Mathematical Theory Applied in Coding and Cryptography Workshop

第二届编码密码学中的数学理论研讨会

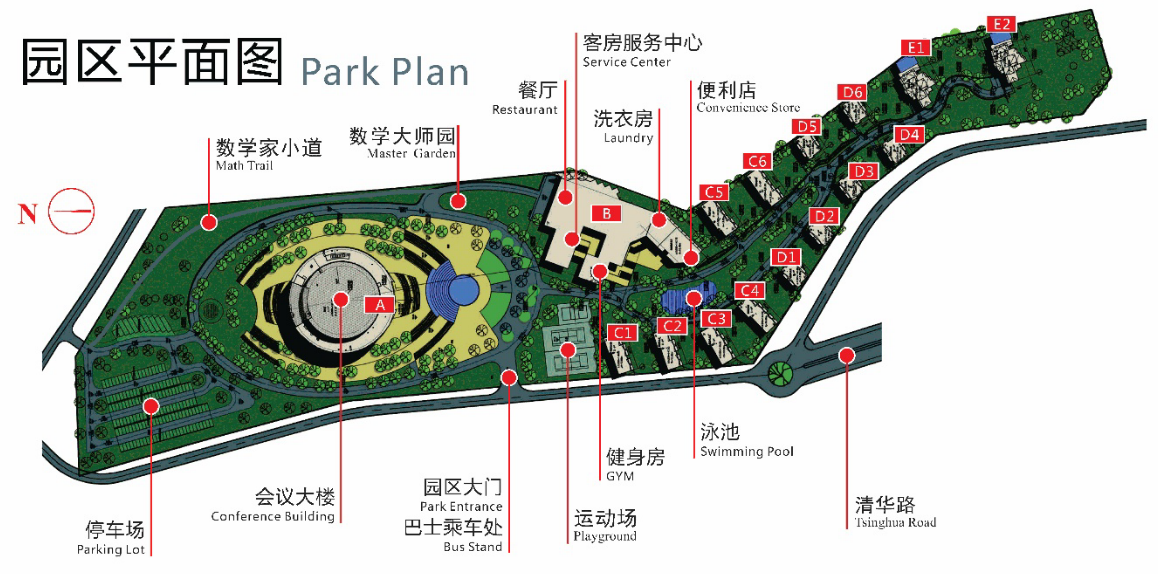
Dec. 10-14, 2018

Welcome to TSIMF

The facilities of TSIMF are built on a 23-acre land surrounded by pristine environment at Phoenix Hill of Phoenix Township. The total square footage of all the facilities is over 29,000 square meter that includes state-of-the-art conference facilities (over 10,000 square meter) to hold many international workshops simultaneously, two libraries, a guest house (over 10,000 square meter) and the associated catering facilities, a large swimming pool, workout gym and sport courts and other recreational facilities.

Mathematical Sciences Center (MSC) of Tsinghua University, assisted by TSIMF's International Advisory Committee and Scientific Committee, will take charge of the academic and administrative operation of TSIMF. The mission of TSIMF is to become a base for scientific innovations, and for nurturing of innovative human resource; through the interaction between leading mathematicians and core research groups in pure mathematics, applied mathematics, statistics, theoretical physics, applied physics, theoretical biology and other relating disciplines, TSIMF will provide a platform for exploring new directions, developing new methods, nurturing mathematical talents, and working to raise the level of mathematical research in China.

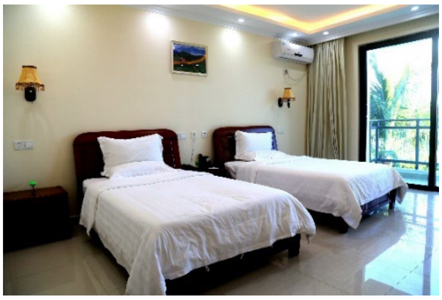
About Facilities



Registration

Conference booklets, room keys and name badges for all participants will be distributed at the front desk. Please take good care of your name badge. It is also your meal card and entrance ticket for all events.

Guest Room



All the rooms are equipped with: free Wi-Fi (no password), TV, air conditioner and other utilities.

Family rooms are also equipped with kitchen and refrigerator.

Library

Opening Hours: 09:00am-22:00pm

TSIMF library is available during the conference and can be accessed by using your room card. There is no need to sign out books but we ask that you kindly return any borrowed books to the book cart in library before your departure.

