第五届中韩编码理论及相关领域国际学术会议

The 5th Sino-Korea International Conference on Coding Theory and Its Related Topics

Shanghai, China

July 2-6, 2018

Organized by

Department of Mathematics, Shanghai University

Supported by

Gaoyuan Discipline of Shanghai —— Mathematics

Committee

Organizing Committee

Sunghyu Han	KOREATECH, Korea
Jong Yoon Hyun	KIAS, Korea
Qing-Wen Wang	Shanghai University, China

Scientific Committee

Keqin Feng	Tsinghua University, China
Rongquan Feng	Peking University, China
Jon-Lark Kim	Sogang University, Korea
Hyun Kwang Kim	POSTECH, Korea
Hongwei Liu	Central China Normal University, China
Chaoping Xing	Nanyang Technology University, Singapore

Local Organizing Committee

Zhengjun Cao, Yang Ding, Zhuoheng He, Lingji Lou, Xiaomei Jia, Jiancai Sun, Fuping Tan, Hongxi Tong, Qing-Wen Wang(Chair), Yunfei Zhou

Information for Participants

Conference agenda

July 2	*Whole day Registration* *Venue: Lobby of New Lehu Hotel*
July 3-July 5	*Conference*
July 6	*Leave*

Accommodation

New Lehu Hotel (Inside the campus), Shanghai University(上海大学乐乎新楼)
716 Jinqiu Road, Baoshan District, Shanghai, China (上海市宝山区锦秋路 716 号)

Transpo

By Airplane

1. **Pudong Airport -> Shanghai University (Baoshan Campus)**

Line 1: Pudong Airport by Metro Line 2 to Jing'an Temple exchange to Metro Line 7 to Shanghai University (Exit No. 2).

Line 2: Directly take taxi to 716 Jinqiu Road, Shanghai University (Baoshan Campus, North Gate).

2. **Hongqiao Airport -> Shanghai University (Baoshan Campus)**

Line 3: Hongqiao Airport by Metro Line 2 to Jing'an Temple exchange to Metro Line 7 to Shanghai University (Exit No. 2).

Line 4: Directly take taxi to 716 Jinqiu Road, Shanghai University (Baoshan Campus, North Gate).

By Train

1. **Shanghai Hongqiao Railway Station -> Shanghai University (Baoshan Campus)**

Line 5: By Metro Line 2 to Jing'an Temple exchange to Metro Line 7 to Shanghai University (Exit No. 2).

Line 6: Directly take taxi to 716 Jinqiu Road, Shanghai University (Baoshan Campus, North Gate).

2. Shanghai Railway Station -> Shanghai University (Baoshan Campus)

Line 7: By Metro Line 1 to Changshu Road exchange to Metro Line 7 to Shanghai University (Exit No. 2).

Line 8: By Metro Line 3 to Zhenping Road exchange to Metro Line 7 to Shanghai University (Exit No. 2).

Line 9: Directly take taxi to 716 Jinqiu Road, Shanghai University (Baoshan Campus, North Gate).

Contact Us

Prof. Qing-Wen Wang wqw@shu.edu.cn

Dr. Yang Ding dingyang@t.shu.edu.cn

Tel: +86-21-66134715(O), +86-18049888591(M)

Fax:+86-21-66133292

Workshop website: **http://math.shu.edu.cn/2018sino-koreacoding/**

Speakers

Yonglin Cao	Shandong University of Technology, China
Minquan Cheng	Guangxi Normal University, China
Eun Ju Cheon	Gyeongsang National University, Korea
Whan-Hyuk Choi	Kangwon National University, Korea
Lucky Erap Galves	Sogang University, Korea
Sang Guen Han	Korea Advanced Institute of Science and Technology, Korea
Sunghyu Han	Korea University of Technology & Education, Korea
Honggang Hu	University of Science and Technology of China, China
Jongyoon Hyun	Korea Institute for Advanced Study, Korea
Lingfei Jin	Fudan University, China
Boran Kim	Ewha Womans University, Korea
Hyun Kwang Kim	Pohang University of Science and Technology, Korea
Jaeseon Kim	Pohang University of Science and Technology, Korea
Jon-Lark Kim	Sogang University, Korea
Seon Jeong Kim	Gyeongsang National University, Korea
Denis Krotov	Sobolev Institute of Mathematics, Russia
Jack Koolen	University of Science and Technology of China, China
Chengju Li	East China Normal University, China
Shu Liu	University of Electronic Science and Technology of China, China

Program

July 2, 2018 (Monday)

Time	Venue: Lobby of Lehu Hotel (乐乎新楼 1 号楼大厅)
Whole day	**Registration**
17:30-19:30	**Dinner**

July 3, 2018 (Tuesday)

