Rank-Metric Codes and Their Applications

Other titles in Foundations and Trends® in Communications and Information Theory

Asymptotic Frame Theory for Analog Coding
Marina Haikin, Matan Gavish, Dustin G. Mixon and Ram Zamir
ISBN: 978-1-68083-908-1

Modeling and Optimization of Latency in Erasure-coded Storage Systems
Vaneet Aggarwal and Tian Lan
ISBN: 978-1-68083-842-8

An Algebraic and Probabilistic Framework for Network Information Theory
S. Sandeep Pradhan, Arun Padakandla and Farhad Shirani
ISBN: 978-1-68083-766-7

Theoretical Foundations of Adversarial Binary Detection
Mauro Barni and Benedetta Tondi
ISBN: 978-1-68083-764-3

Polynomial Methods in Statistical Inference
Yihong Wu and Pengkun Yang
ISBN: 978-1-68083-730-8

Information-Theoretic Foundations of Mismatched Decoding
Jonathan Scarlett, Albert Guillen i Fabregas, Anelia Somekh-Baruch and Alfonso Martinez
ISBN: 978-1-68083-712-4

Rank-Metric Codes and Their Applications

Hannes Bartz
German Aerospace Center (DLR)
hannes.bartz@dlr.de

Lukas Holzbaur
Technical University of Munich
lukas.holzbaur@tum.de

Hedongliang Liu
Technical University of Munich
lia.liu@tum.de

Sven Puchinger
Hensoldt Sensors GmbH
mail@svenpuchinger.de

Julian Renner
Technical University of Munich
julian.renner@tum.de

Antonia Wachter-Zeh
Technical University of Munich
antonia.wachter-zeh@tum.de

the essence of knowledge
Boston — Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

H. Bartz *et al.*. *Rank-Metric Codes and Their Applications.* Foundations and Trends® in Communications and Information Theory, vol. 19, no. 3, pp. 390–546, 2022.

ISBN: 978-1-63828-001-9

Foundations and Trends® in Communications and Information Theory

Volume 19, Issue 3, 2022

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Communications and Information Theory publishes survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2022, Volume 19, 4 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328 . Also available as a combined paper and online subscription.

Contents

Rank-Metric Codes and Their Applications

Hannes Bartz[1], Lukas Holzbaur[2], Hedongliang Liu[2], Sven Puchinger[3], Julian Renner[2] and Antonia Wachter-Zeh[2]

[1] *German Aerospace Center (DLR); hannes.bartz@dlr.de*
[2] *Technical University of Munich; lukas.holzbaur@tum.de, lia.liu@tum.de, julian.renner@tum.de, antonia.wachter-zeh@tum.de*
[3] *Hensoldt Sensors GmbH; mail@svenpuchinger.de*

ABSTRACT

The rank metric measures the distance between two matrices by the rank of their difference. Codes designed for the rank metric have attracted considerable attention in recent years, reinforced by network coding and further motivated by a variety of applications. In code-based cryptography, the hardness of the corresponding generic decoding problem can lead to systems with reduced public-key size. In distributed data storage, codes in the rank metric have been used repeatedly to construct codes with locality, and in coded caching, they have been employed for the placement of coded symbols. This survey gives a general introduction to rank-metric codes, explains their most important applications, and highlights their relevance to these areas of research.

Hannes Bartz, Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, Julian Renner and Antonia Wachter-Zeh (2022), "Rank-Metric Codes and Their Applications", Foundations and Trends® in Communications and Information Theory: Vol. 19, No. 3, pp 390–546. DOI: 10.1561/0100000119.

1

Introduction

Codes composed of matrices are a natural generalization of codes composed of vectors. Codes in the rank metric of length $n \leq m$ can be considered as a set of $m \times n$ matrices over a finite field $\mathbb{F}_q$ or equivalently as a set of vectors of length n over the extension field $\mathbb{F}_{q^m}$. The rank weight of each codeword vector is the rank of its matrix representation and the rank distance between two matrices is the rank of their difference. These definitions rely on the fact that the rank distance is indeed a metric. Several code constructions and basic properties of the rank metric show strong similarities to codes in the Hamming metric. However, there are also notable differences, e.g., in the list decoding properties.

Error-correcting codes in the rank metric were first considered by Delsarte [64], who proved a Singleton-like upper bound on the cardinality of rank-metric codes and constructed a class of codes achieving this bound[1]. This class of codes was reintroduced by Gabidulin [78] in his fundamental paper *"Theory of Codes with Maximum Rank Distance"*. Further, in his paper several properties of codes in the rank metric and

[1] In analogy to MDS codes, such codes are called Maximum Rank Distance (MRD) codes.

an efficient decoding algorithm based on an equivalent of the Euclidean algorithm were shown. Since Gabidulin's publication contributed significantly to the development of error-correcting codes in the rank metric, the most famous class of codes in the rank metric — the equivalents of Reed–Solomon codes — are nowadays called *Gabidulin codes*. These codes can be defined by evaluating non-commutative linearized polynomials, proposed by Ore [201], [202]. Independently of the previous work, Roth [241] discovered in 1991 codes in the rank metric and applied them for correcting crisscross error patterns.

The goal of this survey is to provide an overview of the known properties of rank-metric codes and their application to problems in different areas of coding theory and cryptography.

Section 2 provides a brief introduction to rank-metric codes, their properties and their decoding. After providing basic notations for finite fields and linearized polynomials, we consider codes in the rank metric. We first define the rank metric and give basic properties and bounds on the cardinality of codes in the rank metric (namely, equivalents of the Singleton, sphere-packing, and the Gilbert–Varshamov bounds). Then, we define Gabidulin codes, show that they attain the Singleton-like upper bound on the cardinality and give their generator and parity-check matrices. We describe their decoding up to half the minimum rank-distance by syndrome-based decoding. A summary of how to accomplish this efficiently is given and the problem of error-erasure correction is considered. We also give an overview on list decoding of Gabidulin codes and consider interleaved and folded Gabidulin codes. Finally, further classes of rank-metric codes such as twisted Gabidulin codes are briefly discussed.

Rank-metric codes have several applications in communications and security, including public-key code-based cryptography. In 1978, Rivest, Shamir and Adleman (RSA) [239] proposed the first public-key cryptosystem in order to guarantee secure communication in an asymmetric manner. Since then, public-key cryptography is essential to protect data via encryption, to enable secure key exchange for symmetric encryption, and to protect the authenticity and integrity of data via digital signature schemes. Only one year after the RSA cryptosystem was introduced, whose security relies on the hardness of the integer factorization problem, McEliece [186] proposed the first public key cryptosystem based on error-correcting codes. In his pioneering work McEliece showed that hard problems in coding theory can be used to derive public-key cryptosystems. A crucial drawback of the McEliece cryptosystem compared to other public-key cryptosystems, such as RSA or elliptic curve cryptosystems (ECC), is its large public-key size. The recent developments in quantum computing rendered all of the currently used public-key cryptosystems whose security relies on the integer factorization or the discrete logarithm problem insecure. In particular, Shor's algorithm [250] allows to solve both the integer factorization problem and the discrete logarithm problem in polynomial time, which in turn allows to break the corresponding public-key cryptosystems completely, given a sufficiently large quantum computer. Since code-based public-key cryptosystems are resilient against all known attacks on quantum computers, including Shor's algorithm, they are considered to be *quantum-resistant* (or post-quantum secure) cryptosystems.

