The 7th International Coding Theory Seminar

China (online)

June 27th, 2025

Contents

About

Organizing committee

China

Xiwang Cao
Lingfei Jin (vice chair)
Hongwei Liu (chair)
Gaojun Luo

India

Manish Gupta (chair)
Sartaj Ul Hasan
Anuradha Sharma

Japan

(TBA)

Korea

Whan-Hyuk Choi
Boran Kim
Jon-Lark Kim (chair)

Philippines

Rowena Betty
Romar dela Cruz
Lucky Galvez (chair)

Thailand

Arunwan Boripan
Parinyawat Choosuwan
Somphong Jitman (chair)
Ekkasit Sanwisut

Singapore

Fred Ezerman (chair)

International advisors

Nathan Kaplan (USA)

Patrick Sole (France)

Hong-Yeop Song (Korea)

Chaoping Xing (China)

Timetable

All times listed are in Beijing Standard Time (GMT+8).

Time: June 27th, 2025

Zoom ID: 275 839 8498

Password: 3bMnxY

13:00-14:00	**Committee Discussion**	
14:00–14:45	**Dongchun Han** Chengdu, China	Explicit Constructions of NMDS Self-dual Codes
14:45-15:00	**Discussion**	
15:00–15:45	**Gaojun Luo** Nanjing, China	Bounds and Constructions of Quantum Locally Recoverable Codes From Quantum CSS Codes
15:45–16:00	**Discussion**	
16:00–16:10	**Break**	
16:10–16:55	**Ziling Heng** Xi’an, China	Large Sets of Quasi-Complementary Sequences from Polynomials over Finite Fields and Gaussian Sums
16:55–17:10	**Discussion**	

List of Talks

Talk 1: Explicit Constructions of NMDS Self-dual Codes

Dongchun Han
School of Mathematics,
Southwest Jiaotong University, Chengdu 610000,
China
`han-qingfeng@163.com`

Biography
Dongchun Han received the B.S. and M.S. degrees from Sichuan University, Chengdu, China, in 2009, 2012 and the Ph.D. degree from Nankai University, Tianjin, China, in 2015, both in mathematics. He is currently an associate professor of Southwest Jiaotong University. His research interests include combinatorics, number theory and coding theory.

Abstract
Near maximum distance separable (NMDS) codes are important in finite geometry and coding theory. Self-dual codes are closely related to combinatorics, lattice theory, and have important application in cryptography. In this talk, we construct a class of q-ary linear codes and prove that they are either MDS or NMDS which depends on certain zero-sum condition. In the NMDS case, we provide an effective approach to construct NMDS self-dual codes which largely extend known parameters of such codes.

Bibiography

[1] S. Ball, *On sets of vectors of a finite vector space in which every subset of basis size is a basis*, J. Eur. Math. Soc. (JEMS) 14 (3) (2012) 733–748.
[2] A. Aguglia, L. Giuzzi and A. Sonnino, *Near-MDS codes from elliptic curves*, Des. Codes Cryptogr. 89 (2021) no. 5, 965–972.
[3] P. Beelen, S. Puchinger, J. Rosenkilde, *Twisted Reed-Solomon codes*, IEEE Trans. Inform. Theory 68 (5) (2022) 3047–3061.
[4] A.A. Bruen, J.A. Thas, A. Blokhuis,*On M.D.S. codes, arcs in $PG(n,q)$ with q even, and a solution of three fundamental problems of B. Segre*, Invent. Math. 92 (3) (1988) 441–459.
[5] M. Ceria, A. Cossidente, G. Marino and F. Pavese, *On near-MDS codes and caps*, Des. Codes Cryptogr. 91 (2023) no. 3, 1095–1110.
[6] C. Ding and C. Tang, *Infinite families of near MDS codes holding t-designs*, IEEE Trans. Inform. Theory 66 (9) (2020) 5419–5428.
[7] R. Dodunekova, S. M. Dodunekov and T. Klove, *Almost-MDS and near-MDS codes for error detection*, IEEE Trans. Inform. Theory 43 (1) (1997) 285–290.
[8] S. Dodunekov and I. Landjev, *On near-MDS codes*, J. Geometry 54 (1–2) (1994) 30–43.

[9] S. Dodunekov and I. Landjev, *Near-MDS codes over some small fields*, Discrete Math. 213 (1–3) (2000) 55–65.

[10] S. T. Dougherty, S. Mesnager and P. Sole, *Secret-sharing schemes based on self-dual codes*, in Proc. Inf. Theory Workshop, May 2008, pp. 338–342.

