天元数学国际交流中心

指数和：理论、计算及应用（2025.11.17–21）

我们计划于 2025 年 11 月 17 日至 21 日在天元数学国际交流中心举办学术活动，主要面向国内外从事解析数论、代数数论与代数几何、调和分析、加法组合、编码及密码学等领域研究的学者，围绕指数和的理论、计算与应用展开研讨，并鼓励不同背景的研究人员深入开展合作研究。

活动计划安排 13 场学术报告，每场报告约 1 小时。遵照天元中心的活动精神，鼓励大家广泛交流、自由讨论、深入合作，故报告总时长尽量不超过总活动时长的一半。

活动日程：

报到：2025.11.16（周日）

报告：2025.11.17-21

离会：2025.11.21 下午或 22 全天

会场：天元数学国际交流中心　华罗庚报告厅

注意事项：

1. 本次会议得到天元数学国际交流中心（下称中心）资助，参会人员的住宿及餐饮由中心承担，其余费用由参会人员自行承担。
2. 中心安排接送，由中心往返昆明南站或昆明长水机场。
3. 中心离古城镇中心卫生院约 40 分钟行程，离宜良县医人民院约 1 小时行程，离石林彝族自治县人民医院约 1 小时行程。建议适当随时携带一些必备药品。为医疗应急，中心常备蚊虫叮咬药品、999 感冒灵、连花清瘟胶囊、云南白药喷雾剂、创口贴等药品。
4. 其余相关信息可参见中心网站: http://tianyuan.amss.ac.cn/syyj/index.html

组织者：

万大庆（重庆大学）、郗平（西安交通大学）

天元数学国际交流中心

2025.10.29

天元数学国际交流中心

指数和：理论、计算及应用（2025.11.17–21）

报告人：

曹　阳（山东大学）

陈昌昊（安徽大学）

丁治国（湖南师范大学）

冯　涛（浙江大学）

胡昊宇（南京大学）

黄治中（中国科学院数学与系统科学研究院）

刘博辰（南方科技大学）

万大庆（重庆大学）

王安宇（清华大学）

许大昕（中国科学院数学与系统科学研究院）

张鼎新（上海数学与交叉学科研究院）

张　扬（西安交通大学）

赵立璐（中国科学技术大学）

除了以上学术报告外，还将安排博士后及研究生的海报交流环节，其内容或为自己的研究成果，或为相关课题的研究综述。

指数和：理论、计算及应用

2025.11.17–11.21, 天元数学国际交流中心

云南昆明宜良

11 月 17 日（周一）		
08:50-09:00		简短开幕式
09:00-10:00	胡昊宇	Quantitative sheaf theory and its applications
		茶 歇
10:30-11:30	陈昌昊	Metric theory of Weyl sums
14:30-15:30	赵立璐	Restriction mean value theorems over minor arcs
		茶 歇
16:00-18:00		自由讨论(含墙报)

11 月 18 日（周二）		
09:00-10:00	冯　涛	On the symmetries of finite geometric structures
		茶 歇
10:30-11:30	王安宇	正则校验子译码问题的求解算法研究
14:30-15:30	张鼎新	On the irregular Newton-over-Hodge conjecture for complete intersections
		茶 歇
16:00-18:00		自由讨论(含墙报)

11 月 19 日（周三）		
09:00-10:00	丁治国	Some recent progress on permutation polynomials
		茶 歇
10:30-11:30	万大庆	Non-vanishing of exponential sums
14:30-18:00		自由讨论(含墙报)

11 月 20 日（周四）		
09:00-10:00	许大昕	Frobenius structure on theta connections and rigidity of associated local systems
		茶 歇
10:30-11:30	曹　阳	New step in strong approximation for linear algebraic groups
14:30-15:30	刘博辰	Exponential sums in translational tiling and Fourier restriction
		茶 歇
16:00-18:00		自由讨论(含墙报)

11 月 21 日（周五）		
09:00-10:00	张　扬	On the distinction between Kloosterman sums and multiplicative functions
		茶 歇
10:30-11:30	黄治中	Quadratic forms and the circle method
14:30-18:00		自由讨论(含墙报)