Quantum-resistant cryptography is an important research area to ensure the long-term security of transmitted and stored data. Therefore, the National Institute of Standards and Technology (NIST) opened a standardization call, which meanwhile has reached its final round [200]. In order to reduce the public-key size, many new McEliece variants based on several codes were proposed, both before and independent of the NIST competition and also as submissions to the NIST competition. This includes a long history of variants based on codes in the rank metric. The first McEliece variant in the rank metric was proposed by Gabidulin, Paramonov, and Tretjakov [85] and is therefore known as the GPT cryptosystem. Although no rank-metric based schemes are among the finalists, rank-metric based schemes are considered as potential candidates for future standards [6].

Section 3 gives an overview of rank-metric code-based quantum-resistant encryption and authentication schemes. First, hard problems which can be used to design rank-metric code-based cryptosystems are considered. Then, a general framework to define most GPT variants is given, and the particular variants are described. Finally, an overview on non-GPT-like cryptosystems, including the NIST submission Rank Quasi Cyclic (RQC), and rank-metric code-based signature schemes is given.

Rank-metric codes find applications not only in the cryptographic protection of data, but also in ensuring its integrity. The increase in the amount of data that is stored by distributed storage systems has motivated a transition from replication of the data to the use of more involved storage codes, most commonly Maximum Distance Separable (MDS) codes. By storing one symbol of a codeword on each node, a node failure then corresponds to a symbol erasure and the Hamming distance of the storage code provides a guarantee on the number of failures the system can tolerate before data loss occurs. However, as the number of nodes in these systems grows, not only the number of tolerable node failures, but also the efficiency of the node repair process becomes a concern. Codes with locality [53], [111], [133] address this issue by reducing the number of nodes required for repair in the more likely event of a single or small number of node failures. While these codes are designed for the Hamming metric, codes for the rank metric, in particular, Gabidulin codes have repeatedly been used to construct these codes, especially for the stronger notion of maximally recoverable (MR) locally repairable/recoverable codes (LRCs)[2]. Further, rank-metric codes have also been used in another area related to distributed storage, referred to as coded caching. Caching is a commonly used strategy to reduce the traffic rate during the peak hours. The communication procedure consists of two phases: placement and delivery. The seminal work by Maddah-Ali and Niesen [178] has shown that applying coding merely in the delivery phase can reduce the traffic rate. As a further improved scheme [277] has been shown to be order-optimal under uncoded placement, schemes with coded placement [54], [108] become of interest in order to further reduce the traffic rate during the delivery phase. Rank-metric codes have been utilized in the scheme with coded placement by Tian and Chen [262], which has been shown to outperform the optimal scheme with uncoded placement [277] in the regime of small cache size.

In Section 4, the application of rank-metric codes to distributed data storage is outlined. First, we explore the connection between codes with locality and rank-metric codes by providing a high-level description of

[2]MR LRCs are also referred to as partial MDS (PMDS) codes.

the property exploited by many constructions of (MR) LRCs. Second, we present the application of Maximum Rank Distance (MRD) codes in the coded caching scheme by Tian and Chen [262].

Network coding has been attracting attention since the fundamental works by Ahlswede *et al.* [5] and Li, Yeung, and Cai [161] showed that the capacity of multicast networks can be achieved by performing linear combinations of packets instead of just forwarding them. Rank-metric codes have been used in network coding solutions [74] and error correction in coherent networks [256]. For random networks, rank-metric codes are used to correct errors by the lifting construction [258]. In addition, the subspace metric [150] was introduced for error control, as this metric perfectly captures the type of errors that occur in (random) linear network coding. Due to the close relation between the rank metric and the subspace metric, rank-metric codes are a natural choice to construct subspace codes for error control in random network coding.

Section 5 introduces constructions of network codes based on MRD codes, constructions of subspace codes by lifting rank-metric codes, bounds on the cardinality, and the list decoding capability of subspace codes. We first present constructions based on MRD codes for a class of deterministic multicast networks, which guarantee that all the receivers decode all the messages. Two error models commonly considered in networks are described. We introduce subspace codes, with a focus on constructions based on lifting rank-metric codes and provide upper bounds on the size of subspace codes. Further, an analysis of list decoding subspace codes is provided.

Finally, Section 6 concludes this survey and shortly mentions further applications of rank-metric codes.

References

[1] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Transactions on Information Theory*, vol. 46, no. 7, 2000, pp. 2373–2395.

[2] C. Aguilar Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, A. Hauteville, A. Otmani, O. Ruatta, J. Tillich, and G. Zemor, "ROLLO - rank-ouroboros, LAKE & LOCKER," *Second round submission to the NIST post-quantum cryptography call*, 2019, URL: https://pqc-rollo.org.

[3] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, G. Zemor, A. Couvreur, and Hauteville, "Rank quasi cyclic (RQC)," *Second round submission to the NIST post-quantum cryptography call*, 2019, URL: https://pqc-rqc.org.

[4] C. Aguilar-Melchor, O. Blazy, J. Deneuville, P. Gaborit, and G. Zémor, "Efficient encryption from random quasi-cyclic codes," *IEEE Transactions on Information Theory*, vol. 64, no. 5, May 2018, pp. 3927–3943. DOI: 10.1109/TIT.2018.2804444.

[5] R. Ahlswede, N. Cai, S. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, Aug. 2000, pp. 1204–1216.

[6] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, C. Miller, D. Moody, R. Peralta, R. Perlner, A. R. andDaniel Smith-Tone, and Y.-K. Liu, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," US Department of Commerce, NIST, Tech. Rep., Jul. 2020.

[7] A. A. Albert, "Generalized twisted fields," *Pacific J. Math*, vol. 11, no. 1, 1961, pp. 1–8.

[8] P. Almeida and D. Napp, "A new rank metric for convolutional codes," *Designs, Codes and Cryptography*, vol. 89, no. 1, 2021, pp. 53–73.

[9] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, S. Gueron, T. Güneysu, C. Aguilar Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J. Tillich, V. Vasseur, and G. Zemor, "BIKE - bit flipping key encapsulation," *Second round submission to the NIST post-quantum cryptography call*, 2019, URL: https://pqc-rollo.org.

[10] N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, and G. Zémor, "Durandal: a rank metric based signature scheme," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 728–758, 2019.

[11] N. Aragon and P. Gaborit, "A key recovery attack against LRPC using decryption failures," in *Coding and Cryptography, International Workshop, WCC*, vol. 2019, 2019.

[12] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor, "Low rank parity check codes: new decoding algorithms and applications to cryptography," *IEEE Transactions on Information Theory*, vol. 65, no. 12, 2019, pp. 7697–7717.

[13] N. Aragon, P. Gaborit, A. Hauteville, and J.-P. Tillich, "A new algorithm for solving the rank syndrome decoding problem," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2421–2425, 2018.

[14] D. Augot and M. Finiasz, "A public key encryption scheme based on the polynomial reconstruction problem," *LNCS: Revised selected papers of EUROCRYPT 2003*, vol. 2656, 2003, pp. 229–249.

[15] D. Augot, P. Loidreau, and G. Robert, "Rank metric and Gabidulin codes in characteristic zero," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013. arXiv: 1305.4047.

[16] D. Augot, P. Loidreau, and G. Robert, "Generalized Gabidulin codes over fields of any characteristic," *Designs, Codes and Cryptography*, vol. 86, no. 8, 2018, pp. 1807–1848.

[17] S. Balaji and P. V. Kumar, "On partial maximally-recoverable and maximally-recoverable codes," in *2015 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1881–1885, 2015.

[18] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani, "Enhanced public key security for the McEliece cryptosystem," *Journal of Cryptography*, vol. 29, no. 1, 2016, pp. 1–27.