[11] X. Fang, M. Liu and J. Luo, *New MDS Euclidean self-orthogonal codes*, IEEE Trans. Inform. Theory 67 (1) (2021) 130–137.

[12] W. Fang and F. Fu, *New constructions of MDS Euclidean self-dual codes from GRS codes and extended GRS codes*, IEEE Trans. Inform. Theory 65 (9) (2019) 5574–5579.

[13] W. Fang, S. Xia and F. Fu, *Construction of MDS euclidean self-dual codes via two subsets*, IEEE Trans. Inform. Theory 67 (8) (2021) 5005–5015.

[14] H. Gu, and J. Zhang, *On twisted generalized Reed-Solomon codes with ℓ twists*, IEEE Trans. Inform. Theory 70 (1) (2024) 145–153.

[15] T.A. Gulliver, J.-L. Kim and Y. Lee, *New MDS and near-MDS self-dual codes*, IEEE Trans. Inform. Theory 54 (9) (2008) 4354–4360.

[16] Z. Heng, C. Li and X. Wang, *Constructions of MDS, near MDS and almost MDS codes from cyclic subgroups of $\mathbb{F}_{q^2}^*$*, IEEE Trans. Inform. Theory 68 (2022) no. 12, 7817–7831.

[17] D. Huang, Q. Yue, Y. Niu and X. Li, *MDS or NMDS self-dual codes from twisted generalized Reed-Solomon codes*, Des. Codes Cryptogr. 89 (9) (2021) 2195–2209.

[18] L. Jin and H. Kan, *Self-dual near MDS codes from elliptic curves*, IEEE Trans. Inform. Theory 65 (4) (2019) 2166–2170.

[19] L. Jin and C. Xing, *New MDS self-dual codes from generalized Reed-Solomon codes*, IEEE Trans. Inform. Theory 63 (3) (2017) 1434–1438.

[20] J. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A 105 (1) (2004) 79–95.

[21] I. Landjev and A. Rousseva, *The main conjecture for near-MDS codes*, in Proc. 9th Int. Workshop Coding Cryptogr. (WCC), 2015. [Online]. Available: https://hal.inria.fr/hal-01276222/document

[22] K. Lebed, H. Liu and J. Luo, *Construction of MDS self-dual codes over finite fields*, Finite Fields Appl. 59 (2019) 199–207.

[23] R. M. Roth and A. Lempel, *A construction of non-Reed-Solomon type MDS codes*, IEEE Trans. Inform. Theory 35 (3) (1989) 655–657.

[24] A. Zhang and K. Feng, *A unified approach to construct MDS self-dual codes via Reed-Solomon codes*, IEEE Trans. Inform. Theory 66 (6) (2020) 3650–3656.

Talk 2: Bounds and Constructions of Quantum Locally Recoverable Codes From Quantum CSS Codes

Gaojun Luo
School of Mathematics,
Nanjing University of Aeronautics and Astronautics, Nanjing 210016,
China
gaojun_luo@nuaa.edu.cn

Biography
Gaojun Luo received the Ph.D. degree in mathematics from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2019. From Feb 2021 to Mar 2024, he was a Research Fellow with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

He is currently a Faculty Member with the School of Mathematics, Nanjing University of Aeronautics and Astronautics. His research interests include sequences, quantum information theory and coding theory. He is on the editorial board of Computational and Applied Mathematics.

Abstract
Classical locally recoverable codes (LRCs) have become indispensable in distributed storage systems. They provide efficient recovery in terms of localized errors. Quantum LRCs have very recently been introduced for their potential application in quantum data storage. In this paper, we use classical LRCs to investigate quantum LRCs. We prove that the parameters of quantum LRCs are bounded by their classical counterparts. We deduce bounds on the parameters of quantum LRCs from bounds on the parameters of the classical ones. We establish a characterization of optimal pure quantum LRCs based on classical codes with specific properties. Using well-crafted classical LRCs as ingredients in the construction of quantum CSS codes, we offer the first construction of several families of optimal pure quantum LRCs.

Bibiography

[1] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inform. Theory*, vol. 58, no. 11, pp. 6925–6934, Nov. 2012.

[2] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Optimal linear codes with a local-error-correction property," in *Proc. IEEE Int. Symposium Inform. Theory (ISIT)*, Cambridge, MA, USA, 2012, July 1–6, pp. 2776–2780. [Online]. Available: https://doi.org/10.1109/ISIT.2012.6284028

[3] V. R. Cadambe and A. Mazumdar, "Bounds on the size of locally recoverable codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 11, pp. 5787–5794, Nov. 2015.

