IEEE 信息论学会广州分会季报

IEEE INFORMATION THEORY SOCIETY
GUANGZHOU CHAPTER NEWSLETTER

第二期, 2020 年 10 月 No.2, Oct 2020

主编序语

各位学者：

本期《分会季报》介绍了椭圆码和它的代数列表译码方法，提供一种可替代 Reed-Solomon 码的编码机制。椭圆码是次最大距离可分码，码长可超越有限域大小，具有优异的纠错能力。除此，分会尝试突破疫情影响，举办了 2020 年首场线下学术活动 – 中大网络信息理论与编码研讨会，学者们踊跃参与，气氛活跃，成效喜人。

陈立

From the Editor-in-Chief

Dear Chapter Members,

The current issue introduces elliptic codes and its algebraic list decoding approach. Elliptic codes are almost maximum distance separable (MDS) codes with codeword length greater than the size of finite field, equipped with a good error-correction capability. They can be considered to replace Reed-Solomon codes in future. Moreover, the Chapter has experimented its first onsite workshop of 2020, the SYSU Workshop on Network Information Theory and Coding. It went well with active participations and interactions on the day.

Li Chen

来稿请包含中英文题目、联系人、联系方式、拟投稿栏目，正文内容可以是中文或英文，不超过 800 字。

The submission should include the title in both Chinese and English, author contacts, and the column that the article belongs to. Content of the article can be both in Chinese or English, and is limited to 800 words.

投稿邮箱/Submission email：

itguangzhou@163.com

目录 •Table of Content •

最新结果 • RECENT RESULTS •

Algebraic List Decoding of Elliptic Codes
椭圆码的代数列表译码

Yunqi Wan, Li Chen and Fangguo Zhang, Sun Yat-sen University
万韫琦，陈立，张方国，中山大学
wanyq5@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn, isszhfg@mail.sysu.edu.cn

Algebraic geometric (AG) codes were first introduced by Goppa. They are a class of linear block codes derived from an algebraic curve. Its codeword length is limited by the number of rational points on the algebraic curve. Reed-Solomon (RS) codes can be seen as a special class of AG codes that are constructed from a straight line. The length of an RS code cannot exceed the size of finite field, limiting its minimum Hamming distance and therefore their error-correction capability. However, there exists a number of algebraic curves on which the number of rational points can be greater than the size of finite field. This gives the code a greater codeword length and minimum Hamming distance than a similar rate RS code that is defined over the same finite field. Therefore, AG codes have the potential to replace RS codes in future applications. Among all families of AG codes, elliptic codes have a genus of one, which are either maximum distance separable (MDS) or almost MDS codes, yielding a good tradeoff between its codeword length and distance property.

Decoding of elliptic codes can be categorized into two approaches. One is the syndrome based decoding algorithms, which can correct errors up to half of the code's minimum distance. Another approach is the interpolation based algebraic list decoding (ALD). It has an error-correction capability beyond the above half distance bound. The ALD algorithm consists of two steps, interpolation that constructs the minimum polynomial $Q(x, y, z)$ of ideal I_m of trivariate polynomials that pass through the given interpolation points with a multiplicity of m, and root-finding that determines the z-roots of $Q(x, y, z)$. The interpolation dominates the decoding complexity, which is often realized by Kötter's iterative polynomial construction. By introducing an explicit construction for the zero basis of each affine point on an elliptic curve, ALD of elliptic codes using Kötter's interpolation was proposed by the authors in [1]. However, their complexity remains high. The other interpolation technique is the module basis reduction (BR) [2], which can also yield the Gröbner basis delivered by Kötter's interpolation. But it has a lower complexity than Kötter's interpolation. The BR interpolation consists of basis construction and basis reduction. Based on the interpolation ideal I_m, the output list size l can be determined. Submodule $I_{m,l}$ is defined, which contains trivariate polynomials that satisfy the prescribed interpolation constraints and with z-degree not greater than l. By defining the explicit Lagrange interpolation function over the elliptic function field, a basis of the submodule $I_{m,l}$ is constructed. By mapping, this basis can be presented as a matrix of univariate polynomials. Row operation of the matrix can further reduce it into the desired Gröbner basis, where all rows of the matrix have a different leading position. The interpolation polynomial $Q(x, y, z)$ is the minimum element of the Gröbner basis of $I_{m,l}$. Details of module basis construction and reduction were recently published by the authors in [2]. Table I shows the interpolation complexity of the (80, 27) and (80, 39) elliptic codes, which are defined in GF(64). The complexity is measured as the average number of finite field arithmetic operations in decoding a codeword. Compared with Kötter's interpolation, the BR interpolation substantially reduces the complexity in finding $Q(x, y, z)$. In [2], complexity of the BR interpolation has been analyzed, showing it will be more effective for high rate codes. Note that the interpolation complexity can be further reduced by the re-encoding transform which attribute to a