In order to give readers a better understanding of the contributions made by the Fields Medalists, the library of Tsinghua Sanya International Mathematics Forum (TSIMF) instituted the Special Collection of Fields Medalists as permanent collection of the library to serve the mathematical researchers and readers.
So far, there are 234 books from 47 authors in the Special Collection of Fields Medalists of TSIMF library. They are on display in room A220. The participants are welcome to visit.

Restaurant

All the meals are provided in the restaurant (Building B1) according to the time schedule.

Breakfast	07:30-08:30
Lunch	12:00-13:30
Dinner	17:30-19:00

Laundry

Opening Hours: 24 hours

The self-service laundry room is located in the Building 1 (B1).

Gym

The gym is located in the Building 1 (B1), opposite to the reception hall. The gym provides various fitness equipment, as well as pool tables, tennis tables etc.

Playground

Playground is located on the east of the central gate. There you can play basketball, tennis and badminton. Meanwhile, you can borrow table tennis, basketball, tennis balls and badminton at the reception desk.

Swimming Pool

Please note that there are no lifeguards. We will not be responsible for any accidents or injuries. In case of any injury or any other emergency, please call the reception hall at +86-898-38882828.

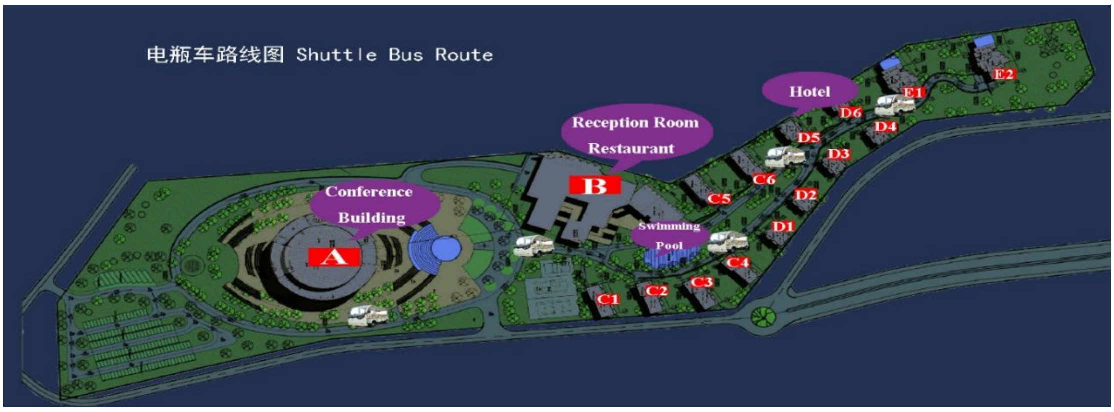
Outside Shuttle Service

We have shuttle bus to take participants to the airport for your departure service. Also, we would provide transportation at the Haihong Square （海虹广场） of Howard Johnson for the participants who will stay outside TSIMF. If you have any questions about transportation arrangement, please feel free to contact Ms. Li Ye (叶莉), her cell phone number is (0086)139-7679-8300.

Free Shuttle Bus Service at TSIMF

We provide free shuttle bus for participants and you are always welcome to take our shuttle bus, all you need to do is wave your hands to stop the bus.

Destinations: Conference Building, Reception Room, Restaurant, Swimming Pool, Hotel etc.



Contact Information of Administration Staff

Location of Conference Affair Office: ***Room 104, Building A***
Tel: 0086-898-38263896
Technical Supervisor: Mr.Shouxi,HE 何守喜
Tel: 0086-186-8980-2225
Email: hesx@ tsimf.cn

Conference Manager: Ms. Xianying, WU 吴显英
Tel:0086-186-8962-3393
Email: wuxianyingjojo@163.com

Location of Accommodation Affair Office: Room 200, Building B1
Tel：0086-898-38882828
Accommodation Manager: Ms. Li YE 叶莉
Tel: 0086-139-7679-8300
Email: yeli@tsimf.cn

Assistant Director of TSIMF
Kai CUI 崔凯
Tel/Wechat: 0086- 136-1120-7077
Email :cuikai@tsimf.cn

Director of TSIMF
Prof.Xuan GAO 高瑄
Email: gaoxuan@tsinghua.edu.cn

Schedule for Mathematical Theory Applied in Coding and Cryptography Workshop，Dec. 10-14, 2018

