SETA 2026

The 13th International Conference on
Sequences and Their Applications

Conference Program

Hubei University

Wuhan, China

19–23 September 2026

Contents

1 Conference Information

Item	Details
Conference	The 13th International Conference on Sequences and Their Applications (SETA 2026)
Dates	September 19–23, 2026 (registration opens Friday, 18 September)
Venue	Conference Room, 3rd Floor, Innovation and Entrepreneurship Building, Hubei University, Wuhan, China
Website	`https://seta2026.github.io`
Host	Hubei University
Registration desk	18 September: Red Wall Garden Hotel; 19–23 September: outside the Conference Room, 3rd Floor, Innovation and Entrepreneurship Building

1.1 Presentation Format

- Contributed talks: 25-minute slot, comprising a 20-minute presentation followed by 5 minutes for questions.
- Keynotes: 50 minutes followed by 10 minutes for questions.
- Speakers should arrive 10 minutes before their session and upload slides in advance.
- Talks marked "(online)" will be delivered remotely via video conference and streamed to the conference room; the session chair will relay audience questions to remote speakers.

1.2 Committees

Honorary Chair

- Tor Helleseth, University of Bergen, Norway

General Chairs

- Nian Li, Hubei University, China
- Ilias Kotsireas, Wilfrid Laurier University, Canada

Program Chairs

- Sihem Mesnager, University of Paris VIII, France
- Zhengchun Zhou, Southwest Jiaotong University, China

Technical Program Committee

- Christof Beierle, Ruhr University Bochum, Germany
- Lilya Budaghyan, University of Bergen, Norway
- Claude Carlet, University of Paris VIII, France and University of Bergen, Norway
- Chao-Yu Chen, National Cheng Kung University, Taiwan, China
- Nikolay S. Kaleyski, University of Bergen, Norway
- Tetsuya Kojima, National Institute of Technology, Tokyo College, Japan

- Yubo Li, Yanshan University, China
- Zilong Liu, University of Essex, UK
- Subhamoy Maitra, Indian Statistical Institute, Kolkata, India
- Pierrick Méaux, University of Luxembourg, Luxembourg
- Udaya Parampalli, University of Melbourne, Australia
- Alexandr Polujan, Otto von Guericke University Magdeburg, Germany
- Pantelimon Stănică, Naval Postgraduate School, USA
- Yang Yang, Southwest Jiaotong University, China
- Xiangyong Zeng, Hubei University, China

Organizing Committee

- Zhao Hu, Hubei University, China
- Xi Xie, Hubei University, China
- Junru Ma, Hubei University, China
- Jingge Liu, Hubei University, China
- Wenqin Zhang, Hubei University, China
- Sicheng Liang, Hubei University, China

2 Program at a Glance

Date	Main program
Friday, 18 September	Registration and badge collection (14:30–20:30, Red Wall Garden Hotel); dinner at the hotel
Saturday, 19 September	Opening; keynote by Arne Winterhof; 10 contributed talks
Sunday, 20 September	Keynote by Chunming Tang; 11 contributed talks
Monday, 21 September	Keynote by Hong-Yeop Song; 4 contributed talks; half-day excursion in the afternoon; conference banquet in the evening
Tuesday, 22 September	Keynote by Ferruh Özbudak; 11 contributed talks
Wednesday, 23 September	Keynote by Chunlei Li; 4 contributed talks; closing session at noon

All times are China Standard Time (UTC+8). Lunch is served at the Red Wall Garden Hotel; dinners on September 18, 19, 20, and 22 are also at the Red Wall Garden Hotel.

3 Conference Program

3.1 Friday, 18 September 2026 — Registration

Time	Program item
14:30–20:30	**Registration and badge collection** *Red Wall Garden Hotel*
18:00–20:30	Dinner — Red Wall Garden Hotel

3.2 Saturday, 19 September 2026 — Opening Day

Morning Program

Time	Program item
08:30–08:50	**Registration and badge collection** *Conference Room, 3rd Floor, Innovation and Entrepreneurship Building*
08:50–09:00	**Opening Ceremony** *Welcome Remarks*
09:00–10:00	**Keynote: Arne Winterhof (Chair: Sihem Mesnager)** **Pseudorandomness of Algebraic Binary Sequences** *Austrian Academy of Sciences, Austria*
10:00–10:20	Coffee Break
Session 1 — Algebraic Aspects of Sequences and Codes	**Session chair: Udaya Parampalli**
10:20–10:45	**Constructions of Two-to-One Mappings over the Finite Field $\mathbb{F}_{2^{2m}}$** Jinfeng Chong, **Guohao Chen**, and Zepeng Zhuo
10:45–11:10	**Some Notes on the Expansion Complexity of Pseudorandom Sequences** **Hezheng Lin**, Zhimin Sun, and Lingmei Xiao
11:10–11:35	**Construction of Self-Orthogonal Codes and Their Applications** **Fuling Chen**, Dongchun Han, Cuiling Fan, and Sihem Mesnager
11:35–12:00	**Self-Orthogonal Twisted Generalized Reed-Solomon Codes and Their Application to Quantum Error-Correcting Codes** **Yanxin Chen**, Yanli Wang, and Tongjiang Yan

Afternoon Program

Time	Program item
12:00–14:00	Lunch — Red Wall Garden Hotel
Session 2 — Correlation and Feedback Functions of Sequences	**Session chair: Yongbo Xia**
14:30–14:55	**Sequences with Thirteen-Valued Cross Correlations** **Yuehui Cui** and Jinquan Luo
14:55–15:20	**On Almost Ideal Arithmetic Autocorrelation** Vladimir Edemskiy, **Feifei Yan**, and Pinhui Ke
15:20–15:45	**On Determining Feedback Functions of Binary de Bruijn Sequences** Zuling Chang, Shujie Wang, and **Yunlong Zhu**
15:45–16:15	Coffee Break
Session 3 — Complementary Sequences and Pairs	**Session chair: Dongchun Han**
16:15–16:40	**Residue Loom for Periodic Complementary Pairs** **Weifeng Shang** and Ilias Kotsireas
16:40–17:05	**A New Class of Optimal Binary Linear Complementary Pairs of Codes** **Yansheng Wu** and Jing Chen
17:05–17:30	**Constructions of Complementary Sequence Sets of Non-Power-of-Two Lengths with Large Codebook Size** Yajing Zhou, Jiyu Yang, and **Hui Zhang**
18:00–20:30	Dinner — Red Wall Garden Hotel

3.3 Sunday, 20 September 2026

Morning Program

Time	Program item
09:00–10:00	**Keynote: Chunming Tang (Chair: Zhengchun Zhou)** **Beyond Classical Properties: Recent Advances and New Perspectives on m-Sequences** *Southwest Jiaotong University, Chengdu, China*
10:00–10:20	Coffee Break
Session 4 — Polyphase, Doppler-Resilient, and ZAZ Sequences	**Session chair: Zuling Chang**
10:20–10:45	**Two Novel Constructions of Asymptotically Optimal and Near-Optimal Periodic Doppler Resilient Complementary Sequence Sets** **Xuanyu Liu**, Pinhui Ke, and Zuling Chang
10:45–11:10	**A Large Set of Polyphase Sequences with Low Correlation and Low Ambiguity Function** **Xinpeng Bian**, Avik Ranjan Adhikary, and Chunming Tang
11:10–11:35	**Sarwate-Type Bounds for Polyphase Auto-ZAZ Sequences and Optimal Sequence Families** **Mengshi Kao**, Gaofei Wu, and Zilong Wang
11:35–12:00	**New Bounds on the Partial Hamming Correlation of Multi-Timeslot Wide-Gap Frequency-Hopping Sequence Sets with Frequency Shift** **Yidong Xiang**, Xianhua Niu, Xing Liu, Siming Pang, Mingpeng Wang, Jianhong Zhao, and Hong Fu