[19] M. Baldi, K. Khathuria, E. Persichetti, and P. Santini, "Cryptanalysis of a code-based signature scheme based on the Lyubashevsky framework," Cryptology ePrint Archive, Report 2020/905, https://eprint. iacr. org/2020/905, Tech. Rep., 2020.

[20] M. Bardet and P. Briaud, "An algebraic approach to the rank support learning problem," *CoRR*, vol. abs/2103.03558, 2021. arXiv: 2103.03558, URL: https://arxiv.org/abs/2103.03558.

[21] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J.-P. Tillich, "An algebraic attack on rank metric code-based cryptosystems," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 64–93, 2020.

[22] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J.-P. Tillich, and J. A. Verbel, "Improvements of algebraic attacks for solving the rank decoding and Min-Rank problems," in *Advances in Cryptology - ASIACRYPT 2020*, ser. Lecture Notes in Computer Science, vol. 12491, pp. 507–536, Springer, 2020.

[23] D. Bartoli, M. Giulietti, and I. Platoni, "On the covering radius of mds codes," *IEEE Transactions on Information Theory*, vol. 61, no. 2, 2014, pp. 801–811.

[24] D. Bartoli, C. Zanella, and F. Zullo, "A new family of maximum scattered linear sets in $\mathrm{PG}(1, q^6)$," *arXiv preprint arXiv:1910.02278*, 2019.

[25] H. Bartz, "Algebraic Decoding of Subspace and Rank-Metric Codes," Ph.D. dissertation, Technische Universität München, 2017.

[26] H. Bartz, T. Jerkovits, S. Puchinger, and J. Rosenkilde, "Fast decoding of codes in the rank, subspace, and sum-rank metric," *IEEE Transactions on Information Theory*, vol. 67, no. 8, 2021, pp. 5026–5050. DOI: 10.1109/TIT.2021.3067318.

[27] H. Bartz and V. Sidorenko, "List and probabilistic unique decoding of folded subspace codes," in *IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, Jun. 2015. DOI: 10.1109/ISIT.2015.7282407.

[28] H. Bartz and V. Sidorenko, "Algebraic decoding of folded Gabidulin codes," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, 2017, pp. 449–467.

[29] H. Bartz and A. Wachter-Zeh, "Efficient interpolation-based decoding of interleaved subspace and Gabidulin codes," in *52nd Annual Allerton Conference on Communication, Control, and Computing*, pp. 1349–1356, Monticello, IL, Sep. 2014. DOI: 10.1109/ALLERTON.2014.7028612.

[30] H. Bartz and A. Wachter-Zeh, "Efficient decoding of interleaved subspace and Gabidulin codes beyond their unique decoding radius using gröbner bases," *Advances in Mathematics of Communications*, vol. 12, no. 4, 2018, p. 773.

[31] L. A. Bassalygo, "New upper bounds for error correcting codes," *Probl. Inf. Transm.*, vol. 1, no. 4, 1965, pp. 41–44.

[32] T. P. Berger, "Isometries for rank distance and permutation group of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 49, no. 11, 2003, pp. 3016–3019.

[33] T. P. Berger, P. Gaborit, and O. Ruatta, "Gabidulin matrix codes and their application to small ciphertext size cryptosystems," in *International Conference in Cryptology in India*, Springer, pp. 247–266, 2017.

[34] E. R. Berlekamp, *Algebraic Coding Theory.* Aegean Park Press, Jun. 1984.

[35] D. Bernstein, T. Chou, T. Lange, I. Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang, "Classic McEliece," *Second round submission to the NIST post-quantum cryptography call*, 2019, URL: https://classic.mceliece.org.

[36] I. Blanco-Chacón, E. Byrne, I. Duursma, and J. Sheekey, "Rank metric codes and zeta functions," *Designs, Codes and Cryptography*, vol. 86, no. 8, 2018, pp. 1767–1792.

[37] M. Blaum, J. L. Hafner, and S. Hetzler, "Partial-MDS codes and their application to RAID type of architectures," *IEEE Transactions on Information Theory*, vol. 59, no. 7, 2013, pp. 4510–4519.

[38] M. Blaum, J. S. Plank, M. Schwartz, and E. Yaakobi, "Construction of partial MDS and sector-disk codes with two global parity symbols," *IEEE Transactions on Information Theory*, vol. 62, no. 5, 2016, pp. 2673–2681.

[39] M. Bombar and A. Couvreur, "Decoding supercodes of Gabidulin codes and applications to cryptanalysis," *arXiv preprint arXiv: 2103.02700*, 2021.

[40] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew cyclic codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 18, no. 4, Aug. 2007.

[41] D. Boucher and F. Ulmer, "Linear codes using skew polynomials with automorphisms and derivations," *Designs, Codes and Cryptography*, Jun. 2012, pp. 1–27. DOI: 10.1007/s10623-012-9704-4.

[42] D. Boucher and F. Ulmer, "Codes as modules over skew polynomial rings," in *Cryptography and Coding*, ser. Lecture Notes in Computer Science, M. Parker, Ed., vol. 5921, Springer, 2009, pp. 38–55. DOI: 10.1007/978-3-642-10868-6_3.

[43] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *J. Symbolic Comput.*, vol. 44, no. 12, Dec. 2009, pp. 1644–1656. DOI: 10.1016/j.jsc.2007.11.008.

[44] E. Byrne, G. Cotardo, and A. Ravagnani, "Rank-metric codes, generalized binomial moments and their zeta functions," *Linear Algebra and its Applications*, vol. 604, 2020, pp. 92–128.

[45] E. Byrne and A. Ravagnani, "Covering radius of matrix codes endowed with the rank metric," *SIAM Journal on Discrete Mathematics*, vol. 31, no. 2, 2017, pp. 927–944.

[46] E. Byrne and A. Ravagnani, "Partition-balanced families of codes and asymptotic enumeration in coding theory," *Journal of Combinatorial Theory, Series A*, vol. 171, 2020, p. 105 169.

[47] N. Cai and R. W. Yeung, "Network coding and error correction," in *IEEE Information Theory Workshop (ITW)*, pp. 119–122, Oct. 2002. DOI: 10.1109/ITW.2002.1115432.

[48] N. Cai and R. W. Yeung, "Network error correction, II: lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, 2006, pp. 37–54.

[49] G. Calis and O. O. Koyluoglu, "A general construction for PMDS codes," *IEEE Communications Letters*, vol. 21, no. 3, 2016, pp. 452–455.

[50] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, Mar. 2006, pp. 777–788.

[51] F. Chabaud and J. Stern, "The cryptographic security of the syndrome decoding problem for rank distance codes," in *Advances in Cryptology — ASIACRYPT '96*, K. Kim and T. Matsumoto, Eds., pp. 368–381, Berlin, Heidelberg: Springer Berlin Heidelberg, 1996.

[52] L. Chaussade, P. Loidreau, and F. Ulmer, "Skew codes of prescribed distance or rank," *Designs, Codes and Cryptography*, vol. 50, no. 3, Mar. 2009, pp. 267–284. DOI: 10.1007/s10623-008-9230-6.

[53] M. Chen, C. Huang, and J. Li, "On the maximally recoverable property for multi-protection group codes," in *2007 IEEE International Symposium on Information Theory*, IEEE, pp. 486–490, 2007.

[54] Z. Chen, P. Fan, and K. B. Letaief, "Fundamental limits of caching: improved bounds for users with small buffers," *IET Communications*, vol. 10, no. 17, 2016, pp. 2315–2318.