Time&Date	Monday (Dec. 10)	Tuesday (Dec. 11)	Wednesday(Dec. 12)	Thursday(Dec. 13)	Friday(Dec. 14)
7:30-8:30	*Breakfast (60 minutes)*				
Chair	Mei LU	San LING	Free Discussion	Maosheng Xiong	Free Discussion
8:30-8:40	Open ceremory				
8:40-9:20	Xiangdong HOU	Qiang WANG		Qing XIANG	
9:20-10:00	Lei HU	Jun ZHANG		Qin YUE	
10:00-10:30	*Group Photo about 5 minutes*	*Coffee Break*			
Chair	Xiangyong ZENG	Yanxun CHANG	Free Discussion	Shixin ZHU	Free Discussion
10:30-11:10	Yongge WANG	Hongwei LIU		Minjia SHI	
11:10-11:50	Dabin ZHENG	Zhonghua SUN		Yansheng WU	
12:00-13:30	*Lunch (90 minutes)*				
Chair	Yuansheng TANG	Dianhua WU	Free Discussion 13:30-17:00 As for the sightseeing	Qing XIANG	*Departure*
13:40-14:20	Ming-Deh HUANG	Yaotsu CHANG		Maosheng Xiong	
14:20-15:00	Liping WANG	Haiyan ZHOU		Yonglin CAO	
15:00-15:30	*Coffee Break*			*Coffee Break*	
Chair	Chunming TANG	Yonglin CAO		Qin YUE	
15:30-16:10	Jinquan LUO	Shudi YANG		Chengju LI	
16:10-16:50	Nian LI	Liming MA		Xiaojing CHEN	
17:30	*Banquet 18:00-20:00*	Dinner			

Determination of a Class of Permutation Trinomials in Characteristic Three

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida, Tampa, FL 33620
xhou@usf.edu

Abstract. Let $f(X) = X(1 + aX^{q(q-1)} + bX^{2(q-1)}) \in \mathbb{F}_{q^2}[X]$, where $a, b \in \mathbb{F}_{q^2}^*$. In a series of recent papers by several authors, sufficient conditions on a and b were found for f to be a permutation polynomial (PP) of $\mathbb{F}_{q^2}$ and, in characteristic 2, the sufficient conditions were shown to be necessary. In the present paper, we confirm that in characteristic 3, the sufficient conditions are also necessary. More precisely, we show that when $\operatorname{char}\mathbb{F}_q = 3$, f is a PP of $\mathbb{F}_{q^2}$ if and only if $(ab)^q = a(b^{q+1} - a^{q+1})$ and $1 - (b/a)^{q+1}$ is a square in $\mathbb{F}_q^*$.

Several classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$

Lei Hu
State Key Laboratory of Information Security
Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China

Abstract. In this talk, several classes of permutation polynomials with the form $(x^{p^m} - x + \delta)^s + x$ are investigated by determining the number of solutions of some equations over $\mathbb{F}_{p^{2m}}$. This is a joint work with Zhengbang Zha.

Post Quantum Cryptography and Code Based Cryptography

Yongge Wang
UNC Charlotte, USA
yonwang@uncc.edu

Abstract. NIST has initiated the plan to design new quantum resistant public key cryptography standards. In this talk, we briefly review the fundamental hard problems for lattice based cryptography and code based cryptography. Then we focus on code based public key encryption schemes. In particular, we will discuss our RLCE proposal to NIST. RLCE stands for Random Linear Code based Encryption scheme. As an example, we will instantiate the RLCE scheme using Generalized Reed-Solomon codes and analyze/recommend the security parameters for AES-128/192/256 equivalent security. The implementation of the GRS based RLCE encryption scheme and software packages for analyzing the security strength of RLCE parameters are available at http://quantumca.org/.

Constructions of involutions over finite fields

Dabin Zheng
Hubei Key Laboratory of Applied Mathematics
Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

Abstract. An involution over finite fields is a permutation polynomial whose inverse is itself. Owing to this property, involutions over finite fields have been widely used in applications such as cryptography and coding theory. As far as we know, there are not many involutions, and there isn't a general way to construct involutions over finite fields. This paper gives a necessary and sufficient condition for the polynomials of the form $x^r h(x^s) \in \mathbb{F}_q[x]$ to be involutions over the finite field $\mathbb{F}_q$, where $r \geqslant 1$ and $s \mid (q-1)$. By using this criterion we propose a general method to construct involutions of the form $x^r h(x^s)$ over $\mathbb{F}_q$ from given involutions over the corresponding subgroup of $\mathbb{F}_q^*$. Then, many classes of explicit involutions of the form $x^r h(x^s)$ over $\mathbb{F}_q$ are obtained.