reduction factor of k/n for both interpolation techniques. Building upon this foundation, the authors are working on algebraic soft-decision decoding of elliptic codes.

Table I Interpolation Complexity of Elliptic Codes

Elliptic codes		(80, 27)			(80,39)		
(m, l)		$(2,3)$	$(4,7)$	$(7,12)$	$(2,3)$	$(4,5)$	$(8,11)$
Kötter		7.93×10^5	1.65×10^7	2.14×10^8	6.78×10^5	8.00×10^6	2.15×10^8
BR	Basis Const.	1.46×10^4	4.85×10^4	1.78×10^5	1.46×10^4	4.85×10^4	2.50×10^5
	Basis Red.	4.48×10^5	1.16×10^7	1.91×10^8	2.80×10^5	4.06×10^6	1.36×10^8

Fig. 1 shows the frame error rate (FER) performance of the (80, 27) elliptic codes and the (63, 21) RS codes. It shows that elliptic code can outperform the similar rate RS code defined over the same finite fields. Note that decoding the elliptic codes with $m = 4$ performs similarly as decoding the RS code with $m = 5$. Our numerical results show decoding the elliptic codes is slightly less complex. Therefore, pivoted by decoding performance, the length advantage of elliptic codes can be transferred into the complexity advantage.

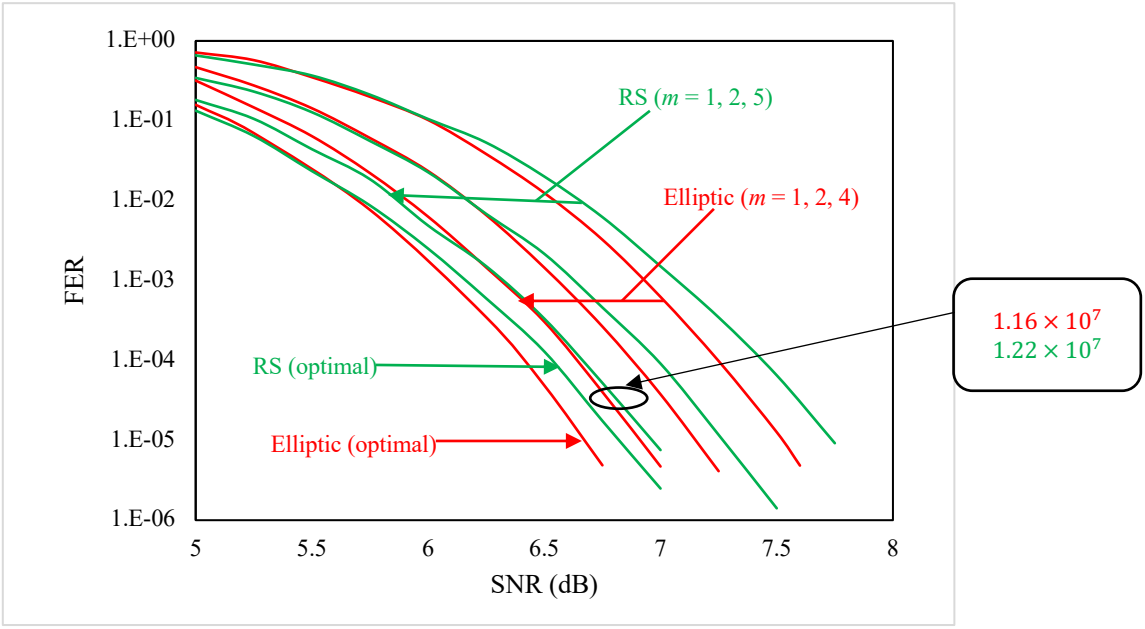

Fig. 1 Performance of the (80, 27) elliptic code and the (63, 21) RS code.