[4] I. Tamo, A. Barg, and A. Frolov, "Bounds on the parameters of locally recoverable codes," *IEEE Trans. Inform. Theory*, vol. 62, no. 6, pp. 3070–3083, June 2016.

[5] J. Hao, S.-T. Xia, K. W. Shum, B. Chen, F.-W. Fu, and Y. Yang, "Bounds and constructions of locally repairable codes: Parity-check matrix approach," *IEEE Trans. Inform. Theory*, vol. 66, no. 12, pp. 7465–7474, Dec. 2020.

[6] L. Jin, “Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes,” *IEEE Trans. Inform. Theory*, vol. 65, no. 8, pp. 4658–4663, Aug. 2019.

[7] B. Chen and J. Huang, “A construction of optimal (r, δ) locally recoverable codes,” *IEEE Access*, vol. 7, pp. 180 349–180 353, 2019.

[8] C. Xing and C. Yuan, “Construction of optimal (r, δ)-locally recoverable codes and connection with graph theory,” *IEEE Trans. Inform. Theory*, vol. 68, no. 7, pp. 4320–4328, July 2022.

[9] G. Zhang, “A new construction of optimal (r, δ) locally recoverable codes,” *IEEE Communications Letters*, vol. 24, no. 9, pp. 1852–1856, Sep. 2020.

[10] I. Tamo, A. Barg, S. Goparaju, and R. Calderbank, “Cyclic LRC codes and their subfield subcodes,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, 2015, June 14–19. [Online]. Available: `https://doi.org/10.1109/ISIT.2015.7282658`.

[11] B. Chen, S.-T. Xia, J. Hao, and F.-W. Fu, “Constructions of optimal cyclic (r, δ) locally repairable codes,” *IEEE Trans. Inform. Theory*, vol. 64, no. 4, pp. 2499–2511, Apr. 2018.

[12] J. Qian and L. Zhang, “New optimal cyclic locally recoverable codes of length $n = 2(q + 1)$,” *IEEE Trans. Inform. Theory*, vol. 66, no. 1, pp. 233–239, Jan. 2020.

[13] Y. Luo, C. Xing, and C. Yuan, “Optimal locally repairable codes of distance 3 and 4 via cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 65, no. 2, pp. 1048–1053, Feb. 2019.

[14] L. Golowich and V. Guruswami, “Quantum locally recoverable codes,” in Proc. 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), New Orleans, Louisiana, U.S.A, 2025, January 12–15, pp. 5512–5522. [Online]. Available: `https://epubs.siam.org/doi/abs/10.1137/1.9781611978322.188` and `https://arxiv.org/pdf/2311.08653.pdf`

[15] I. Tamo and A. Barg, “A family of optimal locally recoverable codes,” *IEEE Trans. Inform. Theory*, vol. 60, no. 8, pp. 4661–4676, Aug. 2014.

[16] D. E. Gottesman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, 1997. [Online]. Available: `https://resolver.caltech.edu/CaltechETD:etd-07162004-113028`

[17] A. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, “Quantum error correction via codes over $GF(4)$,” *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, July 1998.

[18] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4892–4914, Nov. 2006.

[19] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting codes*. Cambridge Univ. Press, 2003.

[20] S. Ling and C. Xing, *Coding Theory: A First Course*. Cambridge Univ. Press, Feb. 2004.

[21] D. Schipani, M. Elia, and J. Rosenthal, “On the decoding complexity of cyclic codes up to the BCH bound,” in *Proc. IEEE Int. Symposium Inform. Theory (ISIT)*. St. Petersburg, Russia: IEEE, 2011, July 31–August 05, pp. 835–839. [Online]. Available: `https://doi.org/10.1109/ISIT.2011.6034253`

[22] R. Bose and D. Ray-Chaudhuri, “On a class of error correcting binary group codes,” *Information and Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960.

[23] A. Hocquenghem, “Codes correcteurs d’erreurs,” *Chiffers*, vol. 2, pp. 147–156, 1959.

[24] P. Delsarte, “On subfield subcodes of modified Reed-Solomon codes (corresp.),” *IEEE Trans. Inform. Theory*, vol. 21, no. 5, pp. 575–576, Sep. 1975.