Weil descent and the security of cryptographic maps

Mingde Huang
University of Southern California, L. A., USA

Abstract. We discuss Weil descent as a tool to strengthen the security of cryptographic maps, more specifically cryptographically interesting trilinear maps.

Ivy: a new code-based IND-CCA secure public key scheme

Liping Wang
Institute of Information Engineering, CAS, Beijing, China

Abstract. In this paper, we propose a new IND-CPA-secure public-key encryption (PKE for short) scheme, i.e., Ivy, which is based on hardness of rank syndrome decoding problem. Then applying a variant of the Fujisaki-Okamoto transform, we obtain an IND-CCA2-secure KEM. We also give the comparison of parameters between our scheme and some proposals of the NIST post-quantum call.

New Class of Perfect Nonlinear Functions

Jinquan Luo
Central China Normal University

Abstract. In this talk we will present a new class of perfect nonlinear(or planar) functions over finite fields of odd characteristic. Moreover we will show that in general these functions are not Carlet-Charpin-Zinoviev(CCZ) equivalent to all the known ones.

A survey on the applications of Niho exponents

Nian Li
Faculty of Mathematics and Statistics
Hubei University, Wuhan, China

Abstract. The Niho exponent was introduced by Yoji Niho, who investigated the cross-correlation function between an m-sequence and its decimation sequence in 1972. Since then, Niho exponents have been used in other research areas such as in cryptography and coding theory. In this talk, we will introduce some research problems related to Niho exponents and survey some recent progress in the application of Niho exponents.

Nonlinear congruential pseudorandom sequences over finite fields

Qiang Wang
Carleton University, Ottawa, Canada

Abstract. A nonlinear congruential psеduorandom sequence $\bar{a} = \{a_0, a_1, a_2, ...\}$ is generated by $a_n = f^{(n)}(a_0)$ with initial value a_0, where f is a permutation polynomial over a finite field and $f^{(n)}$ denotes the n-th composition of f. We study a matrix $A(f)$ defined by the powers of $f(x)$ and explain the connection between the period of the sequence and the order of $A(f)$. We also explore the connection between the rank of $A(f)$ and the cardinality of the value set of f.

Deep holes of doubly-extended Reed-Solomon codes

Jun Zhang
Capital Normal University, Beijing, China

Abstract. In this talk, deep holes of Reed-Solomon (RS) codes are studied. Three classes of deep holes for doubly-extended Reed-Solomon codes are constructed explicitly. In particular, deep holes of doubly-extended Reed-Solomon codes with redundancy three and four are completely obtained. This is a joint work with Daqing Wan (University of California, Irvine) and Krishna Kaipa (IISER, Pune).

On σ-self-orthogonal constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$

Hongwei Liu
School of Mathematics and Statistics
Central China Normal University, Wuhan, 430079
hwliu@mail.ccnu.edu.cn

Abstract. In this talk, we shall talk about the σ-self-orthogonality of constacyclic codes of length p^s over the finite commutative chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, where $u^2 = 0$ and σ is a ring automorphism of $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. We obtain the structure of σ-dual code of a λ-constacyclic code of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Then, by using the structure, we get the necessary and sufficient conditions for a λ-constacyclic code to be σ-self-orthogonal. In particular, we determine the σ-self-dual constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. Finally, we extend the results to constacyclic codes of length $2p^s$. This is joint work with Jingge Liu.

Optimal constacyclic locally repairable codes

Zhonghua Sun
HeFei University of Technology, Heifei, China

Abstract. Being part of distributed storage systems, locally repairable codes (LRCs) have drawn great attention in the past years. In this talk, several classes of optimal LRCs are presented. Specifically, a class of optimal constacyclic (r, δ)-LRCs with unbounded length and minimum distance $\delta + 2e$ is constructed, where $1 \leqslant e \leqslant \delta/2$. An optimal cyclic (r, δ)-LRC with unbounded length and minimum distance 2δ is also presented.