Afternoon Program

Time	Program item
12:00–14:00	Lunch — Red Wall Garden Hotel
Session 5 — Combinatorial Structures and Classical Codes	**Session chair: Chengju Li**
14:30–14:55	**Duality in Periodic Sets** Minjia Shi, Mengru Yang, and **Patrick Solé**
14:55–15:20	**Quinary Repeated-Root Cyclic Codes with Good Parameters** **Yifan Tangfang**, Gaojun Luo, Xiwang Cao, and Yihong Yang
15:20–15:45	**On a Class of Ternary LCD BCH Codes** Mrinal Kanti Bose, **Udaya Parampalli**, and Abhay Kumar Singh
15:45–16:15	Coffee Break
Session 6 — Waveform and Data-Driven Sequence Design	**Session chair: Yubo Li**
16:15–16:40	**Efficient Generation of Shorthand Universal Cycles for Permutations** Zuling Chang, Lingyu Diao, and **Jie Xue**
16:40–17:05	**A New Periodic Total Squared Correlation Bound and Nearly Optimal Constructions of Quaternary Signature Sets** **Xuliang Wang**, Bing Liu, Yuhang Che, Chao Qi, and Jianhong Zhou
17:05–17:30	**Waveform Design for Dual-Functional Radar-Communication Systems Based on Consensus-ADMM** **Enbo Hu**, Runze Liu, Xiaoyu Chen, and Yubo Li
17:30–17:55	**HpLSTM: An MOCSS Generation Method Based on Long and Short Term Memory Network and Discrete Hopfield Neural Network** **Yuhang Che**, Haiyi Zhao, and Bing Liu
18:00–20:30	Dinner — Red Wall Garden Hotel

3.4 Monday, 21 September 2026

Morning Program

Time	Program item
09:00–10:00	**Keynote: Hong-Yeop Song (Chair: Minjia Shi)** **Connection between Florentine Rectangles and the Family of Perfect Polyphase Sequences with Optimum Cross-Correlation** *Yonsei University, Seoul, Korea*
10:00–10:20	Coffee Break
Session 7 — Wide-Gap and Low-Hit-Zone Frequency Hopping	**Session chair: Xianhua Niu**
10:20–10:45	**New Constructions of Optimal One-Coincidence Wide-Gap Frequency-Hopping Sequence Set** **Qianhui Wei**, Xinyu Tian, and Xiaoyu Chen
10:45–11:10	**Constructions of Optimal or Near-Optimal Wide-Gap Low-Hit-Zone Frequency-Hopping Sequence Sets Via Interleaving Technique** **Yuwei Chen**, Yang Yang, Wei Su, and Udaya Parampalli
11:10–11:35	**New Constructions for Optimal Sets of Wide-Gap Frequency-Hopping Sequences with Low-Hit-Zone** **Xiaoyan Chen**, Avik Ranjan Adhikary, Zhengchun Zhou, and Udaya Parampalli
11:35–12:00	**New Bounds on the Partial Hamming Correlation of Wide-Gap Low-Hit-Zone Frequency-Hopping Sequences with Frequency Shift** Kun Hu, **Hongyu Han**, and Sheng Zhang

Afternoon Program

Time	Program item
12:00–14:00	Lunch — Red Wall Garden Hotel
14:00–14:15	**Excursion Assembly** *Meeting Point: Red Wall Garden Hotel Lobby*
14:15–17:30	**Conference Excursion** *Destination: East Lake*
17:30–18:30	Return and Personal Time

Evening Program

Time	Program item
18:30–20:00	**SETA 2026 Conference Banquet**

3.5 Tuesday, 22 September 2026

Morning Program

Time	Program item
09:00–10:00	**Keynote: Ferruh Özbudak (Chair: Chunlei Li)** **Bounds and Constructions for Orthogonal and Covering Arrays** *Sabancı University, Istanbul, Turkey*
10:00–10:20	Coffee Break
Session 8 — Codebooks and Frequency-Hopping Constructions	**Session chair: Zhimin Sun**
10:20–10:45	**A Generic Construction of Complex Codebooks from Functions over Abelian Groups** Ziling Heng, **Chenkun Xie**, Jiantao Hu, and Xiaoyan Jing
10:45–11:10	**Compatible Permutations by Schur-Complement Extensions and Their Applications to NOMA Codebooks and MUBs** **Chunlei Li**, Constanza Riera, and Pantelimon Stănică
11:10–11:35	**Optimal Frequency-Hopping Sequences from Partition-Type Difference Family with Chaotically Enhanced Linear Complexity** **Gejun Zhu**, Shanding Xu, Tianyi Liu, and Xiangyong Feng
11:35–12:00	**New Constructions of Optimal Frequency-Hopping Sequence Sets Based on a Refined Interleaving Framework** **Xingyu Zheng** and Zhengchun Zhou

Afternoon Program

Time	Program item
12:00–14:00	Lunch — Red Wall Garden Hotel
Session 9 — Linear Codes, Hulls, and Projective Constructions	**Session chair: Kangquan Li**
14:30–14:55	**A New Family of Few-Weight Minimal Linear Codes via Bivariate Trace Functions** **Tong Cui**, Shanding Xu, and Gejun Zhu
14:55–15:20	**Subfield Codes and Hull Dimensions of a Family of Projective Optimal Linear Codes** **Liang Shao**, Zhao Hu, and Nian Li
15:20–15:45	**Several Classes of Linear Codes from Projective Spaces** Guangkui Xu, **Weiqi Wang**, and Heqian Xu
15:45–16:10	**Double Cyclic Codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ and Their Application to EAQECC** Pinakin Dave and **Amit Sharma**
16:10–16:40	Coffee Break
Session 10 — Sequences, Codes, and Pseudorandomness (Online)	**Session chair: Jie Li**
16:40–17:05	**k-ary Legendre Pairs** **Ilias Kotsireas**, Huaning Liu, and Arne Winterhof
17:05–17:30	**Correlation Bounds and Markov Analysis for RO Based TRNGs** Miguel Alcocer-Pérez, Ana Isabel Gómez, and **Domingo Gómez-Pérez**
17:30–17:55	**New Classes of Binary Quantum CSS-T Codes Based on Plateaued Functions** **Melike Çakmak**, Sihem Mesnager, Ahmet Sınak, and Oğuz Yayla
18:00–20:30	Dinner — Red Wall Garden Hotel

3.6 Wednesday, 23 September 2026

Morning Program

Time	Program item
09:00–10:00	**Keynote: Chunlei Li (Chair: Patrick Solé)** **Sequences with Good Periodic and/or Aperiodic Autocorrelation** *University of Bergen, Norway*
10:00–10:20	Coffee Break
Session 11 — Sequence Complexity and Code Constructions	**Session chair: Haode Yan**
10:20–10:45	**On the k-error Linear Complexity of the Ding-Helleseth-Martinsen Sequences** Jingwei Zhang, **Changan Zhao**, and Yunlong Zhu
10:45–11:10	**Trace Representation of Binary Sequences Derived from Euler Quotients Modulo pq^m** **Jingwei Zhang** and Changan Zhao
11:10–11:35	**Self-Orthogonal Codes over Non-Unital Non-Commutative Rings from Simplicial Complexes** **Yan Wang**, Tong Su, Xudong Wang, and Chenhuang Wu
11:35–12:00	**Binary Goppa Codes with A_4 Automorphism Groups and Their Parameters** **Tianni He**, Kangquan Li, and Longjiang Qu
12:00–12:15	**Closing Session** *Acknowledgements and farewell*
12:15–14:00	Lunch — Red Wall Garden Hotel
End of SETA 2026	

