our colleague S. B. Stechkin (this is now the Institute of Mechanics and Mathematics of the Ural Branch of the RAS); in 1957, on the initiative of M. V. Keldysh, the Institute of Applied Mathematics was organized (and now bears his name).

The process of organizing the Siberian Branch of the Academy of Sciences was begun in 1957 on the initiative of Academicians M. A. Lavrent'ev, S. L. Sobolev, and S. A. Khristianovich. Lavrent'ev became the first chairman of the Siberian Branch. Among the institutes that emerged as part of the Siberian Branch were the Institute of Mathematics (now bearing Sobolev's name), the Institute of Hydrodynamics (now carrying the name of Lavrent'ev), and the Institute of Theoretical and Applied Mechanics (now named after Khristianovich).



Directors of the Mathematical Institute

In 1983 Vinogradov died. He was succeeded as director by N. N. Bogolyubov (1983–1988) and then V. S. Vladimirov (1988–1993). The 1990s was a period of trials for our institute, which were the lot of Yu. S. Osipov, the president of the Academy, who headed the institute from 1993 through 2004. During this period 30 researchers left the institute, either taking positions abroad or shifting to business structures. Nonetheless, even in this complicated period much was done. One of the main achievements then was that the project of constructing a new building for the Mathematical Institute was realized, based on a decision of the Politburo of the Central Committee of the Communist Party on development of the mathematical sciences in our country. The construction work of 1994–1996 was supervised by the chief engineer of the Steklov Institute, B. A. Balagurov. The new building hosts also the Institute for Numerical Mathematics, the offices of Russian mathematical journals, and an excellent mathematics library, which is a branch of the

Library of Natural Sciences of the RAS. Our library is a proud holder of the personal libraries of Steklov, Lyapunov, Markov, Luzin and other prominent mathematicians, who bequeathed them to the institute.

What is the Mathematical Institute these days?

It has 12 departments with 115 research fellows. Our staff includes 88 Doctors of the Sciences and 31 Ph.D.'s. (Although 88 and 31 total more than 115, there is no contradiction, because several of these colleagues hold no-research positions.) The staff of the institute includes 15 academicians and 15 corresponding members of the RAS, not counting ones having full-time positions at other institutions. On the average, a researcher publishes 2.2–2.3 papers a year. These are theoretical papers written without collaborators, so this is not bad at all. However, in number of publications we lag behind Daniel Bernoulli.

Unfortunately, the age distribution of our staff is not a thing we can boast of. Quite a half the researchers are older than 60. Aging of research staff is a common problem throughout the Academy. But in 2008 we were able to hire five new researchers, four of them young and with brilliant prospects.

One of our important achievements is the Research and Education Centre established four years ago and headed by D. V. Treshchev, a corresponding member of the RAS. The centre organizes lectures and seminars for students. In three years more than 60 lecture courses have been given, attended by more than 200 students from the Faculty of Mechanics and Mathematics and the Faculty of Physics of Moscow State University, the Moscow Institute for Physics and Technology, and some other institutions of higher education. This enabled us to double to 18 the number of our postgraduate students. I do not think this number is quite up to our potentials: we could take more.

Every year the Mathematical Institute holds 8–10 conferences, including international ones. In June of 2009 we held an international conference in Moscow and St. Petersburg dedicated to the 75th anniversary of the institute. The All-Institute Research Seminar works on a permanent basis, and is attended by many our colleagues from the whole of Moscow. We make video records of talks at this seminar, which are available on the web. I must say that this is an effective method of popularizing our work.

In 1992 the Mathematical Institute organized an access hub to electronic mail for its staff, the first stone in a gradually constructed building of a communications network for the Academy of Sciences. In 1995, with the help of the Russian Foundation for Basic Research, we organized the Southern Moscow Backbone, from which the development of the Internet in Moscow actually started. N. N. Repin, a research fellow from the Steklov Institute, became the director of the SMB project. The local network in the new building of the Mathematical Institute was designed in accordance with the highest standards of the time of its construction (it was one of the five best Russian networks and one of the leading 100 worldwide). The institute network matches high international requirements also today. More than 20 institutes of the Academy of Sciences are connected with the World Wide Web via the Steklov Institute.

Four volumes of the *Trudy Matematicheskogo Instituta* (Proceedings of the Mathematical Institute; E. F. Mishchenko as editor-in-chief) are published every year. With its own money the institute publishes limited editions of two serials: *Sovremennye Problemy Matematiki* (Current Problems of Mathematics; executive editor A. G. Sergeev) and *Lektsionnye Kursy Nauchno-Obrazovatel'nogo Tsentra* (Lecture Notes of the Research and Education Centre; executive editor D. V. Treshchev). We have already published 12 issues of *Sovremennye Problemy Matematiki* and 11 issues of *Lektsionnye Kursy Nauchno-Obrazovatel'nogo Tsentra*.