[55] D. Coggia and A. Couvreur, "On the security of a Loidreau's rank metric code based encryption scheme," in *Workshop on Coding and Cryptography (WCC)*, 2019.

[56] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes.* Elsevier, 1997.

[57] G. Cohen, M. Karpovsky, H. Mattson, and J. Schatz, "Covering radius—survey and recent results," *IEEE Transactions on Information Theory*, vol. 31, no. 3, 1985, pp. 328–343.

[58] J.-M. Couveignes and R. Lercier, "Elliptic periods for finite fields," *Finite Fields and Their Applications*, vol. 15, no. 1, 2009, pp. 1–22.

[59] J. de la Cruz, M. Kiermaier, A. Wassermann, and W. Willems, "Algebraic structures of MRD codes," *Advances in Mathematics of Communications*, vol. 10, no. 3, 2016, pp. 499–510.

[60] B. Csajbók, G. Marino, O. Polverino, and C. Zanella, "A new family of MRD-codes," *Linear Algebra and its Applications*, vol. 548, 2018, pp. 203–220.

[61] B. Csajbók, G. Marino, O. Polverino, and Y. Zhou, "MRD codes with maximum idealizers," *Discrete Mathematics*, vol. 343, no. 9, 2020, p. 111 985.

[62] B. Csajbók, G. Marino, and F. Zullo, "New maximum scattered linear sets of the projective line," *Finite Fields and Their Applications*, vol. 54, 2018, pp. 133–150.

[63] T. Debris-Alazard, N. Sendrier, and J.-P. Tillich, *Wave: A new code-based signature scheme*, 2018. arXiv: 1810.07554.

[64] P. Delsarte, "Bilinear forms over a finite field with applications to coding theory," *Journal of Combinatorial Theory*, vol. 25, no. 3, 1978, pp. 226–241.

[65] L. E. Dickson, "On finite algebras," *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, vol. 1905, 1905, pp. 358–393.

[66] L. E. Dickson, "On commutative linear algebras in which division is always uniquely possible," *Transactions of the American Mathematical Society*, vol. 7, no. 4, 1906, pp. 514–522.

[67] Y. Ding, "On list-decodability of random rank metric codes and subspace codes," *IEEE Transactions on Information Theory*, vol. 61, no. 1, Jan. 2015, pp. 51–59. DOI: 10.1109/TIT.2014.2371915.

[68] Y. Ding, "On list-decodability of random rank metric codes and subspace codes," *IEEE Transactions on Information Theory*, vol. 61, no. 1, 2015, pp. 51–59.

[69] F. R. K. Djomou, H. T. Kalachi, and E. Fouotsa, "Generalization of low rank parity-check (LRPC) codes over the ring of integers modulo a positive integer," *Arabian Journal of Mathematics*, 2021, pp. 1–10.

[70] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, Jun. 2007, pp. 1949–1969.

[71] J. B. Ebrahimi and C. Fragouli, "Algebraic algorithms for vector network coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, Feb. 2011, pp. 996–1007.

[72] M. Elleuch, A. Wachter-Zeh, and A. Zeh, "A public-key cryptosystem from interleaved Goppa codes," *arXiv preprint arXiv: 1809.03024*, 2018.

[73] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, Feb. 2011, pp. 1165–1173.

[74] T. Etzion and A. Wachter-Zeh, "Vector network coding based on subspace codes outperforms scalar linear network coding," *IEEE Transactions on Information Theory*, vol. 64, no. 4, 2018, pp. 2460–2473.

[75] C. Faure and P. Loidreau, "A new public-key cryptosystem based on the problem of reconstructing p–polynomials," in *International Workshop on Coding and Cryptography*, Springer, pp. 304–315, 2005.

[76] A. Fikes. (2010). "Storage Architecture and Challenges." URL: https://cloud.google.com/files/storage_architecture_and_challenges.pdf.

[77] M. A. Forbes and A. Shpilka, "On identity testing of tensors, low-rank recovery and compressed sensing," in *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, ACM, pp. 163–172, 2012.
[78] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, 1985, pp. 3–16.
[79] E. M. Gabidulin, M. Bossert, and P. Lusina, "Space-time codes based on rank codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, p. 284, Sorrento, Italy, 2000.
[80] E. M. Gabidulin and N. I. Pilipchuk, "Symmetric Rank Codes," *Probl. Inf. Transm.*, vol. 40, no. 2, 2004, pp. 103–117.
[81] E. M. Gabidulin, "Attacks and counter-attacks on the GPT public key cryptosystem," *Designs, Codes and Cryptography*, vol. 48, no. 2, 2008, pp. 171–177.
[82] E. M. Gabidulin, "On public-key cryptosystems based on linear codes: efficiency and weakness.," in *4th IMA Conference on Cryptography and Coding*, IMA Press, 1993.
[83] E. M. Gabidulin and A. V. Ourivski, "Modified GPT PKC with right scrambler," *Electronic Notes in Discrete Mathematics*, vol. 6, 2001, pp. 168–177.
[84] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Transactions on Information Theory*, vol. 49, no. 12, 2003, pp. 3289–3293.
[85] E. M. Gabidulin, A. Paramonov, and O. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, pp. 482–489, 1991.
[86] E. M. Gabidulin, H. Rashwan, and B. Honary, "On improving security of GPT cryptosystems," in *2009 IEEE International Symposium on Information Theory*, IEEE, pp. 1110–1114, 2009.
[87] E. M. Gabidulin, "A fast matrix decoding algorithm for rank-error-correcting codes," *Algebraic Coding*, Lecture Notes in Computer Science, vol. 573, 1992, pp. 126–133.
[88] E. M. Gabidulin, *Rank Codes*, V. Sidorenko, Ed. München: TUM.University Press, 2021.

[89] E. M. Gabidulin and N. I. Pilipchuk, "Symmetric matrices and codes correcting rank errors beyond the [(d-1)/2] bound," *Discrete Applied Mathematics*, vol. 154, no. 2, 2006, pp. 305–312.

[90] E. M. Gabidulin and N. I. Pilipchuk, "Error and erasure correcting algorithms for rank codes," *Designs, Codes and Cryptography*, vol. 49, no. 1-3, 2008, pp. 105–122.

[91] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the rank syndrome decoding problem," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, Feb. 2016, pp. 1006–1019. DOI: 10.1109/TIT.2015.2511786.

[92] P. Gaborit, A. Hauteville, D. H. Phan, and J.-P. Tillich, "Identity-based encryption from codes with rank metric," in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds., pp. 194–224, Cham: Springer International Publishing, 2017.

[93] P. Gaborit, A. Hauteville, D. H. Phan, and J.-P. Tillich, "Identity-based encryption from codes with rank metric," in *Annual International Cryptology Conference*, Springer, pp. 194–224, 2017.

[94] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *Int. Workshop Coding Cryptogr. (WCC)*, pp. 168–180, Bergen, Norway, Apr. 2013.

[95] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the rank syndrome decoding problem," *IEEE Transactions on Information Theory*, vol. 62, no. 2, 2015, pp. 1006–1019.

[96] P. Gaborit and G. Zémor, "On the hardness of the decoding and the minimum distance problems for rank codes," *IEEE Transactions on Information Theory*, vol. 62, no. 12, 2016, pp. 7245–7252. DOI: 10.1109/TIT.2016.2616127.

[97] R. Gabrys, E. Yaakobi, M. Blaum, and P. H. Siegel, "Constructions of partial MDS codes over small fields," *IEEE Transactions on Information Theory*, vol. 65, no. 6, 2018, pp. 3692–3701.