4 Abstracts of Keynotes

4.1 Saturday, 19 September 2026

Pseudorandomness of Algebraic Binary Sequences

Arne Winterhof
Austrian Academy of Sciences, Austria

Any binary sequence $\mathcal{S} = (s_n)_{n=0}^{\infty}$, $s_n \in \{0,1\}$, may be identified with i) a formal power series over the finite field $\mathbb{F}_2$ of two elements $G_{\mathcal{S}}(x) = \sum_{n=0}^{\infty} s_n x^n \in \mathbb{F}_2[[x]]$, ii) a 2-adic integer $G_{\mathcal{S}}(2) = \sum_{n=0}^{\infty} s_n 2^n \in \mathbb{Z}_2$, iii) a real number in the unit interval $\frac{G_{\mathcal{S}}(2^{-1})}{2} = \sum_{n=0}^{\infty} s_n 2^{-n-1} \in [0,1]$. We study (not ultimately periodic) sequences for which either i) $G_{\mathcal{S}}(x)$ is algebraic over $\mathbb{F}_2(x)$ (such sequences are called automatic sequences), for example, the Thue–Morse sequence $(0,1,1,0,1,0,0,1,\ldots)$, that is, $G_{\mathcal{S}}(x)^2 + \frac{1}{x+1} G_{\mathcal{S}}(x) + \frac{x}{(x+1)^3} = 0$, ii) $G_{\mathcal{S}}(2)$ is algebraic over $\mathbb{Q}$ (embedded in $\mathbb{Q}_2$), for example, the sequence identified with $\sqrt{-7} = 1 + 2^2 + 2^4 + 2^5 + 2^7 + \cdots$, iii) or $\frac{G_{\mathcal{S}}(2^{-1})}{2}$ is algebraic over $\mathbb{Q}$ (embedded in $\mathbb{R}$), for example, the sequence identified with $\sqrt{\frac{1}{2}} = \frac{1}{2} + \frac{1}{8} + \frac{1}{16} + \frac{1}{64} + \cdots$. We discuss the behaviour of these sequences with respect to several measures of pseudorandomness, including i) the Nth linear complexity, ii) the Nth 2-adic complexity, iii) the Nth rational complexity. We also study subsequences such as the Thue–Morse sequence along squares.

Biography

Arne Winterhof received his Ph.D. in mathematics from the Technical University of Braunschweig in 1996. In 2001, he obtained his habilitation from the University of Vienna. He was awarded the Hlawka Prize in 2004 and the Advancement Award of the Austrian Mathematical Society in 2010. From 1999 to 2002, he was a research scientist at the Institute of Discrete Mathematics of the Austrian Academy of Sciences in Vienna, and from 2002 to 2003 at Temasek Laboratories at the National University of Singapore. Since 2003, he has been with the Johann Radon Institute for Computational and Applied Mathematics of the Austrian Academy of Sciences in Linz. He serves on the editorial boards of *Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences*, *Journal of Uniform Distribution Theory*, and *Advances in Mathematics of Communications*. He was co-editor of the Sequences and Their Applications (SETA) proceedings in 2008 and 2014. His research focuses on finite fields and their applications, particularly the analysis of pseudorandom sequences. He has published more than 160 papers in international refereed journals and conferences and co-authored the monograph *Applied Number Theory* with Harald Niederreiter. He is widely recognized for his contributions to the theory of pseudorandomness and finite fields.

4.2 Sunday, 20 September 2026

Beyond Classical Properties: Recent Advances and New Perspectives on m-Sequences

Chunming Tang
Southwest Jiaotong University, Chengdu, China

Maximum-length sequences (m-sequences) serve as fundamental building blocks in sequence design. They are classically characterized by their span, decimation, shift-and-add, balance, run, and ideal two-level autocorrelation properties. Because of these optimal pseudorandom features, m-sequences have been extensively applied in spread-spectrum communications, cryptography, radar systems, and coding theory. Despite being well-studied classical mathematical objects, the evolving demands of next-generation technological systems have sparked renewed interest in this field. In this talk, we will present recent advances in the study of m-sequences.

Biography

Chunming Tang is a Research Professor at the School of Information Science and Technology, Southwest Jiaotong University. He received his Ph.D. degree from Peking University in July 2012, and subsequently worked as a postdoctoral researcher at the University of Paris VIII and the Hong Kong University of Science and Technology (HKUST). His primary research interests focus on coding and cryptographic theory oriented towards cyberspace security. As an independent, first, or corresponding author, he has published over 80 papers in prestigious journals within his field, including more than 30 papers in *IEEE Transactions on Information Theory*, the flagship journal in coding and cryptography. In recognition of his outstanding contributions to the field of cryptographic functions, he was awarded the George Boole Prize, a distinguished international academic award in cryptography. His research achievements have also earned him the Second Prize of the Natural Science Award from the Ministry of Education of China (ranked 2nd out of 4). Furthermore, he serves as the Principal Investigator (PI) for both Key and General Programs funded by the National Natural Science Foundation of China (NSFC).

4.3 Monday, 21 September 2026

Connection between Florentine Rectangles and the Family of Perfect Polyphase Sequences with Optimum Cross-Correlation

Hong-Yeop Song
Yonsei University, Seoul, Korea

Florentine rectangles (circular or straight) had been studied earlier in the 1980's as some new combinatorial structures by Professor S. W. Golomb and his group and was a main subject of my PhD thesis in 1991 and published as a section in CRC Handbook of Combinatorial Designs in 1996. After about 25 years later, when I have discovered that the Fermat-quotient sequences of length p^2 is a perfect sequence and also that there exists a way to construct family with optimum cross-correlation, I have noticed some form of permutations play an important role in connection with the size of the family. Pretty soon, it was identified that the set of permutations is exactly the rows of a circular Florentine arrays. We were very much surprised that the subject matters about 25 years ago reappear as some key elements of the current research. We have summarized the result and submitted it in Jan. 2019. It was finally published in Nov. 2021. In the meantime, another independent discovery seemed to happen from Bergen, Norway, and the result was presented at IEEE ISIT 2020 on the same connection. So far, the main story is the relation between the size of the perfect polyphase sequence family of ODD length with optimum cross-correlation and the number of rows in a circular Florentine array. Such a connection is now well known and a lot of results on the families of sequences use this connection. Recently, we were able to generalize this into the cases for EVEN length and successfully identified the connection between a straight (not circular) Florentine rectangle and the size of family of perfect sequences with optimum cross-correlation. This talk will briefly summarize all these.

Biography

Hong-Yeop Song received the B.S. degree in electronic engineering from Yonsei University, Seoul, South Korea, in 1984, and the M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, CA, USA, in 1986 and 1991, respectively. He spent two years as a Research Associate with USC. He was a Senior Engineer in the Standard Team of Qualcomm Inc., San Diego, CA, for two years. Since September 1995, he has been with the Department of Electrical and Electronic Engineering, Yonsei University. His research interests include digital communications and channel coding, design and analysis of various pseudorandom sequences for communications, and cryptography. He is a member of the National Academy of Engineering of Korea (NAEK), the Mathematical Association of America (MAA), the Korean Mathematical Society (KMS), KICS, IEIE, and KIISC. He was awarded the 2017 Special Contribution Award from the Korean Mathematical Society and the 2021 S. J. Choi Award from the Korean Government, both for his contribution to the global wide-spread of the fact that S. J. Choi (1646–1715) from South Korea had discovered a pair of orthogonal Latin squares of order nine much earlier than Euler. He has participated in SETA almost every year since 2001 (Bergen, Norway) and co-edited the Proceedings of SETA 2004 and 2006. He served as the Chair of the IEEE IT Society Seoul Chapter from 2009 to 2016 and as the General Co-Chair for IEEE ITW 2015, Jeju, South Korea.

