# Workshop on Combinatorics and Coding Theory

Schedule July 6–10, 2026

July 5: Registration / Check-in; July 6–10: talks and discussions; July 11: Departure.

| Time | July 6 (Mon.) | July 7 (Tue.) | July 8 (Wed.) | July 9 (Thu.) | July 10 (Fri.) |
|---|---|---|---|---|---|
| Chair | Jianxing Yin | Lijun Ji | | Qing Xiang | Leung Ka Hin |
| 09:00–09:30 | **Guangzhou Chen**<br>Constructions of dimensionally orthogonal Latin $k$-dimensional hypercubes | **Vu Van Khu**<br>Robust Constrained Gray Codes | Discussion | **Chen Wang**<br>A Sequential Random Sampling Approach to PIR in DNA-based Data Storage | **Zuo Ye**<br>Correcting Deletions for Ordered Composite DNA Sequences |
| 09:30–10:00 | **Minquan Cheng**<br>New combinatorial structures for coded caching with linear subpacketization: non-half-sum disjoint packing | **Han Mao Kiah**<br>Repairing Reed-Solomon Codes: Less Helpers, Less Errors | | **Qi Wang**<br>The automorphism groups of random linear codes | **Wenjun Yu**<br>On Zero Skip-Cost Generalized Fractional-Repetition Codes from Covering Designs |
| 10:00–10:30 | Break | Break | | Break | Break |
| Chair | Dianhua Wu | Yujie Gu | | Xiuling Shan | Chengmin Wang |
| 10:30–11:00 | **Wendi Di**<br>Some progress on Singer quadrangles | **Yue Zhou**<br>On the construction of MDS self-dual codes and related graphs | | **Ian Wanless**<br>Transversals of Latin hypercubes | **Tao Zhang**<br>Szemerédi–Trotter-type theorems for polynomial curves in $\mathbb{F}_q^2$ |
| 11:00–11:30 | **Jinping Fan**<br>New Lower Bounds for Weak Superimposed Codes | **Hanlin Zou**<br>On the construction of MDS self-dual codes and related graphs | | **Ziqing Xiang**<br>Uncertainty principle for double algebras | **Da Zhao**<br>Random graphs determined by spectrum with various edge density |
| 11:30–12:00 | **Tao Feng**<br>Fractional clique decompositions of dense multipartite graphs | **Zihong Tian**<br>On generalized Howell designs with block size four and their applications to multiply constant-weight codes | | **Zixiang Xu**<br>On Erdős-Frankl-Pach problem | **Yuhao Zhao**<br>The supersaturation problem for eventown families |
| 12:00–13:00 | Lunch | Lunch | | Lunch | Lunch |
| 14:00–18:00 | Discussion | Discussion | | Discussion | Discussion |

**Constructions of dimensionally orthogonal Latin $k$-dimensional hypercubes**

Guangzhou Chen

Henan Normal University

Let $k, n, r$ and $t$ be positive integers satisfying $t \leq k - r$. A hypercube of dimension $k$, order $n$, class $r$ and type $t$, denoted by $(k, n, r, t)$-*hypercube*, is an $n \times n \times \cdots \times n$ (with $k$ times) arrays on a set of $n^r$ distinct symbols such that in every co-dimension-$t$ subarray (i.e., by fixing $t$ coordinates of the array and letting the remaining $k-t$ coordinates vary), each of the $n^r$ distinct symbols appears exactly $n^{k-t-r}$ times. A $(k, n, r, t)$-hypercube is called *a Latin $k$-dimensional hypercube of order $n$* if $r = 1$ and $t = k - 1$, in other words, a Latin $k$-dimensional hypercube of order $n$ is precisely a $(k, n, 1, k - 1)$-hypercube.

A Latin $k$-dimensional hypercube and its orthogonality can be regarded as generalizations of a Latin square and orthogonal Latin squares, respectively. In this talk, we first propose several novel constructions for a set of dimensionally orthogonal Latin $k$-dimensional hypercubes of order $n$. Second, we list several further problems for orthogonal Latin $k$-dimensional hypercubes of order $n$.