[98] M. Gadouleau and Z. Yan, "Properties of codes with the rank metric," in *IEEE Global Telecomm. Conf. (GLOBECOM)*, pp. 1–5, San Francisco, CA, USA, Nov. 2006. DOI: 10.1109/glocom.2006.173.

[99] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Transactions on Information Theory*, vol. 56, no. 7, Jul. 2010, pp. 3207–3216. DOI: 10.1109/TIT.2010.2048447.

[100] M. Gadouleau and Z. Yan, "Packing and covering properties of rank metric codes," *IEEE Transactions on Information Theory*, vol. 54, no. 9, 2008, pp. 3873–3883.

[101] M. Gadouleau and Z. Yan, "MacWilliams identity for codes with the rank metric," *EURASIP journal on wireless communications and networking*, vol. 2008, 2008, pp. 1–13.

[102] M. Gadouleau and Z. Yan, "Bounds on covering codes with the rank metric," *IEEE Communications Letters*, vol. 13, no. 9, 2009, pp. 691–693.

[103] S. Gao, "A new algorithm for decoding Reed–Solomon codes," *Commun. Inf. Network Sec.*, vol. 712, 2003, pp. 55–68.

[104] K. Gibson, "Severely denting the Gabidulin version of the McEliece public key cryptosystem," *Designs, Codes and Cryptography*, vol. 6, no. 1, 1995, pp. 37–45.

[105] K. Gibson, "The security of the Gabidulin public key cryptosystem," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 212–223, 1996.

[106] M. Giesbrecht, "Factoring in skew-polynomial rings over finite fields," *J. Symb. Computation*, vol. 26, no. 4, Oct. 1998, pp. 463–486. DOI: 10.1006/jsco.1998.0224.

[107] H. Gluesing-Luerssen, "On the sparseness of certain linear mrd codes," *Linear Algebra and its Applications*, vol. 596, 2020, pp. 145–168. DOI: https://doi.org/10.1016/j.laa.2020.03.006.

[108] J. Gómez-Vilardebó, "Fundamental limits of caching: Improved rate-memory tradeoff with coded prefetching," *IEEE Transactions on Communications*, vol. 66, no. 10, Oct. 2018, pp. 4488–4497. DOI: 10.1109/TCOMM.2018.2834364.

[109] P. Gopalan, G. Hu, S. Kopparty, S. Saraf, C. Wang, and S. Yekhanin, "Maximally recoverable codes for grid-like topologies," in *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, SIAM, pp. 2092–2108, 2017.

[110] P. Gopalan, C. Huang, B. Jenkins, and S. Yekhanin, "Explicit maximally recoverable codes with locality," *IEEE Transactions on Information Theory*, vol. 60, no. 9, 2014, pp. 5245–5256.

[111] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Transactions on Information theory*, vol. 58, no. 11, 2012, pp. 6925–6934.

[112] E. Gorla, *Rank-metric codes*, 2019. arXiv: 1902.02650 [cs.IT].

[113] E. Gorla and A. Ravagnani, "Codes endowed with the rank metric," in *Network Coding and Subspace Designs*, Springer, 2018, pp. 3–23.

[114] A. Gruica and A. Ravagnani, "Common complements of linear subspaces and the sparseness of mrd codes," *SIAM Journal on Applied Algebra and Geometry, to appear.*, 2020. arXiv: 2011.02993.

[115] Q. Guo, T. Johansson, and P. Stankovski, "A key recovery attack on MDPC with CCA security using decoding errors," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, pp. 789–815, 2016.

[116] V. Guruswami and A. Rudra, "Explicit codes achieving list decoding capacity: error-correction with optimal redundancy," *IEEE Transactions on Information Theory*, vol. 54, no. 1, 2008, pp. 135–150.

[117] V. Guruswami and C. Wang, "Linear-algebraic list decoding for variants of Reed-Solomon codes," *IEEE Transactions on Information Theory*, vol. 59, no. 6, 2013, pp. 3257–3268. DOI: 10.1109/TIT.2013.2246813.

[118] V. Guruswami, S. Narayanan, and C. Wang, "List decoding subspace codes from insertions and deletions," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS)*, pp. 183–189, Cambridge, Massachusetts, 2012. DOI: 10.1145/2090236.2090252.

[119] V. Guruswami and C. Wang, "Explicit rank-metric codes list-decodable with optimal redundancy," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 20, 2013.

[120] V. Guruswami and C. Wang, “Explicit rank-metric codes list-decodable with optimal redundancy,” *CoRR*, vol. abs/1311.7084, 2013. arXiv: 1311.7084, URL: http://arxiv.org/abs/1311.7084.

[121] V. Guruswami, C. Wang, and C. Xing, “Explicit list-decodable rank-metric and subspace codes via subspace designs,” *IEEE Transactions on Information Theory*, vol. 62, no. 5, 2016, pp. 2707–2718.

[122] Y. Hassan and V. R. Sidorenko, “Fast recursive linearized feedback shift register synthesis,” in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pp. 162–167, Novosibirsk, Russia, Sep. 2010.

[123] A. Hauteville and J.-P. Tillich, “New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2747–2751, 2015.

[124] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Transactions on Information Theory*, vol. 52, no. 10, Oct. 2006, pp. 4413–4430. DOI: 10.1109/TIT.2006.881746.

[125] L. Holzbaur, H. Liu, S. Puchinger, and A. Wachter-Zeh, “On decoding and applications of interleaved Goppa codes,” in *2019 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1887–1891, 2019.

[126] L. Holzbaur, S. Puchinger, E. Yaakobi, and A. Wachter-Zeh, “Correctable erasure patterns in product topologies,” in *2021 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2021.

[127] L. Holzbaur, S. Puchinger, E. Yaakobi, and A. Wachter-Zeh, “Partial MDS codes with regeneration,” *IEEE Transactions on Information Theory*, 2021. DOI: 10.1109/TIT.2021.3091455.

[128] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal, “Extension of Overbeck’s attack for Gabidulin-based cryptosystems,” *Designs, Codes and Cryptography*, vol. 86, no. 2, 2018, pp. 319–340.

[129] A.-L. Horlemann-Trautmann and K. Marshall, "New criteria for MRD and Gabidulin codes and some rank-metric code constructions," *Advances in Mathematics of Communications*, vol. 11, no. 3, 2017, pp. 533–548.

[130] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal, "Considerations for rank-based cryptosystems," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2544–2548, 2016.

[131] A.-L. Horlemann-Trautmann and A. Neri, "A complete classification of partial-MDS (maximally recoverable) codes with one global parity," *Advances in Mathematics of Communications*, vol. 14, no. 1, 2020, pp. 69–88.

[132] G. Hu and S. Yekhanin, "New constructions of SD and MR codes over small finite fields," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1591–1595, 2016.

[133] C. Huang, M. Chen, and J. Li, "Pyramid codes: flexible schemes to trade space for access efficiency in reliable data storage systems," in *Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007)*, pp. 79–86, Jul. 2007. DOI: 10.1109/NCA.2007.37.

[134] N. Jacobson, *The Theory of Rings*. American Mathematical Society, Dec. 1943.

[135] N. Jacobson, *Finite-Dimensional Division Algebras over Fields*, 1st ed. 1996. Corr. 2nd printing 2009. Springer, Jan. 2010.

[136] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, Jun. 2005, pp. 1973–1982. DOI: 10.1109/TIT.2005.847712.