4.4 Tuesday, 22 September 2026

Bounds and Constructions for Orthogonal and Covering Arrays

Ferruh Özbudak
Sabancı University, Istanbul, Turkey

In an orthogonal array of strength t, every possible t-tuple occurs equally often in every projection onto t columns. A covering array requires only that each such tuple occur at least once. This weaker condition leads to rather different problems. We discuss bounds for mixed-level orthogonal arrays and, in particular, the equality cases of a generalized Bierbrauer–Friedman bound, described using a weighted Hamming multigraph. We then turn to covering-radius questions for orthogonal arrays, including arguments based on algebraic curves, and to a related connection between higher Sidon sets and covering radius. The final part concerns ongoing joint work with V. Potapov. We consider covering arrays constructed from systems of maps over finite abelian groups. Coverage of each selected projection is expressed as a surjectivity condition in a corresponding quotient. We describe several explicit examples and compare selected parameters with upper bounds listed in the literature.

Biography

Ferruh Özbudak is a Professor in the Faculty of Engineering and Natural Sciences at Sabancı University, Istanbul, Turkey. He obtained his B.Sc. in Electrical and Electronics Engineering (1993), M.Sc. in Mathematics (1995), and Ph.D. in Mathematics (1997), all from Bilkent University, Ankara, Turkey. Prior to his appointment at Sabancı University, he served as a professor of mathematics at Middle East Technical University (METU), where he also chaired the Cryptography Program at the Institute of Applied Mathematics for more than 15 years. He has received several recognitions, including the Mustafa Parlar Education and Research Foundation Research Award (2001), the Turkish Academy of Sciences Young Scientist Award (2004), the Prof. Masatoshi Gündüz Ikeda Science Award from the Mathematics Foundation (2009), the Alexander von Humboldt Research Fellowship (2012), and the Newton Mobility Grant Award from The Royal Society, UK (2018). He has visited several universities for research collaboration, including Anhui University in China, Universität Duisburg-Essen in Germany, National University of Singapore, Nanyang Technological University in Singapore, Tulane University in the USA, Aalborg University in Denmark, Loughborough University in the UK, and Otto von Guericke University Magdeburg in Germany. He is currently serving as an editor for *Advances in Mathematics of Communications* and *IEEE Transactions on Information Theory*. His research interests include algebraic curves, finite fields, coding theory, and cryptography.

4.5 Wednesday, 23 September 2026

Sequences with Good Periodic and/or Aperiodic Autocorrelation

Chunlei Li
University of Bergen, Norway

Sequences with optimally low periodic autocorrelations share deep, intrinsic connections with combinatorial designs, character sums over finite fields, as well as number theory. In digital communications, they serve as the cornerstone of sequence families with low periodic correlations, sequences with low aperiodic correlation, as well as sequences with low ambiguity for the emerging integrated sensing and communication systems. This talk will start by reviewing the foundational constructions, developments, and theoretical interconnections of sequences with optimally low periodic autocorrelation. We then present recent studies on polyphase sequences with zero autocorrelation, achieved via a permutation-based interleaving technique and raise some open problems for future research.

Biography

Chunlei Li (Senior Member, IEEE) received the Ph.D. degree from the University of Bergen, Norway, in 2014. He was a Postdoctoral Researcher with the University of Stavanger, Norway, from 2015 to 2017. He has been a Researcher with the Department of Informatics, University of Bergen, Norway, from 2017 to 2018, where he was an Associate Professor from 2018 to 2024 and has been a Professor since 2024. His research interests include sequence design, coding theory, and cryptography, particularly focusing on the fundamental problems and the interplay of these fields. He was the Program Co-Chair of the Workshops on Mathematical Methods for Cryptography in 2017, the Sequences and Their Applications (SETA) in 2020 and 2024, and the Norwegian Conference on Information Security in 2024 and 2025. He was a general co-chair for the European School of Information Theory. He served as a Program Committee Member for several workshops, including the International Workshops on the Arithmetic of Finite Fields (WAIFI 2018), SETA 2018/2026, Boolean Functions and their Applications (BFA 2020/2021/2022/2023/2024/2025/2026), Signal Designs and Applications (IWSDD 2019/2022/2025), Workshop on Coding and Cryptography (WCC 2022), and the IEEE Information Theory Workshop (ITW 2023/2024). He serves on the editorial board for the *Advances in Mathematics of Communications* (AIMS) journal and the *Designs, Codes and Cryptography* (Springer) journal. He has been serving on the board of the Norway Section Chapter of the IEEE Information Theory Society since 2024.

5 Abstracts of Contributed Talks

5.1 Saturday, 19 September 2026

Session 1 — Algebraic Aspects of Sequences and Codes

Constructions of Two-to-One Mappings over the Finite Field $\mathbb{F}_{2^{2m}}$

Jinfeng Chong, **Guohao Chen**, and Zepeng Zhuo

Two-to-one mappings over finite fields are widely used in algebra, combinatorics, coding theory and cryptography. With the 0/2 preimage distribution, they supply new options for symmetric cipher nonlinear components and support the design of few-weight linear codes, attracting wide attention recently. After Mesnager and Qu set up the basic criterion, many constructions for few-term two-to-one mappings have been proposed over finite fields of even characteristic.

This paper focuses on two-to-one mappings over $\mathbb{F}_{2^{2m}}$ and presents three main results. Firstly, six new infinite families of trinomials and quadrinomials are constructed, such as $F(x) = x^{\frac{(2^m+1)(2^m-2)}{3}+1} + wx^{2^m+1} + x^2$ and $F(x) = x^{2^{m+1}+1} + x^{2^m+2} + w^2x^2 + wx$. Secondly, we prove that $F(x) = x^{2^m+1} + cx$ is not a two-to-one mapping for any $c \in \mathbb{F}_{2^{2m}}$. Thirdly, a simplified verification method is given to convert preimage counting over the extension field into low-degree equation analysis over the subfield. Our work enriches the construction system and provides new materials for related research.

Some Notes on the Expansion Complexity of Pseudorandom Sequences

Hezheng Lin, Zhimin Sun, and Lingmei Xiao

We review relations between the i(irreducible)-expansion complexity and the linear complexity for finite length sequences and for eventually periodic sequences. We illustrate by examples that the i-expansion complexity and the 2-adic complexity complement each other. We obtain that how large is N when the Nth i-expansion complexity achieves maximum. An open problem is presented in the final section to prove that the average value of Nth i-expansion complexity over all binary sequences of length N is close to $N/2$ and the deviation from $N/2$ is at most of order of magnitude $\log(N)$.

Construction of Self-Orthogonal Codes and Their Applications

Fuling Chen, Dongchun Han, Cuiling Fan, and Sihem Mesnager

A linear code is called self-orthogonal if it is contained in its dual. Such codes play a key role in constructing quantum codes, LCD codes, and even lattices, but their construction remains challenging. In this paper, we construct p-ary self-orthogonal codes via defining sets, determine their parameters and weight distributions, and verify that they are p-ary self-orthogonal codes. Based on these codes, we further derive LCD codes and determine their parameters of the LCD codes.

Self-Orthogonal Twisted Generalized Reed-Solomon Codes and Their Application to Quantum Error-Correcting Codes

Yanxin Chen, Yanli Wang, and Tongjiang Yan

In this paper, two classes of twisted generalized Reed-Solomon (TGRS) codes with multi-twists are studied. Firstly, some sufficient and necessary conditions for these codes to be self-orthogonal and self-dual are established. Then several explicit constructions of self-orthogonal and self-dual codes are presented, from which quantum stabilizer codes are further derived. Finally, some corresponding examples are given, especially that some of these codes are MDS, AMDS or NMDS and that some of the resulting quantum stabilizer codes are optimal, achieving the quantum Singleton bound.

Session 2 — Correlation and Feedback Functions of Sequences

Sequences with Thirteen-valued Cross Correlations

Yuehui Cui and Jinquan Luo

In this paper, we completely determine the cross correlation distribution between an m-sequence (s_t) of period p^n-1 and its d-decimated sequence (s_{dt}), where $d=\frac{p^n-1}{3}+p^i$, $p\equiv 1 \pmod 3$, $\frac{1}{3}p^{-i}(p^n-1)\not\equiv 2 \pmod 3$, and $0\le i<n$. It is shown that the cross correlation is 13-valued. To the best of our knowledge, this is the first time that the cross correlation distribution of so many values has been determined.