**线性分包数编码缓存的新构造结构：非半和不相交填充**

Minquan Cheng

School of Computer Science and Engineering / School of Software / School of Artificial Intelligence, Guangxi Normal University

编码缓存是一种具有前景的技术，它通过利用本地缓存及编码技术带来的组乘增益，有效降低高峰时段网络流量。在编码缓存研究中，我们期望设计具有低分包数和低传输负载的缓存方案，从而在保证较低实现复杂度的同时，实现高峰期的高效传输。尽管已有许多研究对编码缓存方案进行了数学刻画，但这些刻画未能提供明确的构造方法。在本报告中，我们提出了一种新的组合结构——非半和不相交填充（Non-half sum disjoint packing, NHSDP），该结构将编码缓存中的内容放置与传输策略统一于一个组合条件，为设计具有线性子分包数的编码缓存方案提供了框架。通过构造 NHSDP，我们得到一类线性子分包数的编码缓存方案，其传输负载低于现有同等分包数水平的方案。同时，NHSDP 的概念可进一步扩展至多址接入和多天线编码缓存场景，从而得到新的线性子分包数与低传输负载的编码缓存方案。此外，NHSDP 也与若干经典组合结构密切相关，包括循环差填充（Cyclic difference packing, CDP）、无三项算术级数集（Non-three-term arithmetic progression, NTAP）以及完美哈希族（Perfect hash family, PHF）等。这些关联表明，NHSDP 作为独立的研究对象，在组合设计领域具有重要理论意义，其价值已超越编码缓存的应用范畴。

**Some progress on Singer quadrangles**

Wendi Di

East China University of Science and Technology

A generalized quadrangle $\mathcal{S}$ has incidence bipartite graph of diameter 4 and girth 8. We call $\mathcal{S}$ a Singer quadrangle if it has a point-regular automorphism group $G$. An automorphism $\theta$ of $G$ is a multiplier of $\mathcal{S}$ if it induces an automorphism of $\mathcal{S}$. Firstly, we conduct the first systematic study of the properties of multipliers of a Singer quadrangle and have an application on point-primitive generalized quadrangles. Moreover, we get some reduction on Singer quadrangles of odd order.

**New Lower Bounds for Weak Superimposed Codes**

Jinping Fan

Shanggai Normal University

Weak $(t, T)$-superimposed codes were introduced for noisy multimedia fingerprinting to determine the exact size of a coalition (up to $t$ malicious users) under bounded adversarial noise $\|\vec{\epsilon}\| \leq \frac{\sqrt{T}}{2\sqrt{2}t^2}$. It is a specialized variant of classical superimposed codes in binary multi-access channels, which are widely recognized in the literature as disjunct matrices in group testing or cover-free families in combinatorial set systems. Existing results on weak superimposed codes are limited to the lower bound on the largest asymptotic code rate and randomized constructions. In this talk, a new general lower bound on the largest code rate of weak $(t, T)$-superimposed codes is introduced, which was derived by the Lovász local lemma. Moreover, we show that our result improves the best known lower bound on the largest asymptotic code rate of weak $(t, T)$-superimposed codes for infinitely many pairs of $t$ and $T$.

**Fractional clique decompositions of dense multipartite graphs**

Tao Feng

School of Mathematics and Statistics, Beijing Jiaotong University

This talk concerns fractional $K_k$-decompositions of multipartite graphs. For integers $r \geq k \geq 3$, we consider balanced $r$-partite graphs $G$ on $rn$ vertices. We establish necessary conditions for $G$ to admit a fractional $K_k$-decomposition, extending the notion of $k$-admissibility from the case $r = k$ to $r > k$. Using an association scheme on the edge set of a complete $r$-partite

graph, we prove that if $r \geq k+2$ and the partite minimum degree of $G$ is at least $(1-c)n$ with $c \leq 1/((k-2)(k+1)(k-1)^4)$, then $G$ has a fractional $K_k$-decomposition. For $r = k+1$, we show that under the condition $c \leq 1/(3k^3(k-2)^2)$, every $k$-admissible balanced $(k+1)$-partite graph with partite minimum degree at least $(1-c)n$ admits a fractional $K_k$-decomposition. These results provide new degree thresholds for fractional $K_k$-decompositions of multipartite graphs with more than $k$ parts.