[137] T. Jerkovits, V. Sidorenko, and A. Wachter-Zeh, "Decoding of Space-Symmetric Rank Errors," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 658–663, 2021. DOI: 10.1109/ISIT45174.2021.9518115.

[138] S. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inf. Theory*, vol. 8, no. 3, Apr. 1962, pp. 203–207. DOI: 10.1109/TIT.1962.1057714.

[139] R. Jurrius and R. Pellikaan, “On defining generalized rank weights,” *arXiv preprint arXiv:1506.02865*, 2015.

[140] S. Kadhe, S. El Rouayheb, I. Duursma, and A. Sprintson, “Codes with locality in the rank and subspace metrics,” *IEEE Transactions on Information Theory*, vol. 65, no. 9, 2019, pp. 5454–5468.

[141] W. K. Kadir and C. Li, “On decoding additive generalized twisted Gabidulin codes,” *Cryptography and Communications*, vol. 12, no. 5, 2020, pp. 987–1009.

[142] W. K. Kadir, C. Li, and F. Zullo, “On interpolation-based decoding of a class of maximum rank distance codes,” *arXiv preprint arXiv:2105.03115*, 2021.

[143] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, “Codes with local regeneration and erasure correction,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, 2014, pp. 4637–4660.

[144] H. T. Kamche, H. T. Kalachi, F. R. K. Djomou, and E. Fouotsa, “Low-rank parity-check codes over finite commutative rings and application to cryptography,” *arXiv preprint arXiv:2106.08712*, 2021.

[145] H. T. Kamche and C. Mouaha, “Rank-metric codes over finite principal ideal rings and applications,” *IEEE Transactions on Information Theory*, vol. 65, no. 12, 2019, pp. 7718–7735.

[146] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, “XORs in the air: practical wireless network coding,” *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, 2008, pp. 497–510. DOI: 10.1109/TNET.2008.923722.

[147] A. Khaleghi, D. Silva, and F. R. Kschischang, “Subspace codes,” in *Cryptography and Coding*, ser. Lecture Notes in Computer Science, vol. 5921, 2009, pp. 1–21. DOI: 10.1007/978-3-642-10868-6_1.

[148] M. Kim, M. Médard, and J. Barros, "Modeling network coded tcp throughput: a simple model and its validation," in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, ser. VALUETOOLS '11, pp. 131–140, Paris, France: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[149] D. E. Knuth, "Finite semifields and projective planes," Ph.D. dissertation, California Institute of Technology, 1963.

[150] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, Jul. 2008, pp. 3579–3591. DOI: 10.1109/TIT.2008.926449.

[151] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theor.*, vol. 54, no. 8, Aug. 2008, pp. 3579–3591. DOI: 10.1109/TIT.2008.926449.

[152] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, 2003, pp. 782–795. DOI: 10.1109/TNET.2003.818197.

[153] V. Y. Krachkovsky and Y. X. Lee, "Decoding for iterative Reed-Solomon coding schemes," *IEEE Transactions on Magnetics*, vol. 33, no. 5, Sep. 1997, pp. 2740–2742. DOI: 10.1109/20.617715.

[154] J. Lavauzelle, P. Loidreau, and B.-D. Pham, "RAMESSES, a rank metric encryption scheme with short keys," 2019, URL: http://arxiv.org/abs/1911.13119.

[155] J. Lavauzelle and J. Renner, "Cryptanalysis of a system based on twisted reed–solomon codes," *Designs, Codes and Cryptography*, vol. 88, no. 7, 2020, pp. 1285–1300.

[156] P. Lefèvre, P. Carré, and P. Gaborit, "Application of rank metric codes in digital image watermarking," *Signal Processing: Image Communication*, vol. 74, 2019, pp. 119–128.

[157] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proceedings of the 15th annual ACM-SIAM symposium on discrete algorithms (SODA2004), New Orleans, LA, USA*, pp. 142–150, Jan. 2004.

[158] J. B. Lewis and A. H. Morales, "Rook theory of the finite general linear group," *Experimental Mathematics*, vol. 29, no. 3, 2020, pp. 328–346. DOI: 10.1080/10586458.2018.1470045.

[159] C. Li, "Interpolation-based decoding of nonlinear maximum rank distance codes," in *2019 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2054–2058, 2019.

[160] C. Li and W. Kadir, "On decoding additive generalized twisted Gabidulin codes," in *International Workshop on Coding and Cryptography (WCC)*, 2019.

[161] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, Feb. 2003, pp. 371–381. DOI: 10.1109/TIT.2002.807285.

[162] W. Li, V. Sidorenko, and D. Silva, "On transform-domain error and erasure correction by Gabidulin codes," *Designs, Codes and Cryptography*, vol. 73, 2014, pp. 571–586.

[163] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Oct. 1996.

[164] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed. Prentice Hall, Jun. 2004.

[165] S. Liu, C. Xing, and C. Yuan, "List decodability of random subcodes of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 63, no. 1, 2017, pp. 159–163.

[166] P. Loidreau, "Asymptotic behaviour of codes in rank metric over finite fields," *Designs, Codes and Cryptography*, Jul. 2012, pp. 1–14. DOI: 10.1007/s10623-012-9716-0.

[167] P. Loidreau, "An evolution of GPT cryptosystem," in *Int. Workshop Alg. Combin. Coding Theory (ACCT)*, 2016.

[168] P. Loidreau and R. Overbeck, "Decoding rank errors beyond the error correcting capability," in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pp. 186–190, Zvenigorod, Russia, Sep. 2006.

[169] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *Coding and cryptography*, ser. Lecture Notes in Computer Science, vol. 3969, Berlin: Springer, 2006, pp. 36–45.

[170] P. Loidreau, "Properties of codes in rank metric," in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pp. 192–198, Pamporovo, Bulgaria, Jun. 2008.
[171] P. Loidreau, "Designing a rank metric based McEliece cryptosystem," in *International Workshop on Post-Quantum Cryptography*, Springer, pp. 142–152, 2010.
[172] P. Loidreau, "A new rank metric codes based encryption scheme," in *8th Int. Conf. on Post-Quantum Cryptography (PQCrypto)*, 2017.
[173] H.-F. Lu and P. V. Kumar, "Generalized unified construction of space-time codes with optimal rate-diversity tradeoff," in *IEEE International Symposium on Information Theory (ISIT)*, p. 95, Chicago, IL, USA, Jun. 2004.
[174] G. Lunardon, R. Trombetti, and Y. Zhou, "Generalized twisted Gabidulin codes," *Journal of Combinatorial Theory, Series A*, vol. 159, 2018, pp. 79–106.
[175] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Transactions on Information Theory*, vol. 49, no. 10, Oct. 2003, pp. 2757–2760.
[176] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp. 738–755, 2012.
[177] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Co., 1988.
[178] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Transactions on Information Theory*, vol. 60, no. 5, May 2014, pp. 2856–2867. DOI: 10.1109/TIT.2014.2306938.
[179] H. Mahdavifar and A. Vardy, "Algebraic list-decoding on the operator channel," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 1193–1197, Austin, TX, USA, Jun. 2010. DOI: 10.1109/ISIT.2010.5513656.
[180] H. Mahdavifar and A. Vardy, "List-decoding of subspace codes and rank-metric codes up to Singleton bound," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 1488–1492, Cambridge, MA, USA, Jul. 2012. DOI: 10.1109/ISIT.2012.6283511.

[181] G. Marino, M. Montanucci, and F. Zullo, "MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$," *Linear Algebra and its Applications*, vol. 591, 2020, pp. 99–114.