Time	Venue: **Xuehai Hall**(学海厅)—乐乎新楼 2 号楼二楼	
	Speaker\Title	**Chair**
08:10-08:40	**Opening Ceremony** **1. Opening remarks by the Dean of College of Science** **2. Welcome speech by Prof. Keqin Feng** **3. Foreigners speech by Prof. Jon-Lark Kim** **4. Photo-taking**	**Prof. Qing-Wen Wang**
08:40-09:20	**Prof. Hyun Kwang Kim** *Countings in a codebook*	**Prof. Keqin Feng**
09:20-10:00	**Prof. Honggang Hu** *New Classes of Ternary Bent Functions from the Coulter-Matthews Bent Functions*	
10:00-10:20	**Tea Break**	
10:20-11:00	**Prof. Jon-Lark Kim** *On Code-Based Public-key Cryptography*	**Prof. Sunghan Bae**
11:00-11:40	**Prof. Chengju Li** *Constructions of linear codes with one-dimensional hull*	
11:40-12:00	**Dr. Lucky Erap Galves** *Self-dual rank metric codes*	
12:00-13:30	**Lunch**	

14:30-15:10	**Prof. Patrick Sole** *Good algebraic codes exist*	**Prof. Jon-Lark Kim**
15:10-15:50	**Prof. Jack Koolen** *Graphs with smallest eigenvalue at least -3 and their lattices*	
15:50-16:10	**Tea Break**	
16:10-16:50	**Prof. Longjiang Qu** *New Constructions of Systematic Authentication Codes from Three Classes of Cyclic Codes*	**Prof. Rongquan Feng**
16:50-17:30	**Dr. Eun Ju Cheon** *On the maximum size of arcs in the projective plane and some length optimal codes*	
17:30-17:50	**Dr. Shu Liu** *List Decoding of Cover-Metric Codes up to the Singleton Bound*	
18:00	**Dinner**	

Note: Xuehai Hall is located in the 2nd floor of NEW LEHU HOTEL Building 2

July 4, 2018 (Wednesday)

Time	Venue: **Xuehai Hall(学海厅)—乐乎新楼 2 号楼二楼**	
	Speaker\Title	**Chair**
08:30-09:10	**Dr. Jong Yoon Hyun** *Linear codes constructed from simplicial complexes*	**Prof. Hyun-Kwang Kim**
09:10-09:50	**Prof. Minjia Shi** *The largest number of weights in cyclic codes*	
09:50-10:10	**Tea Break**	
10:10-10:50	**Dr. Whan-Hyuk Choi** *Self-dual codes over Galois rings*	**Prof. Denis Krotov**
10:50-11:30	**Prof. Jinquan Luo** *New Constructions of Self-dual MDS Codes*	
11:30-11:50	**Dr. Jaeson Kim** *Construction of linear codes with few weights from defining sets*	
12:00-13:30	**Lunch**	
14:30-15:10	**Prof. Yonglin Cao** *Complete classification and encoding for cyclic codes over Z_4 of length 4n*	**Prof. Jack Koolen**
15:10-15:50	**Prof. Sang Geun Han** *Coding Theory and Lattice Theory at the First NIST Post Quantum Cryptography Standardization Conference*	
15:50-16:10	**Tea Break**	
16:10-16:50	**Prof. Liping Wang** *A new IND-CCA-secure code-based public-key scheme*	**Prof. Fangwei Fu**
16:50-17:30	**Prof. Seon Jeong Kim** *Some configurations of conics in PG(2; q) with q even*	
17:30-17:50	**Dr. Xiaofang Xu** *Constructions of Complete Permutation Polynomials*	
18:00	**Dinner**	

July 5, 2018 (Thursday)

Time	Venue: **Xuehai Hall**(学海厅)—乐乎新楼 2 号楼二楼	
	Speaker\Title	**Chair**
08:30-09:10	**Prof. Denis Krotov** *On the structure of the non-full-rank Steiner triple systems*	**Prof. Xiwang Cao**
09:10-09:50	**Prof. Zhifang Zhang** *A Sphere-Packing Bound for Locally Repairable Codes*	
09:50-10:10	**Tea Break**	
10:10-10:50	**Prof. Hong-Yeop Song** *Some new perfect polyphase sequences and optimal families*	**Prof. Patrick Sole**
10:50-11:30	**Prof. Tao Zhang** *On the nonexistence of linear perfect Lee codes*	
12:00-13:30	**Lunch**	
14:30-15:10	**Prof. Sunghyu Han** *Additive Self-Dual Codes over GF(4) with Minimal Shadow*	**Prof. Qin Yue**
15:10-15:50	**Prof. Lingfei Jin** *A Construction of Permutation Codes and Improvement to the Gilbert-Varshamov Bound*	
15:50-16:10	**Tea Break**	
16:10-16:50	**Dr. Boran Kim** *Minimum weights of two-point algebraic geometry codes*	**Prof. Hong-Yeop Song**
16:50-17:30	**Prof. Minquan Cheng** *Linear Coded Caching Schemes*	
17:30-18:00	**Closing Ceremony** **1. Closing speech by Prof. Hongwei Liu** **2. Closing speech by Prof. Hyun Kwang Kim** **3. Welcome speech by Prof. Sunghyu Han & Prof. Jong Yoon Hyun**	**Prof. Chaoping Xing**
18:00	**Dinner**	

