
苏州大学
SOOCHOW UNIVERSITY
第二届组合数学及相关信息理论
前沿课题研讨会
苏州大学数学科学学院
2023年8月26日-27日

第二届组合数学及相关信息理论前沿课题研讨会

会 议 日 程

8月26日 天元讲堂		
主持人	时间	报告人和报告题目
季利均	8:30-9:00	**开幕式及合影**
常彦勋	9:00-9:40	**刘宏伟**: Generalized symbol-pair weights of linear codes over finite fields
	9:40-10:20	**曹海涛**: New developments on orthogonal arrays
	10:20-10:30	茶歇
雷建国	10:30-11:10	**范翠玲**: Near MDS Codes of Non-Elliptic-Curve Type
	11:10-11:50	**田子红**: A generalization of group divisible t-designs
	12:00-	午餐
唐元生	14:30-15:00	**光炫**: Zero-Error Distributed Function Compression
	15:00-15:30	**方伟军**: Bounds and Constructions of Singleton-Optimal Locally Repairable Codes with Small Localities
	15:30-15:40	茶歇
吴佃华	15:40-16:10	**蔡晗**: Repairing locally repairable codes
	16:10-16:40	**闫起发**: 面向分布式机器学习的自适应梯度编码
	16:40-17:10	**程民权**: Low-Complexity and Communication-Efficient Coded Distributed Computing via Combinatorial Designs
	17:30-	晚餐

8月27日 天元讲堂		
主持人	时间	报告人和报告题目
葛根年	8:30-9:10	**冯荣权**: Two Classes of Power Mappings with Boomerang Uniformity 2
	9:10-9:50	**岳勤**: Twisted Goppa codes with an efficient decoding algorithm and quasi-cyclic properties
	9:50-10:00	茶歇
张先得	10:00-10:30	**张韬**: On the existence of semi-regular relative difference sets
	10:30-11:00	**陶然**: Some results on transitive intriguing sets of finite classical polar spaces
	11:00-11:20	**陆建兵**: On finite generalized quadrangles with PSL$(2, q)$ as an automorphism group
	11:20-11:40	**刘苗**: Constant weight codes and constant composition codes asymptotically attaining the Johnson bound: the odd distance
	12:00-	午餐
季利均	14:30-17:30	自由讨论

第二届组合数学及相关信息理论前沿课题研讨会
报 告 摘 要

Generalized symbol-pair weights of linear codes over finite fields

刘宏伟 教授

华中师范大学

Abstract: In this talk, we introduce the notion of generalized symbol-pair weights of linear codes over finite fields, and study some basic properties of GSPWs of linear codes. We determine generalized symbol-pair weights of Simplex codes and two special binary Hamming codes. An application of GSPWs for symbol-pair read wire-tap channel of type II is also provided. This is joint work with Xu Pan.

New developments on orthogonal arrays

曹海涛 教授

南京师范大学

Abstract: An orthogonal array of index unity, order v, degree k and strength 3, or an $\mathrm{OA}(3, k, v)$ in short, is a $k \times v^3$ array on v symbols and in every $3 \times v^3$ subarray, each 3-tuple column vector occurs exactly once. Few results are known about the existence of an $\mathrm{OA}(3, k, v)$ for $k > 4$. In this talk, we introduce a new combinatorial structure called n-dimensions orthogonal complete large sets of disjoint incomplete Latin squares and use it to obtain some new infinite classes of OAs.

Near MDS Codes of Non-Elliptic-Curve Type

范翠玲 教授

西南交通大学

Abstract: A linear code with the parameters of the form $[n, k, n-k+1]$ is referred to be as an MDS (maximum distance separable) code, and a linear code with the parameters of the form $[n, k, n-k]$ is said to be almost MDS (AMDS). A code is called near MDS (NMDS) if both the code and its dual are AMDS. In this talk, we give several constructions of NMDS codes obtained by extension of MDS codes. We also mention that the resultant NMDS codes are linearly inequivalent to the NMDS codes obtained from elliptic curves, and their weight distributions are completely determined.