[182] U. Martínez-Peñas and F. R. Kschischang, "Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes," *IEEE Transactions on Information Theory*, vol. 65, no. 12, 2019, pp. 7790–7805.

[183] U. Martínez-Peñas, M. Shehadeh, and F. Kschischang, "Codes in the sum-rank metric," *submitted to Fundamentals and Applications*, 2021.

[184] G. Matsaglia and G. Styan, "Equalities and inequalities for ranks of matrices," *Linear and Multilinear Algebra*, vol. 2, no. 3, Jan. 1974, pp. 269–292.

[185] R. J. McEliece, "On the average list size for the guruswami–sudan decoder," in *7th International Symposium on Communications Theory and Applications (ISCTA)*, Ambleside, UK, 2003.

[186] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *Deep Space Network Progress Report*, vol. 42, no. 44, 1978, pp. 114–116.

[187] M. Medard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," in *41st Allerton Conference on Communication, Control and Computing*, 2003.

[188] T. Migler, K. E. Morrison, and M. Ogle, *Weight and rank of matrices over finite fields*, Mar. 2004. arXiv: math/0403314, URL: http://arxiv.org/abs/math/0403314.

[189] E. H. Moore, "A two-fold generalization of Fermat's theorem," *Bull. Amer. Math. Soc.*, vol. 2, 1896, pp. 189–199. DOI: 10.1090/S0002-9904-1896-00337-2.

[190] K. Morrison, "Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 60, no. 11, 2014, pp. 7035–7046.

[191] S. Müelich, S. Puchinger, and M. Bossert, "Low-rank matrix recovery using Gabidulin codes in characteristic zero," *Electronic Notes in Discrete Mathematics*, vol. 57, 2017, pp. 161–166.

[192] S. Müelich, S. Puchinger, D. Mödinger, and M. Bossert, "An alternative decoding method for Gabidulin codes in characteristic zero," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2549–2553, 2016.

[193] S. Muralidhar, W. Lloyd, S. Roy, C. Hill, E. Lin, W. Liu, S. Pan, S. Shankar, V. Sivakumar, L. Tang, *et al.*, "f4: facebook's warm BLOB storage system," in *11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14)*, pp. 383–398, 2014.

[194] D. Napp, R. Pinto, J. Rosenthal, and F. Santana, "Column rank distances of rank metric convolutional codes," in *International Castle Meeting on Coding Theory and Applications*, Springer, pp. 248–256, 2017.

[195] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori, "MRD rank metric convolutional codes," in *2017 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2766–2770, 2017.

[196] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori, "Faster decoding of rank metric convolutional codes," in *23rd International Symposium on Mathematical Theory of Networks and Systems*, 2018.

[197] A. Neri, "Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices," *Linear Algebra and its Applications*, vol. 593, 2020, pp. 116–149. DOI: https://doi.org/10.1016/j.laa.2020.02.002.

[198] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal, "On the genericity of maximum rank distance and Gabidulin codes," *Designs, Codes and Cryptography*, vol. 86, no. 2, 2018, pp. 341–363.

[199] A. Neri, S. Puchinger, and A.-L. Horlemann-Trautmann, "Equivalence and characterizations of linear rank-metric codes based on invariants," *Linear Algebra and its Applications*, vol. 603, 2020, pp. 418–469.

[200] NIST, *Post–quantum cryptography standardization*, 2017, URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[201] Ø. Ore, "On a special class of polynomials," *Transactions of the American Mathematical Society*, vol. 35, 1933, pp. 559–584.

[202] Ø. Ore, "Theory of non-commutative polynomials," *Ann. Math.*, vol. 34, no. 3, 1933, pp. 480–508.

[203] K. Otal and F. Özbudak, "Explicit constructions of some non-Gabidulin linear maximum rank distance codes," *Advances in Mathematics of Communications*, vol. 10, no. 3, 2016, p. 589.

[204] K. Otal and F. Özbudak, "Additive rank metric codes," *IEEE Transactions on Information Theory*, vol. 63, no. 1, 2017, pp. 164–168.

[205] A. Otmani, H. T. Kalashi, and S. Ndjeya, "Improved cryptanalysis of rank metric schemes based on Gabidulin codes," *preprint*, Apr. 2017, URL: http://arxiv.org/abs/1602.08549v1.

[206] A. V. Ourivski and T. Johansson, "New technique for decoding codes in the rank metric and its cryptography applications," *Problems of Information Transmission*, vol. 38, no. 3, Jul. 2002, pp. 237–246. DOI: 10.1023/A:1020369320078.

[207] A. V. Ourivski and E. M. Gabidulin, "Column scrambler for the GPT cryptosystem," *Discrete Applied Mathematics*, vol. 128, no. 1, 2003, pp. 207–221.

[208] R. Overbeck, "A new structural attack for GPT and variants," *LNCS: MYCRYPT*, vol. 3715, 2005, pp. 50–63.

[209] R. Overbeck, "Extending Gibson's attacks on the GPT cryptosystem," *LNCS: Revised Selected Papers of WCC 2005*, vol. 3969, 2006, pp. 178–188.

[210] R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," *Journal of Cryptology*, vol. 21, no. 2, 2008, pp. 280–301.

[211] P. Delsarte, "An algebraic approach to association schemes of coding theory," *Philips research reports supplements*, vol. 10, May 1973, p. 103.

[212] P. Frankl and R. M. Wilson, "The Erdös-Ko-Rado theorem for vector spaces," *Journal of Combinatorial Theory*, vol. 43, May 1986, pp. 228–236.

[213] A. V. Paramonov and O. V. Tretjakov, "An analogue of Berlekamp-Massey algorithm for decoding codes in rank metric," in *Moscow Institute of Physics and Technology (MIPT)*, 1991.

[214] N. Pilipchuk and E. Gabidulin, "On Codes Correcting Symmetric Rank Errors," in *Coding and Cryptography*, vol. 3969, pp. 14–21, Jan. 2005. DOI: 10.1007/11779360_2.

[215] S. Puchinger, J. R. né Nielsen, W. Li, and V. Sidorenko, "Row reduction applied to decoding of rank-metric and subspace codes," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, 2017, pp. 389–409.

[216] S. Puchinger, J. Renner, and A. Wachter-Zeh, "Twisted Gabidulin codes in the GPT cryptosystem," *arXiv preprint arXiv:1806.10055*, 2018.

[217] S. Puchinger, J. Renner, A. Wachter-Zeh, and J. Zumbrägel, "Efficient decoding of Gabidulin codes over Galois rings," in *IEEE International Symposium on Information Theory (ISIT), arXiv preprint arXiv:2102.02157*, 2021.

[218] S. Puchinger, J. Rosenkilde né Nielsen, and J. Sheekey, "Further generalisations of twisted Gabidulin codes," in *International Workshop on Coding and Cryptography (WCC)*, 2017.

[219] S. Puchinger, S. Stern, M. Bossert, and R. F. Fischer, "Space-time codes based on rank-metric codes and their decoding," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, IEEE, pp. 125–130, 2016.

[220] S. Puchinger and A. Wachter-Zeh, "Sub-quadratic decoding of Gabidulin codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016.

[221] S. Puchinger and A. Wachter-Zeh, "Fast operations on linearized polynomials and their applications in coding theory," *Journal of Symbolic Computation*, vol. 89, 2018, pp. 194–215.

[222] T. Randrianarisoa, "A decoding algorithm for rank metric codes," *arXiv preprint arXiv:1712.07060*, 2017.