On Almost Ideal Arithmetic Autocorrelation

Vladimir Edemskiy, **Feifei Yan**, and Pinhui Ke

In this paper, we study the existence of binary periodic sequences with almost ideal arithmetic autocorrelation, that is, whose absolute value equals one for all nonzero shifts. We prove that for a fixed index $d=(p-1)/\mathrm{ord}_p(2)$ (the multiplicative order of 2 modulo p), no such sequences exist for all sufficiently large primes p. Furthermore, for the case $p\equiv 3 \pmod 4$ and $d\le 50$, we show that if every sequence in the family has this property, then the only possible prime is $p=7$. These results indicate that sequences with almost ideal arithmetic autocorrelation are exceptionally rare.

On Determining Feedback Functions of Binary de Bruijn Sequences

Zuling Chang, Shujie Wang, and **Yunlong Zhu**

There are many constructions of de Bruijn sequences in the literature, and a useful one is the successor rule motivated by the cycle joining method (CJM). In this paper, we consider the problem of constructing feedback functions for de Bruijn sequences generated by the successor rule. This problem is challenging due to the complexity of the nonlinear feedback shift registers (NFSRs) that generate de Bruijn sequences. We first propose the generic structure of the feedback functions of de Bruijn sequences generated by the pure cycling register (PCR). Then we present two new classes of de Bruijn sequences based on the complementing circulating register (CCR) and obtain their explicit feedback functions. We propose generic forms of feedback functions for de Bruijn sequences of arbitrary order.

Session 3 — Complementary Sequences and Pairs

Residue loom for periodic complementary pairs

Weifeng Shang and Ilias Kotsireas

The union-of-orbits method, compression, and equivalence pruning have long been used in computational searches for combinatorial structures such as D-optimal matrices, Legendre pairs, and periodic Golay pairs. We develop a unified framework, called the residue loom, that organizes compression data together with subgroup symmetry in a matrix representation. In this representation, subgroup restrictions induce explicit equalities among compression values, allowing certain union-of-orbits spaces to be ruled out without enumerating full sequences. The induced equivalence actions on the residue loom give rise to partial sequence filling, an early pruning method together with a completeness result and an upper bound on its pruning power. These structural ingredients lead to search pipelines for Legendre pairs in subgroup-restricted spaces. Computationally, we carry out an exhaustive search over all nontrivial proper-subgroup union-of-orbits spaces of length 115 and show that none of them contains a Legendre pair. This approach also yields Legendre pairs in lengths 91, 93, and 123, and in particular the first known Legendre pairs for the previously open case of length 169. More broadly, the framework can be adapted to searches for other periodic complementary pairs.

A New Class of Optimal Binary Linear Complementary Pairs of Codes

Yansheng Wu and Jing Chen

Recently, the construction of optimal binary linear complementary pairs (LCPs) is becoming one hotspot in coding theory. Based on the Belov codes, this paper proposes a novel construction of optimal binary LCPs with $\theta = 4$, extending our previous work on $\theta = 3$. Our results not only yield abundant new optimal binary LCPs with flexible parameters, but also enable more optimal binary LCPs with smaller minimum distances.

Constructions of Complementary Sequence Sets of Non-Power-of-Two Lengths with Large Codebook Size

Yajing Zhou, Jiyu Yang, and **Hui Zhang**

This paper proposes two novel constructions of complementary sequence sets (CSSs) based on generalized Boolean functions (GBFs) to address the high peak-to-mean envelope power ratio (PMEPR) problem in Orthogonal Frequency Division Multiplexing (OFDM) systems. CSSs of non-power-of-two lengths ($L = 2^{m-1} + 2^v$) and size 2^{k+2} are successfully generated, with a PMEPR upper bound of 2^{k+2}. Compared with existing constructions, the proposed method significantly increases the codebook size and incorporates the construction of Chen [1] as a special case. The validity of the constructions is verified through concrete examples. This paper provides more flexible sequence design tools with larger codebook capacity for low-PMEPR coding in OFDM systems.

5.2 Sunday, 20 September 2026

Session 4 — Polyphase, Doppler-Resilient, and ZAZ Sequences

Two Novel Constructions of Asymptotically Optimal and Near-Optimal Periodic Doppler Resilient Complementary Sequence Sets

Xuanyu Liu, Pinhui Ke, and Zuling Chang

Sequences exhibiting favorable ambiguity function characteristics are of vital importance in radar detection systems and modern mobile communication applications. As a recently proposed family of sequences, Doppler resilient complementary sequence sets (DRCSSs) can significantly suppress the ambiguity function sidelobes via the coherent summation of the ambiguity functions of their constituent subsequences. In this paper, we propose two algebraic constructions for asymptotically optimal or asymptotically near-optimal periodic DRCSSs by employing perfect nonlinear (PN) or almost perfect nonlinear (APN) functions. These constructions yield asymptotically optimal and asymptotically near-optimal periodic DRCSSs with new parameters and large set sizes.

A Large Set of Polyphase Sequences with Low Correlation and Low Ambiguity Function

Xinpeng Bian, Avik Ranjan Adhikary, and Chunming Tang

Sequences with low correlation and low ambiguity function magnitude are fundamental to modern wireless communication and radar systems. In this paper, we propose a new construction of polyphase sequences over Galois rings, which generalizes a recent finite field construction based on Kloosterman sums to the ring setting. Our construction lies in the ability to generate a large family of sequences while maintaining low correlation and low ambiguity function magnitude simultaneously. We present a sequence set with period $p^n - 1$ and derive its exact size as $M_{(j,m)} \geq \frac{p^{en}(p^{en}-1)}{p^n-1}$, where p is any prime, and n and e are positive integers with $e < \frac{n+2}{2}$. We also provide upper bounds on both the maximum correlation magnitude and the maximum ambiguity magnitude.

Sarwate-Type Bounds for Polyphase Auto-ZAZ Sequences and Optimal Sequence Families

Mengshi Kao, Gaofei Wu, and Zilong Wang

This paper investigates the ambiguity-theoretic limits of polyphase sequences with optimal auto-zero-ambiguity-zone (auto-ZAZ) properties. Our first main result establishes a lower bound on the maximum cross-ambiguity magnitude between any pair of polyphase sequences sharing the same optimal auto-ZAZ configuration. This bound can be regarded as an extension of the classical Sarwate bound for perfect sequences from the correlation domain to the ambiguity-function domain. Then we define optimal families of polyphase auto-ZAZ sequences whose pairwise cross-ambiguity magnitudes attain the proposed bound. Our second main result derives an upper bound on the size of such optimal sequence families. This bound generalizes the upper bound established by Wang et al. (2022) for optimal families of perfect sequences to the broader setting of ambiguity-optimal auto-ZAZ sequence families. These results provide a theoretical framework for studying the tradeoffs among auto-ambiguity optimality, cross-ambiguity performance, and family size in polyphase sequence design.

New Bounds on the Partial Hamming Correlation of Multi-Timeslot Wide-Gap Frequency-Hopping Sequence Sets with Frequency Shift

Yidong Xiang, Xianhua Niu, Xing Liu, Siming Pang, Mingpeng Wang, Jianhong Zhao, and Hong Fu

Frequency-hopping sequences are widely used in anti-jamming and multiple-access communication systems, where Hamming correlation is a fundamental metric for evaluating frequency collisions. In practical systems, sweep jamming, adjacent-band interference, partial observation, burst transmission, imperfect synchronization, and frequency offset may lead to local collisions or interference hits within a finite observation window. To characterize such effects more accurately, this paper investigates multi-timeslot wide-gap frequency-hopping sequence sets with frequency shift under the time-frequency two-dimensional partial Hamming correlation framework. By jointly considering the multi-timeslot wide-gap constraint, the prescribed frequency-shift range, and the correlation window length, two new lower bounds on the maximum time-frequency two-dimensional partial Hamming correlation are derived. The proposed lower bounds can reduce to existing results under the corresponding parameter settings, and concrete examples show that these bounds are attainable.