**Robust Constrained Gray Codes**

Vu Van Khu

VinUniversity, Vietnam

Gray codes are sequences of codewords in which consecutive codewords differ by a small amount —classically, a single bit flip. In many practical applications, codewords must additionally satisfy structural constraints, such as run-length limited (RLL) constraints or constant-weight constraints, giving rise to constrained Gray codes. In this talk, we survey the landscape of constrained Gray codes and introduce the recently proposed notion of robustness: a Gray code is robust if it tolerates errors in the transition sequence while still guaranteeing that consecutive codewords remain close. We discuss constructions for robust constrained Gray codes, highlight their applications in group testing, differential privacy, and close with a collection of open problems in the area.

**Repairing Reed-Solomon Codes: Less Helpers, Less Errors**

Han Mao Kiah

Nanyang Technological University, Singapore

The Guruswami–Wootters trace repair scheme repairs single-node failures in Reed–Solomon codes with low bandwidth. In this talk, we revisit this framework and discuss two directions for improving its performance.

In the first part of the talk, we ask: Can a failed node be repaired using fewer helper nodes? Building on recent works by Lin (2023) and Liu–Wan–Xing (2024), we present a unified perspective on helper-node selection and trace dependencies.

In the second part of the talk, we ask: Can a failed node still be repaired in the presence of erroneous helper nodes? To address this question, we view the collection of downloaded traces as a code and investigate its distance properties.

**On the construction of MDS self-dual codes and related graphs**

Yue Zhou

School of Science, National University of Defense Technology

The construction of MDS self-dual codes over $\mathbb{F}_q$ of various lengths $n$ is an interesting topic in coding theory, with more than 25 papers published on the subject in the past decade. Most existing constructions rely on combinations of cosets of subgroups within the multiplicative group of $\mathbb{F}_q$.

In this talk, we offer a new perspective by interpreting MDS self-dual codes over $\mathbb{F}_q$ as induced sub(di)graphs of the Paley graphs (or Paley tournaments), characterized by the property that every vertex has even degree. Leveraging classical results on quasi-random graphs, induced even/odd subgraphs, and character sums over finite fields, we derive new constructions and enumeration results for such codes.

**On the maximum size of $(a, b)$-town $(\mathrm{mod}\ k)$ families**

Hanlin Zou

Yunnan University

Oddtown and Eventown are classical problems in extremal set theory showing how linear algebra can restrict set systems with prescribed parity conditions. In this talk, I will discuss a modular generalization: families of subsets whose sizes and pairwise intersections are fixed modulo $k$. Let $m_{k,n}(a, b)$ denote the maximum size of such a family on an $n$-element ground set, with set sizes congruent to $a$ and pairwise intersections congruent to $b$ modulo $k$.

I will present sharp upper bounds for $m_{k,n}(a, b)$. In particular, we prove that $m_{k,n}(a, b) \leq n$ whenever $a \not\equiv b \pmod{k}$, resolving a conjecture of Veselinov and Marinov. I will also discuss the diagonal case, where we obtain a general exponential bound and characterize the equality cases. In several special cases, we improve the general bounds or determine exact values. Separately, we disprove another conjecture of Veselinov and Marinov by giving a counterexample. The proofs combine characteristic-zero linear algebra with tools from coding theory and finite geometry.