Abstract

Countings in a codebook

Hyun Kwang Kim

Pohang University of Science and Technology

hkkim@postech.ac.kr

Abstract

Let C be a code of length n with cardinality M. The codebook of C, denoted by $[C]$, is an $M \times n$ matrix whose rows are the codewords of C. In principle, the codebook $[C]$ contains all the information of C, and we have to choose valuable information from a codebook to derive a meaningful result. We first show that Delsarte's linear programming bounds can be derived from a codebook by counting the number of $2 \times k$ submatrices of $[C]$ with odd number of 1's in two ways, namely rowwise in the first hand and columnwise on the other hand. Next we apply our idea to constant codes and obtain several new results on the maximum size of q-ary codes with minimum distance d. We finally mention that MacWilliams identity can be derived from the codebook counting.

New Classes of Ternary Bent Functions from the Coulter-Matthews Bent Functions

Honggang Hu

University of Science and Technology of China

hghu2005@ustc.edu.cn

Abstract

It has been an active research issue for many years to construct new bent functions. Recently, we determined the dual function of the well-known Coulter-Matthews bent function completely. As a consequence, we found many classes of ternary bent functions not reported in the literature previously.

On Code-Based Public-key Cryptography

Jon-Lark Kim

Sogang University

ctryggoggo1@gmail.com

Abstract

Since the McEliece cryptosystem, there has been active research on code-based cryptography. In this talk, we give a current trend in code-based public-key cryptography which is one of candidates for Post-Quantum Cryptography.

Constructions of linear codes with one-dimensional hull

Chengju Li

East China Normal University

lichengju1987@163.com

Abstract

The hull of a linear code is defined to be the intersection of the code and its dual, which was originally introduced to classify finite projective planes. The objective of this paper is to present some sufficient and necessary conditions that linear codes and cyclic codes have one-dimensional hull. It is shown that there is no such binary or ternary cyclic codes. Based on these characterizations, some constructions of linear codes with one-dimensional hull were given by employing quadratic number fields, partial difference sets, and difference sets. We also construct cyclic codes with one-dimensional hull. Some optimal codes with one-dimensional hull are obtained.

Self-dual rank metric codes

Lucky Erap Galves

Sogang University

le_galvez@yahoo.com.ph

Abstract

We construct self-dual matrix codes over finite fields from a self-dual matrix code of a smaller size. We show that every self-dual matrix code can be constructed using this building-up construction. We use this to classify, that is, find a complete set of representatives for the equivalence classes of self-dual matrix codes of small sizes over some field. Our classifications confirm, as well as extend, the results given by Morisson in 2015. This is a joint work with Jon-Lark Kim.

Good algebraic codes exist

Patrick Solé

University of Paris VIII

patrick.sole@telecom-paristech.fr

Abstract

We survey the algebraic structure and asymptotic performance of the self-dual and LCD classes of quasi-cyclic, quasi-twisted, and dihedral codes over finite fields and finite rings. Of special interest is the case of low index: double circulant codes and four circulant codes. An application to additive cyclic codes is given.

Graphs with smallest eigenvalue at least -3 and their lattices

Jack Koolen

University of Science and Technology of China

koolen@ustc.edu.cn

Abstract

In 1976, Cameron, Goethals, Seidel and Shult showed that any connected graph with smallest eigenvalue at least -2 is a generalized line graph or has at most 36 vertices. One year later, in 1977, Hoffman showed that for $\tau > -1 - \sqrt{2}$ any connected graph with smallest eigenvalue at least τ and large enough minimal degree is a generalized line graph and hence its smallest eigenvalue is at least -2. The proof of the result of Cameron et al. uses the classification of the root lattices, whereas Hoffman did not need that. But he had to assume a large minimal degree. In this talk I will explain how to generalize the result of Hoffman to graphs with smallest eigenvalue at least -3 using the natural lattice associated to a graph. On the other hand, I will also show that the result of Cameron et al. is much harder to generalize to graphs with smallest eigenvalue at least -3. This is based on joint work with Akihiro Munemasa (Tohoku University), Masood Ur Rehman (USTC), Qianqian Yang (USTC) and Jaeyoung Yang (Anhui University).

New Constructions of Systematic Authentication Codes from Three Classes of Cyclic Codes

Longjiang Qu

National University of Defense Technology

ljqu_happy@hotmail.com

Abstract

Recently, several classes of cyclic codes with three nonzero weights were constructed. With the generic construction presented by C. Ding, T. Helleseth, T. Kløve and X. Wang, we present new systematic authentication codes based on these cyclic codes. In this paper, we study three special classes of cyclic codes and their authentication codes. With the help of exponential sums, we calculate the maximum success probabilities of the impersonation and substitution attacks on the authentication codes. Our results show that these new authentication codes are better than some of the authentication codes in the literature. As a byproduct, the number of times that each element occurs as the coordinates in the codewords of the cyclic codes is settled, which is a difficult problem in general.