The Mathematical Institute is a co-founder of eight leading mathematical journals: *Uspekhi Matematicheskikh Nauk*, *Matematicheskii Sbornik*, *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, *Funktsional'nyi Analiz i ego Prilozheniya*, *Teoreticheskaya i Matematicheskaya Fizika*, *Matematicheskie Zametki*, *Teoriya Veroyatnostei i ee Primeneniya*, *Diskretnaya Matematika*.

On the basis of the Steklov Mathematical Institute we have developed the All-Russia mathematical portal Math-Net.Ru. The main aim of this project is to develop an up-to-date information system and facilitate access of the Russian and international scientific community to Russian mathematical resources via the Internet. The main section of the portal is a database of publications in Russian mathematical journals. Whether there is free access to the full texts of papers depends on the policies of their publishers. Other databases

on the portal include:

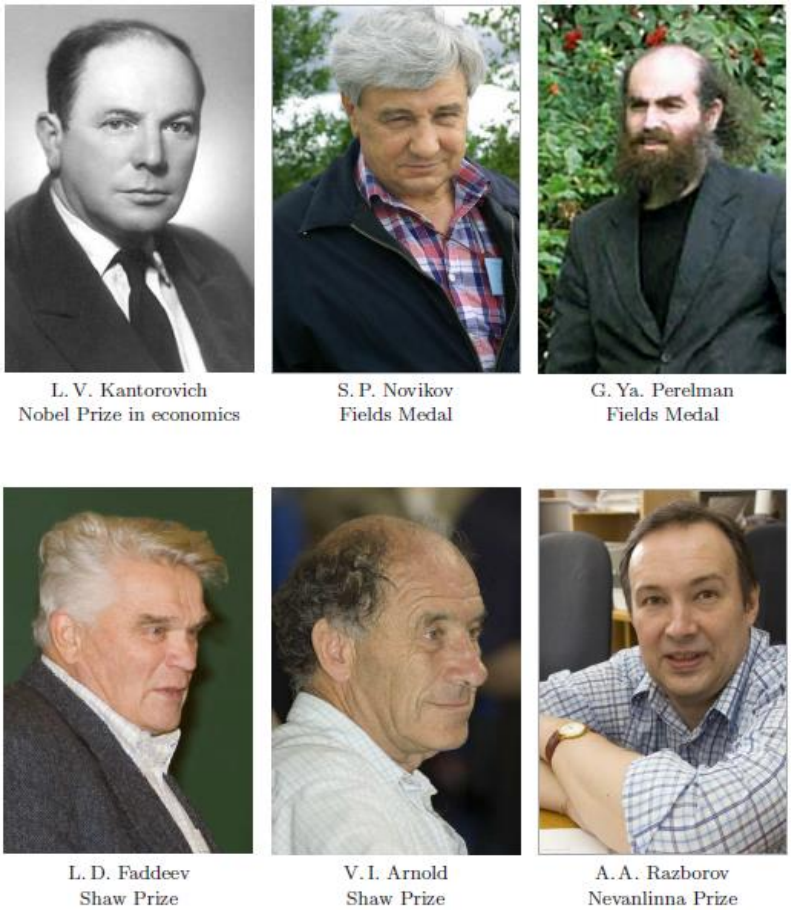
- Persons (Russian and foreign authors, including the authors of the papers represented on the portal);
- Institutions (mathematical institutions or divisions of more general institutions);
- Conferences (academic conferences, schools, seminars);
- Videos (a videotheque of lectures and talks by Russian and foreign mathematicians).

The number of visitors to the portal is constantly growing. On the average we have more than 3500 visits a day. About 60% of the visitors come from Russia and 40% are from abroad (half of them from outside the former Soviet Union). The Internet address of the portal is http://www.mathnet.ru/.

The work of the Steklov Mathematical Institute has been honoured by high state awards: the Order of Lenin in 1967 and the Order of the October Revolution in 1984.

Its staff included M. V. Keldysh, thrice Hero of Socialist Labour, N. N. Bogolyubov and I. M. Vinogradov, twice Heroes of Socialist Labour, and 15 of our colleagues were honoured with the title of Hero of Socialist Labour. Here we have counted only those who received this title while working at the Steklov Institute, but if we also take account of those honoured subsequently, then 29 Heroes of Socialist Labour have worked at the Mathematical Institute. Our researchers received 32 Lenin Prizes and 93 State Prizes of the USSR and the Russian Federation. L. D. Faddeev (2004) and V. I. Arnold (2007) were laureates of the State Prize of the Russian Federation. Given the number of staff, these are impressive figures! Our colleagues were awarded 15 Gold Medals of the Russian Academy of Sciences, and five of them received the Lomonosov Grand Gold Medal.

In 2009 the first Prizes for Young Researchers of the President of the Russian Federation were awarded. The list of the first four recipients contains our colleague, D.Sc. A. G. Kuznetsov. The Mathematical Institute can boast of a Nobel Prize winner, Academician L. V. Kantorovich, who received the Nobel Prize in economics. G. I. Perelman, now known to any man in the street, was awarded the Fields Medal while he was a researcher at the St. Petersburg Department of the Institute.