指数和：理论、计算及应用

2025.11.17–11.21，天元数学国际交流中心
云南昆明宜良

曹阳: New step in strong approximation for linear algebraic groups

The classical theory of strong approximation for linear algebraic groups, developed by Kneser, Prasad, and Platonov in the 1960s, only consider the semi-simple simply connected case; the series works by Colliot-Thélène, Xu, Harari, and Demarche extended these results to more general groups, which necessarily needed cohomological obstructions. In this talk, I will present new approaches to strong approximation that avoid to use the abstract notion of cohomological obstruction. I will discuss two recent results:

1. (joint work with Yijin Wang) almost strong approximation for general linear algebraic group (open question of Rapinchuk and Tralle);

2. (joint work with Zhizhong Huang and Runlin Zhang) arithmetic purity of strong approximation for semi-simple simply connected case (open question of Wittenberg).

陈昌昊: Metric theory of Weyl sums

I will first introduce the Weyl sums and its applications on number theory, PDE and ergodic theory. Then I will talk about the typical asymptotic bounds of Weyl sums in the sense of measures and Hausdorff dimension. Joint works with R. Baker, K. Bryce, J. Maynard and I. Shparlinski.

丁治国: Some recent progress on permutation polynomials

In this talk, we present a new approach to the study of permutation polynomials over finite fields, which makes use of algebraic geometry, elliptic curves, algebraic number theory, and serious group theory. We use this approach to produce many new classes of permutation polynomials, to determine all permutation polynomials within several classes of polynomials, and to resolve some conjectures and open problems in the subject. We give a quick survey on other famous problems including Schur Conjecture and Dickson conjecture, in particular, we explain in more detail our approach to Carlitz–Wan conjecture via Galois theory. This is partially joint with Michael Zieve.

冯涛: On the symmetries of finite geometric structures

The study of highly transitive finite geometric structures is a main theme in finite geometry and has a long history. The important work of Jacques Tits builds a connection between group theory and geometry, and the classification of finite simple groups (CFSG) has played a prominent role in the development of finite geometry. In this talk, I will report some recent classification results on finite generalized quadrangles by using CFSG and an application of geometric methods in group theory.

胡昊宇: Quantitative sheaf theory and its applications

In this talk, we study together the quantitative sheaf theory due to Sawin, Forey, Fresán and Kowalski. This theory deals with an invariant named complexity of a constructible étale sheaf on a variety, that bounds the total Betti number of the sheaf. The main result of the theory is a quantitative form of the finiteness for complexities under Grothendieck's six functors, with a strong analytic number theory flavor. If time permits, we discuss its beautiful applications in the equidistribution of exponential sums and in finiteness of perverse sheaves.

黄治中: Quadratic forms and the circle method

This goal of this talk is to survey recent results (partly joint with D. Schindler and A. Shute) on counting integer solutions related to quadratic forms, with a view towards quantitative strong approximation. Our approach is based on the δ-variant of the Hardy–Littlewood circle method developed by Heath-Brown, which expresses the δ-symbol as a suitable weighted exponential sum.

刘博辰: Exponential sums in translational tiling and Fourier restriction

This talk consists of two parts. In the first half we introduce how counting zeros of exponential sums helps on the periodicity of translational multiple tiling. In the second half we discuss Fourier restriction estimates in the real line and possible applications on upper bound estimates of exponential sums.

万大庆: Non-vanishing of exponential sums

The exponential sum of a polynomial over a finite field is an algebraic integer, which is a trace function. In this lecture, we attempt to classify the degree of the polynomial for which the exponential sum is always non-zero. This leads to a deeper exponential sum analogue of the Carlitz–Wan conjecture for permutation polynomials as proven by Lenstra. Examples and a heuristic argument will be given to support the conjecture.