On the maximum size of arcs in the projective plane and some length optimal codes

Eun Ju Cheon

Gyeongsang National University

enju1000@naver.com

Abstract

In the projective plane $PG(2,q)$, an $(n,r)_q$-arc is a set $\mathcal{K}$ of n points of $PG(2,q)$ such that some r but no $r+1$ of them, are collinear ([**?**]). Let $m_r(2,q)$ denote the maximum size of n for which there exists an $(n,r)_q$-arc for given r and q. We call $(m_r(2,q),r)_q$ -arc the largest arc for given r and q. An interesting problem in finite geometry is to determine the exact values of $m_r(2,q)$ for given r and q. For $(r-2)q+r < m_r(2,q) \leq (r-1)q+r$, the largest $(m_r(2,q),r)_q$-arc corresponds to a 3-dimensional Griesmer code (length optimal code). In this talk, we consider some conics in $PG(2,q)$ to find the largest arcs (length optimal codes) and give some applications.

List Decoding of Cover-Metric Codes up to the Singleton Bound

Shu Liu

University of Electronic Science and Technology of China

sliu017@e.ntu.edu.sg

Abstract

Wachter-Zeh [1] showed that every cover-metric code can be list decoded up to the Johnson-like bound. Furthermore, it was shown in [1] that efficient list decoding of cover-metric codes up to the Johnson-like bound can be performed. From the work of [1], one natural question is whether the Johnson-like bound can be improved. In this paper, we give a confirmative answer to this question by showing that cover-metric codes can be list decoded up to the Singleton bound. Our contributions consist of three parts. Firstly, we prove that the list decodability of cover-metric codes does not exceed the Singleton bound. Secondly, we show that, with high probability, a random cover-metric code can be list decoded up to the Singleton bound which is better than the Johnson-like bound. Thirdly, by applying the existing decoding algorithms for Hamming metric and rank metric codes, we present explicit constructions of cover-metric codes that can be efficiently list decoded up to the Singleton bound.

References

[1] A. Wachter-Zeh, List Decoding of Crisscross Errors, *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 142-149, 2017.

Linear codes constructed from simplicial complexes

Jong Yoon Hyun

Korea Institute for Advanced Study

hyun33@kias.re.kr

Abstract

In this talk, we provide an approach to constructing interesting class of minimal linear codes. We do this by using geometric and combinatorial objects called simplicial complexes. Following Adamaszek we introduce multivariable generating functions associated to simplicial complexes and derive explicit formulae. We then apply the formulae to determine a necessary and sufficient condition for minimality of certain linear codes.

The largest number of weights in cyclic codes

Minjia Shi

Anhui University

smjwcl.good@163.com

Abstract

Upper and lower bounds on the largest number of weights in a cyclic code of given length, dimension and alphabet are given. An application to irreducible cyclic codes is considered. Sharper upper bounds are given for cyclic codes (called here strongly cyclic), all codewords of which have period the length. Asymptotics are derived on the function $\Gamma(k, q)$, the largest number of nonzero weights a cyclic code of dimension k over $\mathbf{F}_q$ can have, and an algorithm to compute it is sketched.

Self-dual codes over Galois rings

Whan-Hyuk Choi

Kangwon National University

whanhyuk@naver.com

Abstract

We introduce some results classification of the free self-dual codes over Galois rings. The class of free self-dual codes is one of the important classes containing most MDS self-dual codes over Galois rings. We present a method of classification and concrete examples of free self-dual codes over Galois rings of moderate lengths.

New Constructions of Self-dual MDS Codes

Jinquan Luo

Central China Normal University

luojinquan@mail.ccnu.edu.cn

Abstract

In this talk we will present several new constructions on self-dual MDS codes over finite fields of odd prime characteristic. These constructions are based on (extended) generalized Reed-Solomon codes. By choosing suitable coefficients in each column of generator matrix, new self-dual MDS codes are given for various length.

Construction of linear codes with few weights from defining sets

Jaeson Kim

Pohang University of Science and Technology

arkenkjs@postech.ac.kr

Abstract

An $[n, k, d]$-(binary) linear code C is a subspace of $GF(2)^n$ and dimension k with the minimum (Hamming) distance d. We say that a linear code C is t-weight if the number of non-zero weight is equal to $t + 1$. A code with few-weight is interesting object in combinatorics. We consider the following linear code. Let D be a subset of $GF(2)^n$. We define

$$\mathcal{C}_D(W; V) = \{c(u) = (s + u \cdot x)_{x \in D^*} | s \in W, u \in V\}.$$

where $W \subset GF(2)$, $V \subset GF(2)^n$. Then $\mathcal{C}_D$ is a linear code of length $|D^*|$ and dimension at most $n + 1$. We call D the defining set of $\mathcal{C}_D$. In this talk, we explicitly determine the weight distribution of the code $\mathcal{C}_D(GF(2); GF(2)^n)$ when the defining set is the Vasil'ev code. Further, we will determine its subcodes whose non-zero weight is less than or equal to three. This is joint work with Hyun Kwang Kim and Jong Yoon Hyun.