Session 5 — Combinatorial Structures and Classical Codes

Duality in Periodic Sets

Minjia Shi, Mengru Yang, and **Patrick Solé**

A periodic set (PS) in Euclidean space is the union of a lattice and a finite number of its translates. PSs with formal duality properties have been known since the work of Cohn, Kumar, and Schürman (2009). We interpret their constructions in dimensions 1 and 6 as coming from Construction A applied to formally self-dual (FSD) non-linear $\mathbb{Z}_4$-codes for the symmetrized weight enumerator in three variables. We give transformation properties of the theta series of such PS, and extend them to PS obtained from Construction A applied to possibly FSD nonlinear binary codes for the weight enumerator in two variables.

Quinary Repeated-Root Cyclic Codes with Good Parameters

Yifan Tangfang, Gaojun Luo, Xiwang Cao, and Yihong Yang

Cyclic codes are widely used in data storage and communication systems. The construction of cyclic codes with optimal or good parameters holds considerable significance in academic research. In this paper, we focus on the constructions of quinary (5-ary) repeated-root cyclic codes with optimal or good parameters. Our approach reduces the design of a repeated-root cyclic code to selecting a nested chain of simple-root cyclic codes. By combining BCH codes with nested simple-root cyclic constituents, we explicitly construct several infinite families of quinary repeated-root cyclic codes. Specifically, a family with minimum distance 4 is proved to be distance-optimal with respect to the sphere-packing bound. Furthermore, additional families with minimum distances $d = 5, 6, 8$ are constructed, achieving good parameters compared with existing linear code tables.

On a Class of Ternary LCD BCH Codes

Mrinal Kanti Bose, **Udaya Parampalli**, and Abhay Kumar Singh

In modern communication systems, linear complementary dual (LCD) BCH codes are of paramount significance due to their dual capacity for highly efficient error correction and robust security against side-channel attacks. Comparing coset leaders, Huang et al. [3] introduced a new concept of absolute coset leaders, which provides advantages for constructing LCD BCH codes. Motivated by their approach, this article aims to investigate the structure of several ternary LCD BCH codes of length $n = \frac{3^{2m}-1}{8}$. Through a detailed analysis of 3-cyclotomic cosets modulo n, we explicitly compute the largest three absolute coset leaders. Utilizing these findings to characterize the defining sets, we present several new classes of ternary LCD BCH codes and determine the weight distributions for some of these codes.

Session 6 — Waveform and Data-Driven Sequence Design

Efficient Generation of Shorthand Universal Cycles for Permutations

Zuling Chang, Lingyu Diao, and **Jie Xue**

For a given integer n, a shorthand universal cycle for permutations is a sequence with period $n!$ satisfying that every $(n-1)$-permutation of $[n] = \{1, 2, \ldots, n\}$ appears exactly once as $n-1$ consecutive elements in it. In this paper, based on new representations of cycles containing $(n-1)$-permutations, new methods of efficiently generating shorthand universal cycles for permutations via the cycle joining method are proposed. Generating the next term in such universal cycles takes $O(n)$ memory and $O(1)$-amortized time.

A New Periodic Total Squared Correlation Bound and Nearly Optimal Constructions of Quaternary Signature Sets

Xuliang Wang, Bing Liu, Yuhang Che, Chao Qi, and Jianhong Zhou

We study the periodic total squared correlation (PTSC) of quaternary signature sets over $\{\pm 1, \pm j\}$. By introducing a cyclic expansion matrix, a lower bound on the PTSC is derived according to the parity of KN. Quaternary signature sets are constructed from binary sequences via the mapping $\phi(u, v) = \exp(\frac{\pi j}{2}(2u + v))$, and numerical results for both odd and even sequence lengths verify the parity-dependent behavior of the bound, showing that the constructed sets closely approach the proposed bound.

Waveform Design for Dual-Functional Radar-Communication Systems Based on Consensus-ADMM

Enbo Hu, Runze Liu, Xiaoyu Chen, and Yubo Li

Dual-functional radar-communication (DFRC) waveform design has attracted significant attention in recent years. The waveforms must simultaneously accommodate downlink multi-user communication and sensing while satisfying the constant modulus constraint (CMC), rendering the optimization problem highly complex. This paper proposes a novel Consensus-alternating direction method of multipliers (ADMM) framework that decouples communication and sensing subproblems through variable splitting. By deriving closed-form communication update expressions and embedding the L-BFGS method in the sensing module, the constant-modulus constraints are effectively addressed. Simulation results verify that the framework achieves stable convergence and outperforms benchmark algorithms in terms of bit error rate (BER), sum rate, and beampattern mean square error (MSE).

HpLSTM: An MOCSS Generation Method Based on Long and Short Term Memory Network and Discrete Hopfield Neural Network

Yuhang Che, Haiyi Zhao, and Bing Liu

Sequences play a crucial role in a wide range of engineering applications, and searching for sequences with desirable properties has long been a fundamental yet challenging research problem. In this paper, we propose a novel approach, termed HpLSTM, that leverages long short-term memory (LSTM) networks to algorithmically search for and generate sequences with target characteristics. Experimental results demonstrate that HpLSTM can successfully generate a large number of mutually orthogonal complementary sequence sets (MOCSSs), many of which are not present in the training set. Compared with the Hp-GAN approach, the proposed method achieves a generation scale improvement of approximately 21%, accelerates convergence by nearly 96%, and reduces the number of training rounds required for the first valid MOCSS generation from 2300 to a single iteration.

5.3 Monday, 21 September 2026

Session 7 — Wide-Gap and Low-Hit-Zone Frequency Hopping

New Constructions of Optimal One-Coincidence Wide-Gap Frequency-Hopping Sequence Set

Qianhui Wei, Xinyu Tian, and Xiaoyu Chen

Traditional frequency-hopping communication fails to achieve efficient and reliable data transmission due to increasingly congested spectrum resources, escalating complex interference, and dynamic communication link environments. To address this issue, this paper investigated one-coincidence wide-gap frequency-hopping sequence (OC-WGFHS) sets characterized by robust resistance to time-delay and follow jamming (FJ). The resultant OC-WGFHS sets demonstrate optimality against generalized Peng-Fan bound, while each individual sequence within the sets achieves optimality with respect to generalized Lempel-Greenberger bound. Compared with existing structures, the proposed OC-WGFHS sets exhibit extended sequence length, enhanced adjacent-frequency intervals, and flexible new parameters.

Constructions of Optimal or Near-Optimal Wide-Gap Low-Hit-Zone Frequency-Hopping Sequence Sets Via Interleaving Technique

Yuwei Chen, Yang Yang, Wei Su, and Udaya Parampalli

This paper aims to simultaneously mitigate multiple access interference (MAI) and follower jamming (FJ) in frequency-hopping multiple access (FHMA) systems by designing novel frequency-hopping sequences (FHSs). Conventional low-hit-zone FHSs (LHZ-FHSs) in quasi-synchronous FHMA systems can suppress MAI but remain susceptible to FJ. To overcome this limitation, we propose an improved scheme called wide-gap LHZ-FHSs (WG-LHZ-FHSs), which leverages adjacent carrier frequencies to combat both MAI and FJ. A general method for constructing WG-LHZ-FHSs is presented by using interleaving techniques, achieving optimal or near-optimal periodic Hamming correlation (PHC) performance.