Laureates of international prizes from the Steklov Mathematical Institute and the St. Petersburg Department of the Mathematical Institute

Such is the history of the Steklov Mathematical Institute, steeped in great traditions. I think that also now the institute is in a quite decent state, although of course, this does not mean there are no problems. Of problems there are plenty, in the Academy as a whole and in each of its institutes.

We have set the goal of making our institute a real international mathematical centre. Much has been done in this direction. For instance, the Euler International Mathematical Institute in St. Petersburg works very fruitfully. In 2007, when we celebrated the 300th anniversary of Euler, his sculpted bust put before the building of the Euler Institute became the first monument in his honour in Russia. We would also like to have a similar international mathematical institute in Moscow. Our plans include further development of the Research and Education Centre, which helps us entice ever growing numbers of talented young mathematicians to the sphere of influence of our institute. This is where our future lies.

Translated by N. KRUZHILI

華中科技大学数学中心
Center for Mathematical Sciences

Wuhan, China

Web: mathcenter.hust.edu.cn E-mail: mathcenter@hust.edu.cn

数学正在发生日新月异的变化。不仅数学内部各分支相互交融，共同推动数学向更高层次发展，而且科学与工程问题牵涉到越来越深的数学课题，对数学提出了重大挑战，激发了新的数学理论和方法的创立，从而推动数学本身的发展。数学也一直在背后推动着科学和工程技术的进步，为现代科学和高新技术的发展奠定坚实基础。世界强国必须是数学强国，数学弱国不可能是现代化强国，而现代高科技竞争同时包含数学研究的竞争。华中科技大学数学中心顺应科学发展趋势于2013年在武汉成立了。

数学中心宗旨

（1）积极倡导数学不同分支之间的交叉研究；激发新的合作探索，催生新的研究领域和研究群体；

（2）努力推动数学与科学，工程，医学之间的交叉研究；建立数学家和科学家之间的广泛联系，从而达到合作共赢；

（3）聚集一流人才，培养优秀学生，做出一流学术研究，引领学科发展，服务国家和社会。

数学中心成员

数学中心已有来自世界各国的优秀学者，包括院士，教授，副教授/副研究员，助理教授，客座教授、访问学者，博士后以及博士研究生。他们从国内外（包括美国、英国、法国、德国、澳大利亚等国家）汇聚到美丽的江城武汉东湖之滨，共同致力于基础数学，计算与应用数学，概率与统计，数据科学，数学物理与交叉科学的发展。

数学中心诚聘海内外英才

无论您来自哪里，数学是我们的共同语言，欢迎您加入我们！

数学中心招聘网址：

https://www.mathjobs.org/jobs/list/ 16913

申请材料请寄段金桥老师：

mathcenter@hust.edu.cn

数学中心招聘二维码

華中科技大學数学中心
Center for Mathematical Sciences
Web: mathcenter.hust.edu.cn E-mail: mathcenter@hust.edu.cn

华中科技大学数学中心招收2024年免推硕士研究生

华中科技大学数学中心招收2024年秋季入学免推硕士研究生（面向有免推资格的本科生。本科专业不限）。

招生视频：https://x.eqxiu.com/s/3obeLrBg?eqrcode=1

华中科技大学数学中心网站：http://mathcenter.hust.edu.cn

研究领域：包括随机动力系统，随机偏微分方程，随机分析，动力系统及其应用，几何与拓扑，偏微分方程，计算数学，应用数学，图像科学，数据科学与统计学，多尺度系统建模与计算模拟，数理地球科学和定量生物学，脑科学与金融数学的应用等。研究生指导团队实行双导师制，由本校专家和海外学者组成，包括院士，国家特聘专家，长江学者，青年学术英才，东湖讲座教授，楚天学者，优青，洪堡学者和华中学者。

数学中心已有来自世界各国的优秀学者，包括教授，副教授，研究员，副研究员，助理教授，客座教授、访问学者，博士后以及博士研究生。他们分别从美国、英国、法国、德国、澳大利亚等国家汇聚到美丽的江城武汉，在东湖之滨研究，学习与合作交流，共同致力于概率与统计，计算与应用数学，基础数学的发展。

欢迎有意愿的学生联系华中科技大学数学中心段金桥主任

（电邮：mathcenter@hust.edu.cn.）

欢迎加盟华中科技大学数学中心！

数学中心网址　　招生视频

地址：中国武汉珞喻路1037号
华中科技大学创新研究院(恩明楼)8楼
邮编：430074
电邮：mathcenter@hust.edu.cn
网页：mathcenter.hust.edu.cn

8th Floor of Enming Building
1037 Luoyu Road, Wuhan, China
Postal Code: 430074
E-mail: mathcenter@hust. edu.cn

内部刊物/免费交流