Complete classification and encoding for cyclic codes over Z_4 of length $4n$

Yonglin Cao

Shandong University of Technology

ylcao@sdut.edu.cn

Abstract

For any positive odd integer n, the structures and a complete classification for all cyclic codes over Z_4 of length $4n$ are presented. Using the structure of each code, the formulas for the number of all codes and the number of codewords in each code are given. Then dual codes and self-duality of these codes are investigated. In particular, an efficient encoder for each of these codes are provided. Especially, all 339 self-dual cyclic codes over Z_4 of length 28 are listed precisely, and 50 new cyclic and self-dual Z_4-codes $\mathcal{C}$ with basic parameters $(28, |\mathcal{C}| = 2^{28}, d_H = 4, d_L = 8, d_E = 8)$ are obtained.

Coding Theory and Lattice Theory at the First NIST Post-Quantum Crypto- graphy (PQC) Standardization Conference

Sang Geun Han

KAIST

ock@kaist.ac.kr

Abstract

In this survey we report summary of submitted algorithms for NIST post-quantum cryptography conference which uses coding theory or lattice theory, and follow their current status after the standardization conference. This report will be based on the submitters documents, presentations, and pqc-forum newsgroup discussions provided by NIST.

Some configurations of conics in $PG(2;q)$ with q even

Seon Jeong Kim

Gyeongsang National University

skim@gnu.ac.kr

Abstract

For even q, all tangent lines to the $q+1$ points on the conic pass through the common point which we call the nucleus of the conic. In 1969, Denniston constructed maximal n-arcs as a union of disjoint conics with common nucleus. In 2002, Mathon generalized this construction. Here, a maximal n-arc means the subset of $PG(2,q)$ such that all lines contain 0 or n points of the set. Since then many researchers studied the maximal arcs constructed using such conics. They consider the set of all conics with the fixed nucleus. For distinct two such conics C_1 and C_2, they define the composition $C_1 \oplus C_2$ of them which is another conic belonging to the set. If two conics C_1 and C_2 are disjoint then $C_1 \oplus C_2$ is disjoint from $C_1 \cup C_2$. In this talk, for given positive integer m, we consider each union of m conics, and compute the spectrum of it. Also we find partitions of the plane using conics, lines and points.

A new IND-CCA-secure code-based public-key scheme

Liping Wang

Chinese Academy of Sciences

wangliping@iie.ac.cn

Abstract

In this paper, we propose a new IND-CPA-secure public-key encryption scheme based on hardness of decoding random linear codes in rank metric. Then applying a variant of the Fujisaki-Okamoto transform, we give IND-CCA-secure key encapsulation mechanism. We also give the comparison of parameters between our new schemes and some proposals of the NIST post-quantum call.

Constructions of Complete Permutation Polynomials

Xiaofang Xu

Hubei University

yenxingxxf@163.com

Abstract

Based on the Feistel and MISTY structures, this paper presents several new constructions of complete permutation polynomials of finite field $\mathbb{F}_{2^n}^2$ for a positive integer n and three constructions of CPPs over $\mathbb{F}_{p^n}^m$ for any prime p and positive integer $m \geq 2$. In addition, we investigate the upper bound on the algebraic degree of these CPPs and show that some of them can have nearly optimal algebraic degree.

On the structure of the non-full-rank Steiner triple systems

Denis Krotov

Sobolev Institute of Mathematics

krotov@math.nsc.ru

Abstract

The p-rank of a Steiner triple system B is the dimension of the linear span of the set of characteristic vectors of blocks of B, over GF(p). The Steiner triple systems of order v whose 3-rank is less than $v-1$ are characterized in terms of latin squares and Steiner triple systems of smaller order; a formula for their number is derived. Similar formula is found for the number of Steiner triple systems of order v whose 2-rank is less than v. The last formula generalizes the formulas for the number of Steiner triple systems of order 2^m-1 of rank 2^m-m, 2^m-m+1, and 2^m-m+2, found by V. D. Tonchev in 2001, V. A. Zinoviev and D. V. Zinoviev in 2013, and D. V. Zinoviev in 2016, respectively. This is a joint work with Minjia Shi and Li Xu.

A Sphere-Packing Bound for Locally Repairable Codes

Zhifang Zhang

Chinese Academy of Sciences

zfz@amss.ac.cn

Abstract

In this work we derive a sphere-packing bound for locally repairable code (LRC). Specifically, for binary LRCs with disjoint local repair groups, we obtain an explicit upper bound on the dimension by the sphere-packing appraoch. This bound covers some previous bounds as special cases. For general structure of local repair groups, we derive explicit bounds for $r=2$ and $d>=5$ respectively. Our new bounds turn out to outperform the C-M bound in most cases and have the advantage of having explicit forms. Moreover, our bounds can be extended to q-ary LRCs.