References:

[1] Y. Wan, L. Chen and F. Zhang, Design of Guruswami-Sudan list decoding for elliptic codes, *the IEEE Information Theory Workshop (ITW)*, Visby, Sweden, Aug. 2019.

[2] Y. Wan, L. Chen and F. Zhang, Algebraic list decoding of elliptic codes through module basis reduction, *the International Symposium on Information Theory and Its Applications (ISITA)*, Kapolei, Hawai'i, USA. Oct. 2020.

交流活动 • RESEARCH ACTIVITIES •

“中大网络信息理论与编码研讨会”成功举办
SYSU Workshop on Network Information Theory and Coding

The Sun Yat-sen University (SYSU) Workshop on Network Information Theory and Coding went well in the University’s Guangzhou South Campus. This workshop was organized by the IEEE Information Theory Society Guangzhou Chapter, co-sponsored by Sun Yat-sen University and the Chinese Institute of Electronics Information Theory Society. More than 50 scholars and industry partners from mainland China participated the Workshop. A few others from Hong Kong, including the first speaker Raymond Yeung of CUHK, participated online due to travel restrictions. The Guangzhou Chapter experimented resuming the first onsite conference after the outbreak of COVID-19. We were pleased it went well.

Network coding is a technique to improve the throughput of information flow by allowing coding on received data packets, instead of traditional receive-and-forward, at intermediate nodes, which has been widely used in distributed storage, coded caching, etc. This workshop aims to provide a platform for scholars in South China to exchange new research results on network information theory and coding, which will be beneficial for the community, Universities and the graduate students of the area. The workshop was chaired by Li Chen, a Professor of Sun Yat-sen University and also the chair of Guangzhou Chapter.

There were seven invited talks in this workshop, with a coverage of multi-source network coding, distributed storage, coded caching, subspace codes, etc. In the morning session, Raymond Yeung of the Chinese University of Hong Kong presented recent results in symmetric multilevel diversity coding system (SMDCS), in which an explicit characterization of the superposition coding rate region was obtained. Then, Xiaohu Tang of Southwest Jiaotong University introduced the placement-delivery array (PDA) and its applications in various distributed models. The morning session ended with the talk by Shutao Xia of Tsinghua Shenzhen International Graduate School, which showed some improved bounds and singleton-optimal constructions of locally repairable codes. The afternoon session started with the talk by Hao Chen of Jinan University, with a focus on several constructions of subspace codes. Then, Minquan Cheng of Guangxi Normal University presented in details the coded caching schemes from PDA. Min Ye of Tsinghua-Berkeley Shenzhen Institute presented some new constructions of cooperative MSR codes. The last talk was presented by Congduan Li of Sun Yat-sen University, who shared the latest research results on multi-source multicast network coding rate region.

Finally, Li Chen summarized the workshop and expressed his gratitude to the SYSU team for their efforts in organizing this fruitful event. He advocated holding regular workshops of different themes in future to provide platforms for scholars of the region, in proliferating information theory research and educating younger talents.

交流活动 • RESEARCH ACTIVITIES •

中山大学数学与编码国际研讨会（预告）
SYSU International Workshop on Mathematics and Coding

The IEEE Information Theory Society Guangzhou Chapter is organizing the Sun Yat-sen University (SYSU) International Workshop on Mathematics and Coding on Dec. 2-3, 2020, which will be free for registration. Information coding is the key for modern communications, and coding is founded on mathematics. For example, classic channel codes are founded on linear algebra, while modern channel codes have been facilitated by probability theory and graph theory. The understanding of network coding requires both linear algebra and graph theory. This workshop aims to look back at the mathematics that we have used for designing and practicing codes, so that we can better look forward. This will be a hybrid conference where overseas scholars will participate online, and domestic ones will be onsite. All are welcome!