Trace index sets of irreducible polynomials over finite fields and their calculations

Yaotsu Chang
I-Shou University, Gaoxiong, Taiwan

Abstract. The concept of trace mapping over finite fields is important from both theoretical and practical viewpoints. It can be found in several finite field applications, such as error-correcting coding theory, cryptography, and so on. In this talk, we will present the concept of trace index set of irreducible polynomial over finite field. We also present some of their properties and calculations.

Counting points on diagonal equations over Galois rings GR(p^2, p^{2r})

Haiyan Zhou
Nanjing Normal University

Abstract. Let $R = GR(p^2, p^{2r})$ be a Galois ring and $N(a_1{x_1}^{k_1} + \cdots + a_n x_n^{k_n} = b)$ denote the number of solutions of diagonal equations $a_1{x_1}^{k_1} + \cdots + a_n x_n^{k_n} = b$ in R, where $a_1, \cdots, a_n \in R\backslash\{0\},\ x_1, \cdots, x_n,\ b \in R$. In this talk, we will express N by Jacobi sums in the finite field $\mathbb{F}_{p^r}$. In particular, the precise number of solutions can be obtained when $k_1 = k_2 = \cdots = k_n = 2$, but in general some estimates can be satisfied.

Pure Weierstrass gaps from a quotient of the Hermitian curve

Shudi Yang
Qufu Normal University, Qufu, China

Abstract. This talk gives an arithmetic characterization of pure Weierstrass gaps at many totally ramified places on a quotient of the Hermitian curve, including the well-studied Hermitian curve as a special case. The cardinality of these pure gaps is explicitly investigated. In particular, the numbers of gaps and pure gaps at a pair of distinct places are determined precisely, which can be regarded as an extension of the previous work by Matthews (2001) considered Hermitian curves.

On subfields of the Hermitian function field involving the involution automorphism

Liming Ma
Yangzhou University, Yangzhou, China

Abstract. A function field over a finite field is called maximal if it achieves the Hasse-Weil bound. Finding possible genera that maximal function fields can achieve has both theoretical interest and practical applications to coding theory and other topics. As a subfield of a maximal function field is also maximal, one way to find maximal function fields is to find all subfields of a maximal function field. Due to the large automorphism group of the Hermitian function field, it is natural to find as many subfields of the Hermitian function field as possible. In literature, most of papers studied subfields fixed by subgroups of the decomposition group at one point (usually the point at infinity). This is because it becomes much more complicated to study the subfield fixed by a subgroup that is not contained in the decomposition group at one point. In this talk, we provide some subfields of the Hermitian function field fixed by subgroups that are not contained in the decomposition group of any point except the cyclic subgroups. It turns out that some new maximal function fields are found.

The shift bound for abelian codes and generalizations of the Donoho-Stark uncertainty principle

Qing Xiang
University of Delaware, Newark, USA

Abstract. Let G be a finite abelian group. If $f : G \to \mathbf{C}$ is a nonzero function with Fourier transform $\hat{f}$, the Donoho-Stark uncertainty principle states that $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| \geqslant |G|$. The purpose of this paper is twofold. First, we present the shift bound for abelian codes with a streamlined proof. Second, we use the shifting technique to prove a generalization and a sharpening of the Donoho-Stark uncertainty principle. In particular, the sharpened uncertainty principle states, with notation above, that $|\operatorname{supp}(f)||\operatorname{supp}(\hat{f})| \geqslant |G| + |\operatorname{supp}(f)| - |H(\operatorname{supp}(f))|$, where $H(\operatorname{supp}(f))$ is the stabilizer of $\operatorname{supp}(f)$ in G.

Polynomial factorizations and their appilactions

Qin Yue
Nanjing University of Aeronautics and Astronautics, Nanjing, China

Abstract. In this talk, we factorize $x^n - a$ into irreducible factors in $\mathbb{F}_q$. As appliactions, we determine all LCD cyclic codes and negacyclic codes and list all self-dual constacyclic codes of length np^s over $\mathbb{F}_q$.

How many weights can a cyclic code have?

Mingjia Shi
School of Mathematical Sciences
Anhui University, Heifei, China

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 the special cyclic codes (called here strongly cyclic), whose nonzero codewords have period equal to the length of the code. Asymptotics are derived on the function $\Gamma(k, q)$, that is defined as the largest number of nonzero weights a cyclic code of dimension k over $\mathbb{F}_q$ can have, and an algorithm to compute it is sketched. The nonzero weights in some infinite families of Reed-Muller codes, either binary or q-ary, as well as in the q-ary Hamming code are determined, two difficult results of independent interest.