Some new perfect polyphase sequences and optimal families

Hong-Yeop Song

Yonsei University

hysong@yonsei.ac.kr

Abstract

We will review some recent development on the construction of perfect polyphase sequences and optimal families, and discuss a generalization of earlier construction (only for a prime length) to those for any odd length. This is joint work with M. K. Song.

On the nonexistence of linear perfect Lee codes

Tao Zhang

Guangzhou University

taozhang@gzhu.edu.cn

Abstract

In 1968, Golomb and Welch conjectured that there does not exist perfect Lee code in $\mathbb{Z}^n$ with radius $r \geq 2$ and dimension $n \geq 3$. Besides its own interests in coding theory and discrete geometry, this conjecture is also strongly related to the degree-diameter problems of abelian Cayley graphs. Although there are many papers on this topic, the conjecture is far from being solved. In this paper, we prove the nonexistence of linear perfect Lee codes by introducing some new algebraic methods. Using these new methods, we show the nonexistence of linear perfect Lee codes of radii $r = 2, 3$ in $\mathbb{Z}^n$ for infinitely many values of the dimension n. In particular, there does not exist linear perfect Lee codes of radius 2 in $\mathbb{Z}^n$ for all $3 \leq n \leq 100$ except 8 cases.

Additive Self-Dual Codes over $GF(4)$ with Minimal Shadow

Sunghyu Han

KOREATECH

sunghyu@koreatech.ac.kr

Abstract

We define additive self-dual codes over $GF(4)$ with minimal shadow, and we prove the nonexistence of extremal Type I additive self-dual codes over $GF(4)$ with minimal shadow for some parameters.

A Construction of Permutation Codes and Improvement to the Gilbert- Varshamov Bound

Lingfei Jin

Fudan University

lfjin@fudan.edu.cn

Abstract

Due to recent applications to communications over powerlines, multi-level flash memories and block ciphers, permutation codes have received a lot of attention from both coding and mathematical communities. Although there have been several constructions of permutation codes, the Gilbert-Varshamov bound still remains to be the best asymptotical lower bound except for a recent improvement in the case of constant minimum distance. In this talk, we present an algebraic construction of permutation codes and it turns out that, this class of permutation codes improves the Gilbert-Varshamov bound for some cases.

Minimum weights of two-point algebraic geometry codes

Boran Kim

Ewha Womans University

avril012@naver.com

Abstract

We present two-point algebraic geometry codes (AG codes) on algebraic curves over a finite field. We dene the order-like bound on the minimum weights of two-point AG codes on arbitrary algebraic curves. We explicitly determine the order-like bounds for one-point AG codes and two-point AG codes on norm-trace curves over the finite fields of characteristic 2. This is a joint work with Yoonjin Lee (Ewha Womans University).

Linear Coded Caching Schemes

Minquan Cheng

Guangxi Normal University

chengqinshi@hotmail.com

Abstract

Coded caching scheme has recently become quite popular in the wireless network due to the efficiency of reducing the load during peak traffic times. Recently the most concern in the coded caching scheme is the problem of subpacketization level especially in practice. In this talk, we will first characterize a coded caching scheme from the viewpoints of Linear Algebra. Then linear coded caching scheme can be realized by constructing some related matrices with certain rank properties. Finally by means of the concepts of eigenvectors and eigenvalues, several classes of linear coded caching schemes are obtained.

List of Participants

No.	Name	Institute	Email
1.	Sunghan Bae	KAIST	shbae@kaist.ac.kr
2.	Xiwang Cao	Nanjing University of Aeronautics and Astronautics	xwcao@nuaa.edu.cn
3.	Yonglin Cao	Shandong University of Technology	ylcao@sdut.edu.cn
4.	Yuan Cao	Shangdong University of Technology	yuancao@sdut.edu.cn
5.	Minquan Cheng	Guangxi Normal University	chengqinshi@hotmail.com
6.	Xiaoyan Cheng	Yangzhou University	xycheng@yzu.edu.cn
7.	Eun Ju Cheon	Gyeongsang National University	enju1000@naver.com
8.	Whan-Hyuk Choi	Kangwon National University	whanhyuk@naver.com
9.	Weijun Fang	Nankai University	nankaifwj@163.com
10.	Keqin Feng	Tsinghua University	kfeng@math.tsinghua.edu.cn
11.	Rongquan Feng	Peking University	fengrq@math.pku.edu.cn
12.	Fangwei Fu	Nankai University	fwfu@nankai.edu.cn
13.	Lucky Erap Galves	Sogang University	le_galvez@yahoo.com.ph
14.	Jian Gao	Shandong University of Technology	dezhougaojian@163.com
15.	Yun Gao	Nankai University	gaoyun2014@126.com
16.	Sang Geun Han	KAIST	ock@kaist.ac.kr
17.	Sunghyu Han	KOREATECH	sunghyu@koreatech.ac.kr
18.	Daitao Huang	Anhui University	dthuang666@163.com
19.	Fan Huang	University of Science and Technology of China	lanplush@mail.ustc.edu.cn