Talk 3: Large Sets of Quasi-Complementary Sequences From Polynomials over Finite Fields and Gaussian Sums

Ziling Heng
School of Science,
Chang'an University, Xi'an 710064,
China
zilingheng@chd.edu.cn

Biography

Ziling Heng received the B.Sc. degree in mathematics from Henan Normal University, Xinxiang, China, in 2012, and the Ph.D. degree in mathematics from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2017. From July 2017 to July 2018, he was a Post-Doctoral Fellow with The Hong Kong University of Science and Technology, Hong Kong, China. He is currently a Professor with the School of Science, Chang'an University, Xi'an, China. His research interests include coding theory and sequences and he has published more than 55 papers in these fields.

Abstract

Perfect complementary sequence sets (PCSSs) are widely used in multi-carrier code-division multiple-access (MC-CDMA) communication systems. However, the set size of a PCSS is upper bounded by the number of row sequences of each two-dimensional matrix in the PCSS. Then quasi-complementary sequence sets (QCSSs) were proposed to support more users in MC-CDMA communications. For practical applications, it is desirable to construct an $(M, K, N, \vartheta_{\max})$-QCSS with M as large as possible and $\vartheta_{\max}$ as small as possible, where M is the number of matrices with K rows and N columns in the set and $\vartheta_{\max}$ denotes its periodic tolerance. Nevertheless, there exists a tradeoff among these parameters. Constructing QCSSs achieving or nearly achieving the known correlation lower bound has been an interesting research topic. Up to now, only a few constructions of asymptotically optimal or near-optimal periodic QCSSs have been reported in the literature. In this talk, we first propose three new constructions of periodic QCSSs with large set sizes, low periodic tolerances and small alphabet size p from some polynomials over finite fields. These QCSSs are asymptotically optimal or near-optimal with respect to the correlation lower bound. Then we present a generic construction of periodic QCSSs containing the three constructions as special cases. Besides, we also give a construction of asymptotically optimal periodic QCSSs from multiplicative and additive characters of finite fields. Their periodic tolerances are determined by Gaussian sums. Each family of the constructed QCSSs in this talk has set size $\Theta(K^2)$ or $\Theta(K^3)$ for some flock size K. To the best of our knowledge, only a small amount of known families of periodic QCSSs with set size $\Theta(K^2)$ have been constructed and most of other known periodic QCSSs have set sizes much smaller than $\Theta(K^2)$. Our new constructed periodic QCSSs with set size $\Theta(K^2)$ have better parameters than some known QCSSs in the literature. They have larger set sizes or lower periodic tolerances. The periodic QCSSs with set size $\Theta(K^3)$ constructed by us have the largest set size among all known families of asymptotically optimal or near-optimal periodic QCSSs.

Bibiography

[1] A. W. Bluher, “On $x^{q+1}+ax+b$,” *Finite Fields Appl.*, vol. 10, no. 3, pp. 285-305, 2004.

[2] A. R. Adhikary, Y. Feng, Z. Zhou, and P. Fan, “Asymptotically optimal and near-optimal aperiodic quasi-complementary sequence sets based on Florentine rectangles,” *IEEE Trans. Commun.*, vol. 70, no. 3, pp. 1475–1485, Mar. 2022.

[3] A. R. Adhikary, H. Zhang, Z. Zhou, Q. Wang and S. Mesnager, “Quasi complementary sequence sets: new bounds and optimal constructions via quasi-Florentine rectangles,” *IEEE Trans. Inf. Theory*, vol. 71, no. 3, pp. 2271-2291, March 2025.

[4] H.-H. Chen, J.-F. Yeh, and N. Suehiro, “A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications,” *IEEE Commun. Mag.*, vol. 39, no. 10, pp. 126-135, 2001.

[5] H.-H. Chen, *The Next Generation CDMA Technologies*. Hoboken, NJ, USA: Wiley, 2007.

[6] J. A. Davis, J. Jedwab, “Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-M$\ddot{u}$ller codes,” *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397-2417, 1999.

[7] P. Fan, W. Yuan, and Y. Tu, “Z-complementary binary sequences,” *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 509-512, 2007.

[8] K. H. Kim and S. Mesnager, "Solving $x^{2k+1}+x+a=0$ in $\mathbb{F}_2^n$ with $\gcd(n,k)=1$," *Finite Fields Appl.*, vol. 63, Art. no. 101630, 2020.

[9] J. Li, A. Huang, M. Guizani, and H.-H. Chen, “Inter-group complementary codes for interference-resistant CDMA wireless communications,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 166-174, 2008.