New Constructions for Optimal Sets of Wide-Gap Frequency-Hopping Sequences with Low-Hit-Zone

Xiaoyan Chen, Avik Ranjan Adhikary, Zhengchun Zhou, and Udaya Parampalli

Low-hit-zone frequency-hopping sequence (LHZ-FHS) sets effectively suppress multi-access interference (MAI) in quasi-synchronous FHMA systems, but they remain vulnerable to follower jamming (FJ) attacks because neighboring carrier frequencies lack sufficient gaps. The recently introduced wide-gap LHZ-FHS (WG-LHZ-FHS) sets address both MAI and FJ simultaneously. In this paper, we propose a general framework for constructing WG-LHZ-FHS sets and derive three specific classes with optimal periodic Hamming correlation properties. Among them, two classes relax the restrictive conditions imposed in existing constructions, while the third class features entirely new parameters, thereby offering greater flexibility and broader applicability.

New Bounds on the Partial Hamming Correlation of Wide-Gap Low-Hit-Zone Frequency-Hopping Sequences with Frequency Shift

Kun Hu, **Hongyu Han**, and Sheng Zhang

In this paper, we generalize the concept of time frequency two dimensional partial Hamming correlation of wide-gap low-hit-zone frequency hopping sequences (TFTD-PHC-WG-LHZ-FHSs) with frequency shift by placing restrictions on the parameters. Then we derive new theoretical bounds on the maximum periodic Hamming correlation of TFTD-PHC-WG-LHZ-FHSs.

5.4 Tuesday, 22 September 2026

Session 8 — Codebooks and Frequency-Hopping Constructions

A Generic Construction of Complex Codebooks from Functions over Abelian Groups

Ziling Heng, **Chenkun Xie**, Jiantao Hu, and Xiaoyan Jing

This paper proposes two general constructions of complex codebooks based on functions over finite Abelian groups. By selecting perfect nonlinear functions, we systematically construct several families of codebooks that are optimal or asymptotically optimal with respect to the Levenshtein bound or the Welch bound. These two constructions not only cover some previously known optimal codebooks but also yield a number of codebooks with new parameters.

Compatible Permutations by Schur-Complement Extensions and Their Applications to NOMA Codebooks and MUBs

Chunlei Li, Constanza Riera, and Pantelimon Stănică

For a positive integer n and a permutation $\pi = [\pi(1), \ldots, \pi(n)]$, let $Q_\pi(x) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)}$ be the quadratic Boolean function attached to the Hamiltonian path Γ_π, which has vertices labeled by $1, \ldots, n$ and the form $\pi(1) - \cdots - \pi(n)$. Two permutations are compatible when their corresponding quadratic sums are bent in even dimension or near-bent in odd dimension. Large sets of pairwise compatible permutations are desired in the design of NOMA codebooks and mutually unbiased bases (MUBs).

This paper proposes a block-matrix framework for studying sets of pairwise permutations, termed compatible sets. We start with a Schur-complement criterion for extensions from S_n to S_{n+m} for even n and m. This criterion guides the construction and search of compatible permutation families by extension. Specifically, based on an observation that the Schur complements can be invariant under iterative extensions, we construct infinite families of L compatible permutations in dimension $n + tk$ with even integers n and t for an arbitrary integer $k \geq 1$, and provide illustrative instances with parameters $(n, t, L) \in \{(4, 4, 6), (6, 6, 8), (8, 8, 11), (6, 4, 6)\}$. We also explore more general extensions for obtaining larger compatible sets. By starting a dimension-6 compatible set of size 9 as a seed and conducting iterative extensions by dimension-4 permutations, we obtain compatible sets of size 9 in dimension $4k + 2$ for any $k \geq 1$. Finally, we point out that any even-dimensional compatible set can be extended to an odd-dimensional compatible set of the same size and also provide an upper bound on the maximal size of compatible sets in odd dimensions.

Optimal Frequency-Hopping Sequences from Partition-type Difference Family with Chaotically Enhanced Linear Complexity

Gejun Zhu, Shanding Xu, Tianyi Liu, and Xiangyong Feng

This paper proposes a frequency hopping sequence construction method based on partition-type difference families using the absolute trace function over finite fields for UAV networks. By partitioning the multiplicative group into subsets with a constant difference covering degree, the multiple-access interference is deterministically bounded. Furthermore, a chaotic bijective permutation algorithm is designed to elevate the linear complexity to a combinatorial lower bound $\binom{n}{k}$ while preserving the Hamming correlation properties. Simulation results demonstrate the superior performance of the proposed FHS sets in both frequency uniformity and linear complexity.

New Constructions of Optimal Frequency-Hopping Sequence Sets Based on a Refined Interleaving Framework

Xingyu Zheng and Zhengchun Zhou

We study constructions of frequency-hopping sequence (FHS) sets with optimal Hamming correlation and propose a refinement of the interleaving framework of Niu and Xing. For base constructions in which a distinguished position is occupied by a special symbol, the interleaving terms corresponding to this position are treated separately. The resulting FHS sets preserve the sequence length, the number of sequences, and the maximum Hamming correlation, while requiring a smaller alphabet size. This gives several optimal FHS sets with improved parameter sets. We further show that recursive applications of the refined framework produce parameter sets of the same form as those obtained by Zeng, Cai, Tang, and Yang from generalized cyclotomy.

Session 9 — Linear Codes, Hulls, and Projective Constructions

A New Family of Few-Weight Minimal Linear Codes via Bivariate Trace Functions

Tong Cui, Shanding Xu, and Gejun Zhu

Linear codes with few nonzero weights have important applications in cryptography, secret sharing, and combinatorial designs. This paper proposes a new construction of linear codes by combining bivariate trace codes with concatenated codes. The inner code is defined via a bivariate trace function over a carefully chosen defining set that imposes two trace conditions, while the outer code is an MDS code over an extension field. For odd extension degree, the resulting code is shown to be a four-weight minimal linear code with explicitly determined parameters; its two natural subcodes are two-weight codes. All constructed codes satisfy the Ashikhmin–Barg condition, making them directly applicable to democratic secret-sharing schemes.

Subfield Codes and Hull Dimensions of a Family of Projective Optimal Linear Codes

Liang Shao, Zhao Hu, and Nian Li

In this paper, we investigate the subfield codes and hull dimensions of a family of projective optimal linear codes over $\mathbb{F}_q$ constructed from general simplicial complexes. First, the exact parameters of their subfield codes are determined. Moreover, for simplicial complexes with two maximal elements, their parameters are derived in a more explicit form. By thoroughly studying the optimality of the resulting subfield codes, we obtain infinite families of subfield codes with small Griesmer defect over $\mathbb{F}_p$. Finally, we determine the hull dimensions of both the original codes and their subfield codes, and investigate their self-orthogonality. As a result, several families of self-orthogonal codes are constructed.

Several Classes of Linear Codes from Projective Spaces

Guangkui Xu, **Weiqi Wang**, and Heqian Xu

Linear codes with special properties have received considerable attention in the last decade because of their significant theoretical and practical applications. In this paper, we concentrate on linear codes from projective space. We construct several infinite families of q-ary linear codes, including some Griesmer codes, distance-optimal codes, and almost distance-optimal codes. The weight distributions of these codes are explicitly determined.

Double Cyclic Codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ and Their Application to EAQECC

Pinakin Dave and **Amit Sharma**

In this paper, we study double cyclic codes over the semisimple ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$, $u^2 = u$, $v^2 = v$, $uv = 0$. Using the idempotent decomposition of R, we determine the algebraic structure, generator polynomials, and generator matrices of these codes. We further investigate their hulls. For separable double cyclic codes, a Gray map is employed to obtain linear codes over $\mathbb{F}_q$. By utilizing the hulls of the Gray image codes, we construct new families of entanglement-assisted quantum error-correcting codes. Several examples are included to illustrate the constructions of the resulting EAQECCs.

Session 10 — Sequences, Codes, and Pseudorandomness (Online)

k-ary Legendre Pairs

Ilias Kotsireas, Huaning Liu, and Arne Winterhof

In this paper we study k-ary Legendre pairs. We provide some non-existence results and discuss constructions of Butson Hadamard matrices from Legendre pairs. Finally, we study ternary Legendre pairs in more detail and obtain them for (all possible) lengths $\ell \leq 26$.