20.	Honggang Hu	University of Science and Technology of China	hghu2005@ustc.edu.cn
21.	Jongyoon Hyun	KIAS	hyun33@kias.re.kr
22.	Lingfei Jin	Fudan University	lfjin@fudan.edu.cn
23.	Boran Kim	Ewha Womans University	avril012@naver.com
24.	Hyun Kwang Kim	POSTECH	hkkim@postech.ac.kr
25.	Jaeseon Kim	POSTECH	arkenkjs@postech.ac.kr
26.	Jon-Lark Kim	Sogang University	ctryggoggo1@gmail.com
27.	Seon Jeong Kim	Gyeongsang National University	skim@gnu.ac.kr
28.	Jack Koolen	University of Science and Technology of China	koolen@ustc.edu.cn
29.	Denis Krotov	Sobolev Institute of Mathematics	krotov@math.nsc.ru
30.	Chengju Li	East China Normal University	lichengju1987@163.com
31.	Ruihu Li	Air Force Engineering University	llzsy110@163.com
32.	Qunying Liao	Sichuan Normal University	qunyingliao@sicnu.edu.cn
33.	Dongdai Lin	Chinese Academy of Sciences	ddlin@iie.ac.cn
34.	Jingge Liu	Central China Normal University	jinggeLiu@ mail.ccnu.edu.cn
35.	Hongwei Liu	Central China Normal University	hwliu@mail.ccnu.edu.cn
36.	Shu Liu	University of Electronic Science and Technology of China	sliu017@e.ntu.edu.sg
37.	Yan Liu	Yancheng Institute of Technology	liuyan0916@126.com
38.	Gaojun Luo	Nanjing University of Aeronautics and Astronautics	gjluo1990@163.com
39.	Jinquan Luo	Central China Normal University	luojinquan@mail.ccnu.edu.cn
40.	Fanghui Ma	Nankai University	fhma@mail.nankai.edu.cn
41.	Liming Ma	Yangzhou University	lmma@yzu.edu.cn

42.	Longjiang Qu	National University of Defense Technology	ljqu_happy@hotmail.com
43.	Minjia Shi	Anhui University	smjwcl.good@163.com
44.	Hong-Yeop Song	Yonsei University	hysong@yonsei.ac.kr
45.	Lin Sok	Anhui University	soklin_heng@yahoo.com
46.	Patrick Sole	University of Paris VIII	patrick.sole@telecom-paristech.fr
47.	Yuansheng Tang	Yangzhou University	ystang@yzu.edu.cn
48.	Gang Wang	Nankai University	1120160011@mail.nankai.edu.cn
49.	Liping Wang	Chinese Academy of Sciences	wangliping@iie.ac.cn
50.	Qingwen Wang	Shanghai University	wqw@shu.edu.cn
51.	Rongsheng Wu	Anhui University	wrs2510@163.com
52.	Yansheng Wu	Nanjing University of Aeronautics and Astronautics	wysasd@163.com
53.	Chaoping Xing	Nanyang Technological University	xingcp@ntu.edu.sg
54.	Xiaofang Xu	Hubei University	yenxingxxf@163.com
55.	Shudi Yang	Qufu Normal University	yangshd3@mail2.sysu.edu.cn
56.	Siman Yang	East China Normal University	smyang@math.ecnu.edu.cn
57.	Wei Yan	University of Science and Technology of China	yan1993@mail.ustc.edu.cn
58.	Lin You	Hangzhou Dianzi University	youlin@hdu.edu.cn
59.	Qin Yue	Nanjing University of Aeronautics and Astronautics	yueqin@nuaa.edu.cn
60.	Hongwei Zhu	Anhui University	zhwgood66@163.com
61.	Tao Zhang	Guangzhou University	taozhang@gzhu.edu.cn
62.	Shumin Zhang	Qinghai Normal University	zhsm_0926@sina.com
63.	Zhifang Zhang	Chinese Academy of Sciences	zfz@amss.ac.cn