[10] Y. Li, T. Liu, and C. Xu, "Constructions of asymptotically optimal quasi-complementary sequence sets," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1516-1519, Aug. 2018.

[11] Y. Li, L. Tian, T. Liu, and C. Xu, "Two constructions of asymptotically optimal quasi-complementary sequence sets," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 1910-1924, Mar. 2019.

[12] Y. Li, L. Tian, T. Liu, and C. Xu, "Constructions of quasi-complementary sequence sets associated with characters," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4597-4608, Jul. 2019.

[13] Y. Li, T. Yan, and C. Lv, "Construction of a near-optimal quasi-complementary sequence set from almost difference set," *Cryptogr. Commun.*, vol. 11, no. 4, pp. 815-824, 2019.

[14] Y. Li, L. Tian, and C. Xu,“Constructions of asymptotically optimal aperiodic quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7499–7511, Nov. 2019.

[15] Z. Liu, Y. Guan, B. C. Ng, and H. H. Chen, “Correlation and set size bounds of complementary sequences with low correlation zone,” *IEEE Trans. Commun.*, vol. 59, no. 12, pp. 3285-3289, 2011.

[16] Z. Liu, U. Parampalli, Y. L. Guan, and S. Boztas, “Constructions of optimal and near-optimal quasi-complementary sequence sets from singer difference sets,” *IEEE Wireless Commun. Lett.*, vol. 2, no. 5,pp. 487-490, Oct. 2013.

[17] Z. Liu, Y. L. Guan, and W. H. Mow, “A tighter correlation lower bound for quasi-complementary sequence sets,” *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 388-396, 2014.

[18] T. Liu, C. Xu, and Y. Li, “Multiple complementary sequence sets with low inter-set cross-correlation property,” *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 913–917, Jun. 2019.

[19] G. Luo, X. Cao, M. Shi, and T. Helleseth, "Three new constructionsof asymptotically optimal periodic quasi-complementary sequence setswith small alphabet sizes," *IEEE Trans. Inf. Theory*, vol. 67, no. 8,pp. 5168-5177, Aug. 2021.

[20] R. Lidl, H. Niederreiter. *Finite Fields*. Cambridge: Cambridge University Press, 1997.

[21] A. Pezeshki, A. R. Calderbank, W. Moran, and S. D. Howard, “Doppler Resilient Golay Complementary Waveforms,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4254-4266, 2008.

[22] K. Pommerening. Quadratic Equations in Finite Fields of Characteristic 2. [Online]. Available: https://www.staff.uni-mainz.de/ pommeren/MathMisc/QuGlChar2.pdf.

[23] P. Spasojevic and C. N. Georghiades, “Complementary sequences for ISI channel estimation,” *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1145-1152, 2001.

[24] P. Sarkar, C. Li, S. Majhi, and Z. Liu, “New correlation bound and construction of quasi-complementary sequence sets,” *IEEE Trans. Inf. Theory*, vol. 70, no. 3, pp. 2201–2223, Mar. 2024.

[25] B. Shen, T. Yu, Z. Zhou and Y. Yang. “Asymptotically optimal aperiodic quasi-complementary sequence sets based on extended Boolean functions,” *Des. Codes Cryptogr.*, vol. 92, pp. 4213-4230, 2024.

[26] C. C. Tseng, C. L. Liu, “Complementary sets of sequences,” *IEEE Trans. Inf. Theory*, vol. IT-18, no. 5, pp. 644-652, 1972.

[27] M. Wang, T. Liu, M. Liu and Y. Li, “Two constructions of aperiodic quasi-complementary sequence sets with new parameters,” *IEEE Trans. Commun.*, vol. 73, no. 1, pp. 93-102, Jan. 2025.

[28] L. Welch, “Lower bounds on the maximum cross correlation of signals (Corresp.),” *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397-399, 1974.

[29] H. Xiao, G. Luo and X. Cao, “New Constructions of asymptotically optimal quasi-complementary sequence sets with small alphabet sizes," *IEEE Trans. Commun.*, 2024, doi: 10.1109/TCOMM.2024.3524020.

[30] G. Xu, X. Cao and L. Qu, "Infinite families of 3-designs and 2-designs from almost MDS codes," *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4344-4353, Jul. 2022.

[31] Z. Zhou, F. Liu, A. R. Adhikary, and P. Fan, “A generalized construction of multiple complete complementary codes and asymptotically optimal aperiodic quasi-complementary sequence sets,” *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3564–3571, Jun. 2020.