Correlation Bounds and Markov Analysis for RO Based TRNGs

Miguel Alcocer-Pérez, Ana Isabel Gómez, and **Domingo Gómez-Pérez**

True Random Number Generators (TRNGs) based on ring oscillators require rigorous statistical validation to ensure cryptographic quality. While the Mauduit–Särközy k-th order correlation measure provides theoretical bounds on pseudorandomness, and Maurer's Universal Statistical Test offers empirical entropy assessment, no prior work has correlated these metrics. This paper focus on the relationship between Maurer's tests to 2nd-order correlation in this setting. First, we study the mathematical interplay of the two previous measures along with the behaviour of the high-order Markov chain transition probabilities in counter-based TRNGs and oscillator sampling architectures. Our results are computationally validated using data coming from the framework OpenTRNG and a hardware implementation. Initial results suggest a strong positive correlation between these tests. This fosters other questions relating to an improvement on the measuring of the quality of the statistical test early in the design phase before standardization.

New Classes of Binary Quantum CSS-T Codes Based on Plateaued Functions

Melike Çakmak, Sihem Mesnager, Ahmet Sınak, and Oğuz Yayla

Calderbank-Shor-Steane (CSS)-T codes have recently been introduced as a class of quantum error-correcting codes that admit a transversal implementation of the T gate, which is a crucial non-Clifford gate required for universal fault-tolerant quantum computation. Each CSS-T code is defined through a CSS-T pair consisting of two binary linear codes $(\mathcal{C}_1, \mathcal{C}_2)$ that satisfy specific algebraic conditions. In this work, we construct new families of binary linear codes derived from plateaued Boolean functions using the generalized second construction method. We show that these codes are minimal according to the Ashikhmin–Barg criterion, which highlights a link between fault-tolerant quantum computation and minimal linear codes and suggests possible applications to secret-sharing schemes. We explicitly determine the weight distributions of these codes. In addition, we use them to produce suitable CSS-T pairs. Our analysis proves that the constructed pairs $(\mathcal{C}_1, \mathcal{C}_2)$ satisfy the defining conditions of CSS-T codes. Consequently, the proposed construction yields new families of binary quantum CSS-T codes whose parameters are explicitly determined.

5.5 Wednesday, 23 September 2026

Session 11 — Sequence Complexity and Code Constructions

On the k-error Linear Complexity of the Ding-Helleseth-Martinsen Sequences

Jingwei Zhang, **Changan Zhao**, and Yunlong Zhu

Precise values have been established for the k-error linear complexity of the Ding-Helleseth-Martinsen sequences with period $2p$, provided that 2 is a primitive root modulo p. The result demonstrates the remarkable stability inherent in these sequences.

Trace Representation of Binary Sequences Derived from Euler Quotients Modulo pq^m

Jingwei Zhang and Changan Zhao

Let p and q be two distinct odd primes where $p \mid (q-1)$. In this paper, we define a family of binary sequences with period $pq^m + 1$ based on Euler quotients. This family generalizes the binary sequences derived from Euler quotients modulo pq. We then reduce the problem of determining their trace representations to that of finding the defining pairs of the sequences and their subsequences. Therefore, their linear complexity can be computed efficiently once these trace representations are determined.

Self-Orthogonal Codes over Non-Unital Non-Commutative Rings from Simplicial Complexes

Yan Wang, Tong Su, Xudong Wang, and Chenhuang Wu

Recently, the construction of optimal linear codes from simplicial complexes has garnered considerable attention, resulting in numerous excellent results. Let q be a prime power. In this paper, we construct five families of linear codes over the ring $a\mathbb{F}_{2^m} + c\mathbb{F}_{2^m}$ by employing simplicial complexes of $\mathbb{F}_q^m$ with a unique maximal element. The parameters and Lee weight distributions of these five families of codes are completely determined. Notably, several self-orthogonal codes are obtained via the Gray map. Furthermore, we investigate a subfield-like code associated with $\mathcal{C}_{\mathcal{L}}$ and derive several optimal and self-orthogonal codes from it.

Binary Goppa Codes with A_4 Automorphism Groups and Their Parameters

Tianni He, Kangquan Li, and Longjiang Qu

Goppa codes are a well-known class of linear codes with important applications in cryptography. Constructing Goppa codes with prescribed automorphism groups and determining their parameters are meaningful and challenging problems. In this paper, we construct binary Goppa codes and their related codes with A_4 automorphism groups. These constructions also naturally yield binary quasi-cyclic Goppa codes and their related codes. Moreover, we determine the dimensions and minimum distances of a class of these codes, and derive a sharper dimension lower bound for another class.

6 Introduction to Hubei University

Hubei University is a key comprehensive university in Wuhan, China, jointly supported by the Hubei Provincial Government and the Ministry of Education. It is included in national and provincial initiatives for first-class university development and in the national Basic Capacity Building Project for Universities in Central and Western China.

Founded in 1931 as Hubei Provincial College of Education, the University underwent several name changes and relocations before becoming Hubei University in 1984. For more than nine decades, it has remained rooted in Hubei and committed to education and talent development.

Located in Wuhan, Hubei University has three campuses—Wuchang, Changjiang New Area, and Hankou—on both banks of the Yangtze River. Covering more than 1,500 mu (about 100 hectares), the campuses provide an excellent environment for teaching, research, and campus life.

The University covers 13 major disciplinary categories, excluding military science, and has 26 schools and colleges. It offers 73 undergraduate programs, 11 first-level doctoral disciplines, 8 postdoctoral stations, 33 first-level master's disciplines, and 25 professional master's categories. Eight disciplines—Materials Science, Chemistry, Engineering, Plant & Animal Science, Environment/Ecology, Biology & Biochemistry, Geosciences, and Social Sciences—rank among the global top 1% in ESI. Sixteen disciplines appear in the U.S. News global subject rankings, and seven in the ShanghaiRanking Global Ranking of Academic Subjects.

The University has more than 23,000 full-time undergraduates and over 13,000 master's and doctoral students. It was among the first institutions in China to promote first-class undergraduate education, high-quality graduate education, top innovative talent cultivation, and integrated bachelor's, master's, and doctoral education. It has received 7 national and 113 provincial teaching achievement awards, developed 37 national and 118 provincial first-class undergraduate courses, and educated more than 400,000 graduates since its founding.

Hubei University has more than 1,700 faculty members, including over 1,000 with senior professional titles, more than 300 doctoral supervisors, and nearly 1,200 master's supervisors. It has more than 530 high-level talent appointments and honors at various levels.

The University hosts or participates in national and ministerial research platforms, including the National-Local Joint Engineering Research Center for High-Throughput Drug Screening Technology, a national demonstration base for innovative talent cultivation, and three Key Laboratories of the Ministry of Education. It also has more than 70 key provincial and municipal science and technology innovation platforms and 33 provincial- and ministerial-level humanities and social science research platforms. Since 2021, it has received four first prizes of the Hubei Provincial Science and Technology Awards, led three National Key Research and Development Program projects, and published four papers in total in the flagship journals *Cell*, *Nature*, and *Science*. It actively promotes technology transfer and cooperation with major enterprises.

Hubei University has a vibrant campus culture and has received national awards for campus and online culture. Its student futsal team has won the national league championship 11 times and represented China at the World University Futsal Championship. Its dragon and lion dance troupe has toured overseas nine times and won two world championship titles.

The University has partnerships with more than 190 universities and research institutions in over 60 countries and regions. It has established the Manchester Metropolitan Joint Institute with Manchester Metropolitan University in the UK and three Confucius Institutes and Classrooms in Brazil, São Tomé and Príncipe, and Poland. It admits international students on a rolling basis and offers the Chinese Government Scholarship, the International Chinese Language Teachers Scholarship, and the Hubei Provincial Government Scholarship.

Hubei University continues to strengthen its standing as a high-level comprehensive university with growing national recognition and international influence.