A generalization of group divisible t-designs

田子红 教授

河北师范大学

Abstract: Cameron, Robert, Andrea et al. defined the concepts of generalized t-design (packing, covering), which form a common generalization of t-design, resolvable design, orthogonal array, 1-factorizations of complete graph. In this talk, we introduce a new class of combinatorial designs which simultaneously provide a generalization of both generalized t-design and group divisible t-design. In certain cases, we derive necessary conditions and parameters relationship for the existence of generalized group divisible t-design (packing, covering), and then point out close connections with various well-known classes of designs, including mixed orthogonal array, factorizations of the complete multipartite graph, large sets of group divisible design and group divisible design with (orthogonal) resolvability. Moreover, we investigate constructions for generalized group divisible t-design (packing, covering) and their existence for $t = 2, 3$ and small block sizes. This talk is based on joint work with Sijia Liu, Yue Han, Lijun Ma and Lidong Wang.

Zero-Error Distributed Function Compression

光炫 教授

南开大学

Abstract: In this talk, we put forward the model of zero-error distributed function compression system of two binary memoryless sources X and Y, where there are two encoders En_1 and En_2 and one decoder De, connected by two channels (En_1, De) and (En_2, De) with the capacity constraints C_1 and C_2, respectively. The encoder En_1 can observe X or (X, Y) and the encoder En_2 can observe Y or (X, Y) according to the two switches s_1 and s_2 open or closed (corresponding to taking values 0 or 1). The decoder De is required to compress the binary arithmetic sum $f(X, Y) = X + Y$ with zero error by using the system multiple times. We use $(s_1s_2; C_1, C_2; f)$ to denote the model in which it is assumed that $C_1 \geq C_2$ by symmetry. The compression capacity for the model is defined as the maximum average number of times that the function f can be compressed with zero error for one use of the system, which measures the efficiency of using the system. We fully characterize the compression capacities for all the four cases of the model $(s_1s_2; C_1, C_2; f)$ for $s_1s_2 = 00, 01, 10, 11$. Here, the characterization of the compression capacity for the case $(01; C_1, C_2; f)$ with $C_1 > C_2$ is highly nontrivial, where a novel graph coloring approach is developed. Furthermore, we apply the compression capacity for $(01; C_1, C_2; f)$ to an open problem in network function computation that whether the best known upper bound of Guang et al. on computing capacity is in general tight.

Bounds and Constructions of Singleton-Optimal Locally Repairable Codes with Small Localities

方伟军 研究员

山东大学

Abstract: An $(n, k, d; r)_q$-locally repairable code (LRC) is called a Singleton-optimal LRC if it achieves the Singleton-type bound. Analogous to the classical MDS conjecture, the maximal length problem of Singleton-optimal LRCs has attracted a lot of attention in recent years. In this talk, we give an improved upper bound for the length of q-ary Singleton-optimal LRCs with disjoint repair groups based on the parity-check matrix approach. Furthermore, we establish equivalent connections between the existence of Singleton-optimal $(n, k, d; r)_q$-LRCs for $d = 6, r = 3$ and $d = 7, r = 2$ with disjoint repair groups and some subsets of lines in finite projective space with certain properties. Consequently, we prove that the length of q-ary Singleton-optimal LRCs with minimum distance $d = 6$ and locality $r = 3$ is upper bounded by $O(q^{1.5})$ and determine the exact value of the maximum code length for some specific q. We also prove the existence of $(n, k, d = 7; r = 2)_q$-Singleton-optimal LRCs for $n \approx \sqrt{2}q$.

Repairing locally repairable codes

蔡晗 副教授

西南交通大学

Abstract: In this talk, the problem of repairing erasures that go beyond the locality is addressed for locally repairable codes. In one aspect, two repair schemes are described to reduce the repair bandwidth for Tamo-Barg codes. One of them can provide optimal repair bandwidth. On the other hand, the cut-set bound is established for locally repairable codes. Notably, our repair schemes are optimal with respect to the cut-set bound. Furthermore, we consider the partial repair problem for locally repairable codes, and introduce both repair schemes and bounds for this scenario.

面向分布式机器学习的自适应梯度编码

闫起发 副教授

西南交通大学

Abstract: 分布式机器学习已被广泛应用, 其中最典型的任务是梯度聚合. 但因分布式环境中时常有缓慢节点的出现, 因此常引入编码以应对缓慢节点. 针对机器学习中应用最为广泛的梯度计算, 我们提出了一种自适应的梯度编码新方案, 可以实现计算负载、缓慢节点容忍度和通信开销之间的最佳平衡, 特别是它允许根据实际环境中未知的实时的缓慢节点数量来最小化通信开销.