Evaluation of some exponential sums and their applications to Walsh transform

Yansheng Wu
Department of Mathematics
Nanjing University of Aeronautics and Astronautics, Nanjing, 211100, China
wysasd@163.com

Abstract. Walsh transform is a basic tool in research of properties of cryptographic functions. A long-standing problem about the Walsh transform is to find functions with a few Walsh transform values and determine its distribution. Let $\mathbb{F}_p$ be a finite field with p elements, where p is a prime. Let $N \geq 2$ be an integer and d be the least positive integer satisfying $p^d \equiv -1 \pmod{N}$. Let $q = p^{2sd}$ for some integers s. In some special cases, we obtain explicit evaluation of the following exponential sums $S(a, b) = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{Tr_{q/p}(ax^{\frac{q-1}{N}}+bx)}$. As applications, Walsh spectrums of monomial functions $Tr_{q/p}(x^{\frac{q-1}{N}})$ in three cases are investigated. Our results show that Walsh spectrums of the monomial functions have at most 4, 5 or 7 distinct values, respectively. Furthermore, three families of the monomial functions with three-valued Walsh spectrums are presented. Consequently, certain previously known results by Li and Yue (Cryptogr Commun 7(2): 217-228, 2015) and Moisio (Finite Fields Appl 15(6): 644-651, 2009) are extended. This is a joint work with Qin Yue and Fengwei Li.

On the Complete Weight Distribution of Subfield Subcodes of Algebraic-Geometric Codes

Maosheng Xiong
Department of Mathematics
Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong
mamsxiong@ust.hk

Abstract. In this talk we report our study on the deviation of the complete weight distribution of a linear code from that of a random code. Then we consider a large family of subfield subcodes of algebraic-geometric codes over prime fields which include BCH codes and Goppa codes and show that the complete weight distribution is close to that of a random code if the code length is large compared with the genus of the curve and the degree of the divisor defining the code.

Construction and enumeration for self-dual cyclic codes of even length over $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$

Yonglin Cao
School of Mathematics and Statistics
Shandong University of Technology, Zibo, Shandong 255091, China

Abstract. Let $\mathbb{F}_{2^m}$ be a finite field of cardinality 2^m, $R = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ $(u^2 = 0)$ and s, n be positive integers such that n is odd. In this talk, an explicit representation for every self-dual cyclic code over the finite chain ring R of length $2^s n$ is provided. On that basis, a clear formula to count the number of all these self-dual cyclic codes is given. As an application, self-dual and 2-quasi-cyclic codes over $\mathbb{F}_{2^m}$ of length $2^{s+1}n$ can be obtained from self-dual cyclic code over R of length $2^s n$ and by a Gray map from R onto $\mathbb{F}_{2^m}^2$.

On two classes of primitive BCH codes and some related codes

Chenju Li
East China Normal University, Shanghai, China

Abstract. BCH codes are an interesting type of cyclic codes and have wide applications in communication and storage systems. Generally, it is very hard to determine the minimum distances of BCH codes. In this paper, we determine the weight distributions of two classes of primitive BCH codes $\mathcal{C}_{(q,m,\delta_2)}$ and $\mathcal{C}_{(q,m,\delta_3)}$ and their extended codes, which solve two problems proposed by Ding, Fan, and Zhou. It is shown that the extended codes $\overline{\mathcal{C}}_{(q,m,\delta_2)}$ have four nonzero weights. We also employ the Hartmann-Tzeng bound to present the minimum distance of the dual code $\mathcal{C}^{\perp}_{(q,m,\delta_2)}$ for $q \geq 5$. Inspired by the idea, we then determine the dimensions of a class of cyclic codes and give lower bounds on their minimum distances, which is greatly improved comparing with the BCH bound. Some optimal codes are obtained.

On the construction of entanglement-assisted quantum MDS codes

Xiaojing Chen
HeFei University of Technology, Heifei, China

Abstract. Recently, entanglement-assisted quantum error correcting codes (EAQECCs) have been constructed by cyclic codes and negacyclic codes. In this talk, by decomposing the defining set of constacyclic codes, four classes of new EAQECCs which satisfy the entanglement-assisted quantum Singleton bound are constructed.