王安宇: 正则校验子译码问题的求解算法研究

正则校验子译码 (RSD) 问题是经典校验子解码问题的一个变体，其核心特征在于错误向量被划分为连续的等长块，且每块中仅有一个非零元素。近年来，由于其在安全多方计算、零知识证明等密码协议中的广泛应用，RSD 问题的计算复杂性分析已成为后量子密码领域的一个研究热点。

本报告介绍一种求解 RSD 问题的新型混合算法。该算法将传统信息集译码 (ISD) 算法中的中间相遇枚举步骤替换为针对正则错误结构的代数方程求解。理论分析与实验结果表明，混合算法能显著降低 RSD 问题的求解复杂度。对于现有密码方案中所采用的典型参数集，新算法的计算复杂度较此前最优求解算法降低了约 2^{20}。此外，将新算法应用于评估两个密码协议的实际安全性：零知识证明协议 Wolverine 和不经意传输协议 Ferret。评估结果显示，Wolverine 协议的安全级别从其目标的 128 比特降至约 111 比特；新算法也首次将 Ferret 协议的安全级别降至其 128 比特的目标值以下。

许大昕: Frobenius structure on theta connections and rigidity of associated local systems

In this talk, we first review the local monodromy at infinity of the Bessel F-isocrystals following Dwork, Sperber. Then we explain a generalization of this story for theta connections. Theta connections are certain rigid connections over $\mathbf{P}^1$ minus two points, related to epipelagic representations under the geometric Langlands correspondence. As an application, we verify a conjecture of Reeder–Yu on the epipelagic Langlands parameters under some technical conditions and a conjecture of Heinloth-Ngo-Yun on the rigidity of Kloosterman sheaves for reductive groups. The talk is based on my joint work with Xinwen Zhu and a joint work in progress with Lingfei Yi.

张鼎新：On the irregular Newton-over-Hodge conjecture for complete intersections

Let (U, f) be a smooth variety over a number field k equipped with a regular function. On one side, C. Sabbah, J.-D. Yu, and T. Mochizuki introduced the irregular Hodge numbers $\{h^{p,q}_{\alpha} : p, q \in \mathbf{Z},\ \alpha \in \mathbf{Q}\}$ associated to the exponentially twisted de Rham cohomology $\mathbf{H}^*\big(U, (\Omega^{\bullet}_{U/k}, \mathrm{d} + \mathrm{d}f)\big)$. On the other side, for a sufficiently large prime $\mathfrak{p}$ of k with residue field κ, one can study the exponential sums $S_{\mathfrak{p}}(U, f) = \sum_{x \in U(\kappa)} \exp\big(\frac{2\pi \mathrm{i}}{p} \mathrm{Tr}_{\kappa/\mathbf{F}_p} f(x)\big)$, where p is the characteristic of κ. Deligne conjectured that the p-adic behavior of $S_{\mathfrak{p}}(U, f)$ is connected with the irregular Hodge numbers in a precise way. Until recently, this conjecture was known only in special situations, such as in the "nondegenerate toric" and "curve" cases. In this talk, I will report on joint work with Rufei Ren and Daqing Wan, in which we establish this conjecture for a large class of functions on a smooth complete intersection with unipotent monodromy at ∞.

张扬: On the distinction between Kloosterman sums and multiplicative functions

The Kloosterman sum $\mathrm{Kl}(a, n)$ is one of the most important objects in Analytic number theory. It is generally believed that $\mathrm{Kl}(a, n)$ as an arithmetic function is not far away from being a multiplicative function. In this talk, I will challenge this belief. More precisely, fix any integers $a \neq 0$ and $k \geq 2$, for any given nonzero complex number η and complex valued multiplicative function f, we will show that 100% of the square-free k-almost primes n satisfy $\mathrm{Kl}(a, n) \neq \eta f(n)$.

In the first half of the talk, I will recall some basic results on Kloosterman sums, and report some recent progress on the distribution of $\mathrm{Kl}(a, n)$ at almost prime moduli n. In the second half, I will introduce our results and give a sketch of the proofs.

赵立璐: Restriction mean value theorems over minor arcs

In the study of the Roth type theorem, the restriction mean value theorems play an important role. In this talk, we shall give a brief survey on restriction mean value theorems and its applications. We shall also introduce the restriction mean value theorem over minor arcs and its application to the Roth type theorem for higher degree equations.