Low-Complexity and Communiation-Efficient Coded Distributed Computing via Combinatorial Designs

程民权 教授

广西师范大学

Abstract: Coded distributed computing (CDC) introduced by Li et al. can greatly reduce the communication load for MapReduce computing systems. In the general cascaded CDC with K workers, N input files and Q Reduce functions, each input file will be mapped by r workers and each Reduce function will be computed by s workers such that coding techniques can be applied to create multicast opportunities. The main drawback of most existing CDC schemes is that they require the original data to be split into a large number of input files that grows exponentially with K, which would significantly increase the coding complexity and degrade the system performance. In this talk, we construct several classes of CDC schemes which perform significantly better than the known schemes.

Two Classes of Power Mappings with Boomerang Uniformity 2

冯荣权 教授

北京大学

Abstract: In 1999, Wagner introduced a new cryptanalysis method against block ciphers, namely, the boomerang attack. It can be regarded as a generalization of the differential attack, and it allows new avenues of attack for many ciphers previously deemed safe from differential cryptanalysis. In this talk, the boomerang uniformities of two power mappings are studied via their differential properties.

Twisted Goppa codes with an efficient decoding algorithm and quasi-cyclic properties

岳勤 教授

南京航空航天大学

Abstract: In this talk, we introduce twisted Goppa codes, which generalize classical Goppa codes by adding a twisted term. Then we provide an efficient decoding algorithm for twisted Goppa codes. The Niederreiter cryptosystem is bassed on linear error-correcting codes in which the public key is a parity check matrix. When twisted Goppa codes are applied to the Niederreiter cryptosystem, the public key size is overlarge. To reduce the public key size, we construct quasi-cyclic twisted Goppa codes via a non-trivial automorphism group carefully selecting the defining set and the matched polynomial. Moreover, we obtain a family of cyclic twisted Goppa codes.

On the existence of semi-regular relative difference sets

张韬 副教授

之江实验室

Abstract: In this talk, we study semi-regular relative difference sets. The main contribution of this talk is:

1. Give some nonexistence results on abelian (mn, n, mn, m) relative difference sets. In particular, we focus on the case when m is prime and show that, for any fixed integer $n \geq 2$, there are at most finitely many primes p for which an abelian (pn, n, pn, p) relative difference set may exist.

2. Give a complete classification of abelian (mn, n, mn, m) relative difference sets attaining Turyn' s bound, where $\gcd(m, n) = 1$ and m is self-conjugate modulo mn.

3. Give some results on the existence of (mq, q, mq, m) relative difference sets, where $\gcd(m, q) = 1$ and m is self-conjugate modulo mq.

Some results on transitive intriguing sets of finite classical polar spaces

陶然 助理研究员

山东大学

Abstract: Intriguing sets of finite classical polar spaces are well studied geometric objects due to their connections with two-character sets and strongly regular graphs. In this talk, I will present some of our recent results on the classification of transitive intriguing sets in finite classical polar spaces. We firstly determine all $PSU_3(q)$-invariant intriguing sets of $Q^+(7, q)$ for $q \equiv 2 \pmod 3$. It turns out that such an intriguing set is the unitary ovoid, $q^2 + q$-ovoid, q^3-ovoid or their complements. The group $PSU_3(q)$ is transitive on the unitary ovoid and q^3-ovoid. Finally, we classify the m-ovoids of finite classical polar spaces that admit a transitive automorphism group acting irreducibly on the ambient vector space.

On finite generalized quadrangles with $\mathrm{PSL}(2, q)$ as an automorphism group

陆建兵 博士

浙江大学

Abstract: Let $\mathcal{S}$ be a finite thick generalized quadrangle, and suppose that G is an automorphism group of $\mathcal{S}$. If G acts primitively on both the points and lines of $\mathcal{S}$, then it is known that G must be almost simple. In this paper, we show that if the socle of G is $\mathrm{PSL}(2, q)$ with $q \geq 4$, then $q = 9$ and $\mathcal{S}$ is the unique generalized quadrangle of order 2.

Constant weight codes and constant composition codes asymptotically attaining the Johnson bound: the odd distance

刘苗 博士

山东大学

Abstract: We show that for all fixed weights and odd distances, there exist constant weight codes and constant composition codes asymptotically attaining the Johnson bound, up to an $1 - o(1)$ factor, where $o(1)$ tends to 0 as the code length tends to infinity.