Organizers: IEEE Information Theory Society Guangzhou Chapter, School of Electronics and Information Technology of Sun Yat-sen University
Chairs: Pingzhi Fan, Li Chen
Venue: Sun Yat-sen University Kaifeng Hotel, Guangzhou, China. Access link will be provided for oversea registrants.
Dates: Dec 2-3, 2020, Beijing Time
Local Arrangements: Xijun Wang, Congduan Li, Shiqiu Liu, Yunqi Wan
Contact：itguangzhou@163.com
Registration: Please register via wechat (微信) link or the following link by Nov. 17, 2020.
https://m.eqxiu.com/s/Cqqe84uT

Program

Beijing Time	Speakers
Dec. 2	
Morning, Moderator: Li Chen	
8:30-8:35	Opening
8:35-9:20	Alexander Barg, University of Maryland (Dec. 1, 19:35-20:20) Stolarsky's invariance principle for the Hamming space and energy maximization
9:20-10:05	Jun Chen, McMaster University (Dec. 1, 20:20-21:05) TBD
10:05-10:30	Coffee break
10:30-11:15	Krishna Narayanan, Texas A&M University (Dec. 1, 20:30-21:05) TBD
11:15-12:00	Paul Siegel, University of California, San Diego (Dec. 1, 19:15-20:00) TBD
12:00-14:00	Photo & Lunch

Afternoon, Moderator: Pingzhi Fan	
14:00-14:45	Erdal Arıkan, Bilkent University （Dec. 2, 9:00-9:45） Polarization Adjusted Convolutional (PAC) Codes
14:45-15:30	Martin Bossert, Ulm University （Dec. 2, 7:45-8:30） TBD
15:30-16:00	Coffee break
16:00-16:45	Bob Li, University of Electronic Science and Technology of China Commutative Algebra in Network Coding
16:45-17:30	Li Chen, Sun Yat-sen University The Gröbner Bases in Decoding of Reed-Solomon Codes
Dec. 3	
Morning, Moderator: Li Chen	
8:30-9:15	Frank Kschischang, University of Toronto (Dec. 1, 19:30-20:15) TBD
9:15-10:00	Dmitry Trukhachev, Dalhousie University (Dec. 1, 21:15-22:00) Braided Block Codes in Fiber-Optical Communications
10:00-10:30	Coffee break
10:30-11:15	Hamid Ebrahimzad, Huawei, Canada (Dec. 1, 21:30-22:15) Polar Code in Optical communication
11:15-12:00	Kai Niu, Beijing University of Post and Telecommunications Polar Spectrum: A Bridge between Polar Codes and Algebraic Codes
12:00-14:00	Lunch
Afternoon, Moderator: Pingzhi Fan	
14:00-14:45	Peter Trifonov, Saint Petersburg Polytech. University (Dec. 3, 9:00-9:45) TBD
14:45-15:30	Pingyi Fan, Tsinghua University MIM-GAN: Interpretable Generative Adversarial Networks with Exponential Function
15:30-16:00	Coffee break
16:00-16:45	Fangwei Fu, Nankai University Optimal Cyclic (r, δ) Locally Repairable Codes with Unbounded Length
16:45-17:30	Raymond Leung, Huawei Coding: Not only Mathematics

征稿启事 • CALL FOR PAPERS

征稿:分布式存储系统的编码和信息理论
Special Issue "Coding and Information Theory for Distributed Storage Systems" of Entropy

Data storage systems, housing massive amounts of information, have become an indispensable component in modern communication networks, as well as cloud computing and network applications. The trend towards ubiquitous data storage in current and future applications induces stringent requirements for data storage, especially in the aspects of reliability and security—not only for storing the data but also for disseminating the data to users and different nodes in the systems. The use of information theory and coding to study the fundamental limits of data storage systems and to innovate efficient coding schemes has gained significant attention from both academia and industry.

This Special Issue will collect original papers within the research area of coding for distributed storage, including the derivation of fundamental trade-offs in storage systems, the design of practical codes that enable efficient data access and update, and the construction of coding schemes that keep stored data confidential and protect the privacy of users. Papers on network coding, physical-layer network coding, secure network coding, and coded caching are also welcome.