64.	Zhengchu Zhou	Southwest Jiaotong University	zzc@home.swjtu.edu.cn
65.	Zhengjun Cao	Shanghai University	caozhj@shu.edu.cn
66.	Yang Ding	Shanghai University	dingyang@shu.edu.cn
67.	Zhuoheng He	Shanghai University	zhuohenghe@shu.edu.cn
68.	Fuping Tan	Shanghai University	fptan@shu.edu.cn
69.	Hongxi Tong	Shanghai University	tonghx@shu.edu.cn
70.	Jiancai Sun	Shanghai University	jcsun@shu.edu.cn
71.	Xiaomei Jia	Shanghai University	xmjia@shu.edu.cn
72.	Yunfei Zhou	Shanghai University	yfz@shu.edu.cn
73.	Lingji Lou	Shanghai University	lingji_lou@shu.edu.cn
74.	Xiaohua Lu	Shanghai University	2257857324@qq.com
75.	Mengyan Xie	Shanghai University	814032276@qq.com
76.	Xiangjian Xu	Shanghai University	xu.xj@ntu.edu.cn
77.	Tao Li	Shanghai University	ttaoli123@163.com
78.	Huihui Wang	Shanghai University	2463265146@qq.com
79.	Yiling Wu	Shanghai University	1099193856@qq.com
80.	Chongquan Zhang	Shanghai University	marcaszhang@gmail.com
81.	Farouk Adda	Shanghai University	adda-farouk@hotmail.com

上海大学数学系简介

上海大学是国家“211 工程”重点建设高校之一。上海大学数学系现有教职工 116 人，专职教师 100 人，其中教授 26 名、博士生导师 25 人、副教授 35 人、院士 1 名、国家千人计划专家 2 名、上海千人 1 名、教育部长江学者 1 名、杰青 1 名、中国科学院百人计划 1 名、上海领军人才 1 名、曙光学者 1 名、上海浦江人才计划 4 名、上海青年东方学者 3 名，45 岁以下博士比例 100%，获得海外学位或有海外研究经历的人员比例为 95%；在校本科生 500 多人、硕士研究生 200 多人、博士研究生 60 多人。

数学系有数学一级学科博士点、数学博士后流动站，数学、统计学两个一级学科硕士点；有上海市教委重点学科、上海市重点学科、上海高校一流学科、上海市高校高原学科。上海市应用数学与系统科学研究所、上海大学核心数学研究所、上海大学优化开放实验室、上海大学数学与编码密码研究所、上海大学张量与矩阵研究中心、上海大学系统科学研究所均挂靠数学系；上海市青少年科技人才培养基地—上海大学数学科学实践工作站是全国首家数学工作站。

2017 年 USNEWS（《美国新闻和世界报导》）全球最佳大学数学学科排名上海大学位居第 80;美国 ESI 数据库最新数据,全球前 1%的数学研究机构有 241 个，上海大学排第 119, 进入全球前 5‰行列。近年来数学系每年有近 300 位国内外著名专家学者前来讲学交流，包括菲尔兹奖得主 Zelmanov 及杨乐等 30 多位海内外院士来上海大学数学系访问和科学合作研究。主办或承办了包括“第 14 届国际线性代数协会年会”在内的大型国内外学术会议 40 多次。

Brief Introduction

The Department of Mathematics, Shanghai University

Shanghai University (SHU) is one of China's key universities of 'Project 211'. The Department of Mathematics is the home of 116 well qualified people, among them 100 are full-time faculty members. The team of faculty members is formed by 26 professors, 25 doctoral advisors, 35 associate professors, 1 academician, 2 National Thousand Talent Plan, 1 Shanghai Thousand Talent Plan, 1 Chang Jiang Scholars Program, 1 National Science Fund for Distinguished Young Scholars, 1 Chinese Academy of Sciences Hundred Talents Program, 1 Shanghai Leading Talent, 1 Dawn Program of Shanghai Education Commission, 4 Shanghai Pujiang Talent Program, 3 Shanghai Oriental distinguished professors, 100% of doctors under the age of 45, 95% of overseas graduates or staff with overseas research experience. It has over 500 undergraduates, 200 graduate, and 60 doctoral candidates.

The Department of Mathematics consists of one first-level doctoral program in mathematics, one mathematics postdoctoral research station , two first-level graduate programs in mathematics and statistics; and Shanghai municipal education commission key disciplines, Shanghai key disciplines, Shanghai first-class discipline, Shanghai plateau discipline. In addition, Shanghai Institute of Applied Mathematics and Systems Science,

Institute of Core Mathematical Research of Shanghai University, Shanghai University Open Laboratory for Operations Research & Optimization, Institute of Mathematics and Coding & Cryptography of Shanghai University, International Research Center for Tensor and Matrix Theory of Shanghai University, Institute of Systems Science of Shanghai University are all affiliated to The Department of Mathematics. The Shanghai youth talent training base—The workstation on mathematics practice workstation of Shanghai University is a pioneering undertaking for the national mathematics workstation.

In 2017, SHU won the 80th place in the USNEWS World's Best University Mathematics Ranking. According to the latest data from the US ESI database, there are 241 mathematics research institutions occupy world's top 1% , among which, Shanghai University ranks 119, entering the top 5‰ in the world. In recent years, there are nearly 300 famous experts welcomed by The Department of Mathematics for extensive academic communications and research cooperation. Among them, more than 30 domestic and foreign academicians including Fields Medal winner – Zelmanov and o Yang Le have visited. Besides, The Department of Mathematics hosted or undertook more than 40 large-scale domestic and foreign academic conferences including the 14th International Annual Association of Linear Algebra Associations.