**On generalized Howell designs with block size four and their applications to multiply constant-weight codes**

Zihong Tian

School of Mathematical Sciences, Hebei Normal University

Generalized Howell designs (GHDs) are doubly resolvable designs which can be displayed in a square array. They are generalizations of Howell designs and Kirkman squares. In this paper, we investigate the existence of generalized Howell designs with block size four. Using starters and adders together with Weil′s theorem, we establish asymptotic existence results for GHDs of order $3p+1$ for prime $p \equiv 1 \pmod 4$, except when $p \equiv 1 \pmod{32}$. In addition, several classes of optimal multiply constant-weight codes with weight 6 and distance 10 are obtained as applications of these designs.

**A Sequential Random Sampling Approach to PIR in DNA-based Data Storage**

Chen Wang

Faculty of computer science, Technion-Israel Institute of Technology, Israel

With the development of DNA-based storage systems, protecting user privacy during data retrieval from such systems can become increasingly relevant. In such systems, data are often stored as unordered DNA strands and accessed by uniform random sampling, which rules out deterministic addressing as well as computations performed directly on stored strands. This inherent randomness renders traditional private information retrieval (PIR) schemes inapplicable. In this work, we introduce the concept of private information retrieval schemes in DNA-based storage systems and propose a model for one possible embodiment of this paradigm. In our setting, information is sequentially communicated from the data server to the user and the user can stop the flow at any point. We establish fundamental lower bounds on the download cost as a function of privacy leakage. Furthermore, we propose explicit DNA PIR schemes and characterize their performance trade-offs between download cost and privacy leakage. The construction is optimal in certain simple regimes.

**The automorphism groups of random linear codes**

Qi Wang

Department of Computer Science and Engineering, Southern University of Science and Technology

The study of automorphism groups of linear codes is a fundamental topic in coding theory. The matching codewords framework is currently the standard tool for assessing the security of cryptographic schemes whose security relies on the hardness of the Linear Code Equivalence (LCE) problem, such as the LESS signature scheme. This framework often relies on the assumption that $q$-ary random codes have trivial automorphism groups. However, this assumption has

not been formally proved in the literature. In this talk, we prove that with high probability, $k$-dimensional random linear codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ have a trivial automorphism group as $n$ goes to infinity as long as $\min\{k, n-k\} \geq (2+\varepsilon)\log_q n$, for any $\varepsilon > 0$.

**Transversals of Latin hypercubes**

Ian Wanless

Monash University, Australia

A Latin hypercube is a higher-dimensional analogue of a permutation. Transversals in two-dimensional Latin hypercubes (also known as Latin squares) have been studied since Euler's seminal work. In this brief survey talk I will consider how much of the theory from two dimensions generalises to higher dimensions. There are, of course, still plenty of open problems.

**Uncertainty principle for double algebras**

Ziqing Xiang

Southern University of Science and Technology

We will first survey Donoho-Stark uncertainty principle and its generalizations. Then, we will discuss an analogue for double algebras.

**On Erdős-Frankl-Pach problem**

Zixiang Xu

School of Mathematical Sciences, Zhejiang University

The Vapnik–Chervonenkis (VC) dimension is a central concept in statistical learning theory that has also played a growing role in extremal combinatorics. A classical result in this area, the Sauer–Shelah Lemma, precisely determines the maximum size of non-uniform set systems with bounded VC-dimension. In contrast, the uniform setting, where each set has the same size, remains far less understood, and determining tight bounds in this case is a longstanding open problem, originally proposed by Erdős, Frankl and Pach in 1980s. In this talk, I will discuss recent progress on this question.

**Correcting Deletions for Ordered Composite DNA Sequences**

Zuo Ye

Institute of Mathematics and Interdisciplinary Sciences, Xidian University

To increase the information capacity of DNA storage, composite DNA letters were introduced in recent years. In 2025, Dollma *et al* proposed a novel channel model for composite DNA in which composite sequences are decomposed into ordered standard non-composite sequences. In the $k$-resolution ordered composite DNA channel, each codeword can be viewed as a $k \times n$ array over a $q$-ary alphabet, where every column is nondecreasing and the $k$ rows are transmitted through independent channels. This brings new coding problems.