Keywords:
Coded caching
Coding for distributed storage
Fundamental limits in data storage systems
Physical-layer network coding
Secure network coding
Secure storage systems

Deadline for manuscript submissions: 15 May 2021.

A special issue of Entropy (ISSN 1099-4300). This special issue belongs to the section "Information Theory, Probability and Statistics".

https://www.mdpi.com/journal/entropy/special_issues/coded_caching

Guest Editors:
Siu-Wai Ho
Lawrence Ong
Kenneth Shum

机会信息 • OPPORTUNITIES •

AP/Postdoc Positions Opening
副教授/助理教授/博士后招聘

Li Chen, Sun Yat-sen University
陈立，中山大学
chenli55@mail.sysu.edu.cn

The Information Coding and Intelligent Transmission (ICIT) Laboratory of the School of Electronics and Information Engineering, Sun Yat-sen University is recruiting associate professors/assistant professors/postdoc at home and abroad, and sincerely invites young talents to join. The lab is directed by Prof. Li Chen.

1. Recruit Field
Information theory and coding, *Computation for information theory*, *Intelligent networks*

2. Recruit Positions
- *Associate Professor:* The applicant should have a PhD degree from a well recognized University or research institute, a strong independent research capability and high academic achievements. Applicants should demonstrate their potential in academia, and have at least 3 years working experience at home or abroad. In general, the applicant should not exceed 40 years old.
- *Assistant Professors:* The same as above but the applicant should not exceed 35 years old.
- *Postdoc:* The applicant should have a PhD degree and an appropriate amount of publications. They should not exceed 35 years old.

3. How to Apply
- Applicants submit their CV (including date of birth, education history, working experience, publications, awards, and etc.) to Prof. Li Chen, with email subject specifying the type of job position.
- The lab and the School will review the applications and if suited, the applicants will be contacted. They will be sent the application form, and guided the preparation of other application materials, including references.
- A School interview will be further arranged. If approved, a University interview will be needed for AP applicants.

新锐风采 • NEW TALENTS •

Suihua Cai (蔡穗华) received the B.Sc. degree in Information and Computer Science from China University of Geosciences, Wuhan, in 2011. He received the M.S. degree in Fundamental Mathematics in 2016 and the Ph.D. degree in Information and Communication Engineering in 2019, both from Sun Yat-sen University, Guangzhou. He is currently a Post-Doctoral Fellow with Sun Yat-sen University.

His research interests are in information theory and channel coding. During his Ph.D. studies, he worked on the block Markov superposition transmission (BMST) techniques. He proposed the BMST-BCH codes with a sliding window decoding algorithm, which can be analyzed by the genie-aided bounds and the density evolution method. It was shown that the BMST-BCH codes can be constructed to achieve a very low error floor, and may find applications in optical transport networks. His recent research focuses on constructing short-length codes by superposition coding. He proposed the free-ride coding scheme for extra data transmissions, which can transmit a small number of extra bits over an existing coded transmission link without any cost of extra transmission energy or extra bandwidth. He also proposed a new coding scheme, called the twisted-pair superposition transmission (TPST), to construction short codes with near capacity performance. The main publications are listed as below.

[1] S. Cai, S. Zhao and X. Ma, “Free ride on LDPC coded transmission,” submitted. Available: https://arxiv.org/abs/1906.10806

[2] S. Cai, W. Lin, X. Yao, B. Wei and X. Ma, “Systematic convolutional low density generator matrix code,” submitted. Available: https://arxiv.org/abs/2001.02854

[3] S. Cai and X. Ma, “Twisted-Pair superposition transmission for low latency communications,” in *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, CA, USA, 2020, pp. 303-308.

[4] S. Cai, S. Zhao and X. Ma, “Packing additional bits into LDPC coded data,” *Electronics Letters*, vol. 55, no. 18, pp. 997-998, 2019.

[5] S. Cai, N. Lin and X. Ma, “Block Markov superposition transmission of BCH codes with iterative erasures-and-errors decoders,” *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 17-27, 2019.