In this talk, I will share our results on codes correcting deletions in ordered composite DNA sequences.

**On Zero Skip-Cost Generalized Fractional-Repetition Codes from Covering Designs**

Wenjun Yu

Institute of Mathematics and Interdisciplinary Sciences, Xidian University

In this talk, we study generalized fractional repetition codes that have zero skip cost, and which are based on covering designs. We show that a zero skip cost is always attainable, perhaps at a price of an expansion factor compared with the optimal size of fractional repetition codes based on Steiner systems. We provide three constructions, as well as show non-constructively, that no expansion is needed for all codes based on sufficiently large covering systems.

**Szemerédi–Trotter-type theorems for polynomial curves in $\mathbb{F}_q^2$**

Tao Zhang

Institute of Mathematics and Interdisciplinary Sciences, Xidian University

We study incidences between point sets in $\mathbb{F}_q^2$ and graphs of polynomials of degree at most $k$. Using a fiber-centered normalization of the incidence discrepancy, we prove that over fields of characteristic $p > k-1$,

$$\left| I(P,L) - \frac{|P||L|}{q} \right| \ll_k q^{-\frac{1}{2}} D_{\mathrm{restr}}(L)\sqrt{D_{\mathrm{vert}}(P)},$$

where $D_{\mathrm{vert}}$ and $D_{\mathrm{restr}}$ measure the vertical and translate-fiber fluctuations, respectively. The proof is based on a short power-sum multiplicity argument.

Our method extends naturally to parametrized curve families with controlled additive multiplicity. As an application, we obtain an incidence bound for the rational curves $y = ax + \frac{b}{x} + c$ over $\mathbb{F}_q^\times$.

We will also present several open problems.

This is a joint work with Thang Pham and Le Anh Vinh.

**Random graphs determined by spectrum with various edge density**

Da Zhao

East China University of Science and Technology, Shanghai

This is based on joint work with Wei Wang, Yanrui Xu.

Edwin van Dam and Willem Haemers conjectured that almost all graphs are determined by their spectra. Van Vu conjectured that almost all random symmetric $\pm 1$ matrices are determined by their spectra. In this talk, we will review the recent progress on van Dam–Haemers conjecture and present new results. This includes but not limited to the work by Van de Berg, Van Werde, Wang, Wang, Wissing, Wu, Xiang, Xu, and Zhao [1, 2, 3, 4, 5, 6, 7, 8].

## 参考文献

[1] N. Van de Berg, A. Van Werde Are sparse graphs typically determined by their spectrum? on the arXiv. arXiv:2602.22757

[2] W. Wang and D. Zhao, Graph isomorphism and multivariate graph spectrum. *Advances in Applied Mathematics* **173** (2026) pp. 102994.

[3] W. Wang and S. Wu, On a generalization of the johnson-newman theorem to multiple rank-one perturbations. on the arXiv. arXiv:2512.12599.

[4] W. Wang and D. Zhao, Almost all graphs have no cospectral mate with fixed level. on the arXiv. arXiv:2509.05781.

[5] P. Wissing, Self-converse mixed graphs are extremely rare. *Discrete Mathematics* **345** (2022) pp. 112989.

[6] Z. Xiang, Natural graph spectra. on the arXiv. arXiv:2602.00936.

[7] Y. Xu and D. Zhao, Generalized block diagonal Laplacian spectrum of graphs. on the arXiv. arXiv:2511.23246.

[8] D. Zhao, Almost all graphs have no cospectral mates with height relative small to its order. on the arXiv. arXiv:2604.02165v2.

**The supersaturation problem for eventown families**

Yuhao Zhao

University of Science and Technology of China

The eventown and oddtown theorems of Berlekamp and Graver are classical results in extremal combinatorics and serve as fundamental examples of the linear algebra method. Over the decades, numerous extensions and variants of the eventown and oddtown problems have been studied in the literature. In this talk, I will present some of our progress on the supersaturation problem for eventown families.