[223] T. Randrianarisoa and J. Rosenthal, "A decoding algorithm for twisted Gabidulin codes," in *2017 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2771–2774, 2017.

[224] T. H. Randrianarisoa, "A geometric approach to rank metric codes and a classification of constant weight codes," *CoRR*, vol. abs/1907.04372, 2019. arXiv: 1907.04372, URL: http://arxiv.org/abs/1907.04372.

[225] H. Rashwan, E. M. Gabidulin, and B. Honary, "A smart approach for GPT cryptosystem based on rank codes," in *2010 IEEE International Symposium on Information Theory*, IEEE, pp. 2463–2467, 2010.

[226] H. Rashwan, E. M. Gabidulin, and B. Honary, "Security of the GPT cryptosystem and its applications to cryptography," *Security and Communication Networks*, vol. 4, no. 8, 2011, pp. 937–946.

[227] A. Ravagnani, "Rank-metric codes and their duality theory," *Designs, Codes and Cryptography*, vol. 80, no. 1, 2016, pp. 197–216.

[228] N. Raviv and A. Wachter-Zeh, "Some Gabidulin codes cannot be list decoded efficiently at any radius," *IEEE Transactions on Information Theory*, vol. 62, no. 4, 2016, pp. 1605–1615. DOI: 10.1109/TIT.2016.2532343.

[229] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 60, no. 1, 2014, pp. 212–236. DOI: 10.1109/TIT.2013.2288784.

[230] J. Renner, S. Puchinger, and A. Wachter-Zeh, "Interleaving Loidreau's rank-metric cryptosystem," in *XVI International Symposium "Problems of Redundancy in Information and Control Systems"*, 2019.

[231] J. Renner, T. Jerkovits, and H. Bartz, "Efficient decoding of interleaved low-rank parity-check codes," in *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, pp. 121–126, 2019. DOI: 10.1109/REDUNDANCY48165.2019.9003356.

[232] J. Renner, T. Jerkovits, H. Bartz, S. Puchinger, P. Loidreau, and A. Wachter-Zeh, "Randomized decoding of Gabidulin codes beyond the unique decoding radius," in *International Conference on Post-Quantum Cryptography (PQCrypto)*, Paris, France, Apr. 2020.

[233] J. Renner, A. Neri, and S. Puchinger, "Low-rank parity-check codes over Galois rings," *Designs, Codes and Cryptography*, vol. 89, no. 2, 2021, pp. 351–386.

[234] J. Renner, S. Puchinger, and A. Wachter-Zeh, "Decoding high-order interleaved rank-metric codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Melbourne, Australia, Jul. 2021.

[235] J. Renner, S. Puchinger, and A. Wachter-Zeh, "LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding," *Designs, Codes and Cryptography*, vol. 89, no. 6, 2021, pp. 1279–1319.

[236] J. Renner, S. Puchinger, A. Wachter-Zeh, C. Hollanti, and R. Freij-Hollanti, "Low-rank parity-check codes over the ring of integers modulo a prime power," *IEEE International Symposium on Information Theory (ISIT)*, 2020.

[237] G. Richter and S. Plass, "Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm," in *International ITG Conference on Systems, Communications and Coding 2004 (SCC)*, Erlangen, Germany, 2004.

[238] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *IEEE International Symposium on Information Theory (ISIT)*, p. 398, Chicago, IL, USA, 2004. DOI: 10.1109/ISIT.2004.1365435.

[239] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, 1978, pp. 120–126.

[240] G. Robert, "A quadratic Welch-Berlekamp algorithm to decode generalized Gabidulin codes, and some variants," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 2559–2563, 2016.

[241] R. M. Roth, “Maximum-rank array codes and their application to crisscross error correction,” *IEEE Transactions on Information Theory*, vol. 37, no. 2, 1991, pp. 328–336.

[242] R. M. Roth, “Tensor codes for the rank metric,” *IEEE Transactions on Information Theory*, vol. 42, no. 6, 1996, pp. 2146–2157.

[243] R. M. Roth, “On decoding rank-metric codes over large fields,” *IEEE Transactions on Information Theory*, vol. 64, no. 2, 2017, pp. 944–951.

[244] R. M. Roth and G. Seroussi, “On generator matrices of MDS codes (corresp.),” *IEEE transactions on information theory*, vol. 31, no. 6, 1985, pp. 826–830.

[245] N. Sendrier, “Decoding one out of many,” in *Post-Quantum Cryptography*, B.-Y. Yang, Ed., pp. 51–67, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[246] J. Sheekey, “A new family of linear maximum rank distance codes,” *Advances in Mathematics of Communications*, vol. 10, no. 3, 2016, pp. 475–488.

[247] J. Sheekey, “13. MRD codes: constructions and connections,” in *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*, K. Schmidt and A. Winterhof, Eds., vol. 23, de Gruyter, 2019, pp. 255–286.

[248] J. Sheekey, “New semifields and new MRD codes from skew polynomial rings,” *Journal of the London Mathematical Society*, 2019. DOI: 10.1112/jlms.12281.

[249] H. A. Shehhi, E. Bellini, F. Borba, F. Caullery, M. Manzano, and V. Mateu, “An IND-CCA-secure code-based encryption scheme using rank metric,” in *Progress in Cryptology – AFRICACRYPT 2019*, J. Buchmann, A. Nitaj, and T. Rachidi, Eds., pp. 79–96, Cham: Springer International Publishing, 2019.

[250] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, 1999, pp. 303–332.

[251] V. R. Sidorenko and M. Bossert, "Decoding interleaved Gabidulin codes and multisequence linearized shift-register synthesis," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 1148–1152, Austin, TX, USA, Jun. 2010.

[252] V. R. Sidorenko, L. Jiang, and M. Bossert, "Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, Feb. 2011, pp. 621–632.

[253] V. R. Sidorenko, G. Richter, and M. Bossert, "Linearized shift-register synthesis," *IEEE Transactions on Information Theory*, vol. 57, no. 9, 2011, pp. 6025–6032. DOI: 10.1109/TIT.2011.2162173.

[254] V. Sidorenko and M. Bossert, "Fast skew-feedback shift-register synthesis," *Designs, Codes and Cryptography*, vol. 70, no. 1-2, 2014, pp. 55–67.

[255] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2858–2862, Seoul, Korea, Jun. 2009. DOI: 10.1109/ISIT.2009.5205272.

[256] D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," *IEEE Transactions on Information Theory*, vol. 55, no. 12, Dec. 2009, pp. 5479–5490. DOI: 10.1109/tit.2009.2032817.

[257] D. Silva, "Error Control for Network Coding," Ph.D. dissertation, University of Toronto, Toronto, Canada, Toronto, Canada, 2009.

[258] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, 2008, pp. 3951–3967.

[259] C. Sippel, C. Ott, S. Puchinger, and M. Bossert, "Reed–Solomon codes over fields of characteristic zero," in *2019 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1537–1541, 2019.

[260] R. Tajeddine, A. Wachter-Zeh, and C. Hollanti, "Private information retrieval over random linear networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, Jul. 2019, pp. 790–799.

[261] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," *IEEE Transactions on Information Theory*, vol. 60, no. 8, 2014, pp. 4661–4676.

[262] C. Tian and J. Chen, "Caching and delivery via interference elimination," *IEEE Transactions on Information Theory*, vol. 6, no. 3, Mar. 2018, pp. 1548–1560. DOI: 10.1109/TIT.2018.2794543.

[263] A.-L. Trautmann, N. Silberstein, and J. Rosenthal, "List decoding of lifted Gabidulin codes via the plücker embedding," in *International Workshop on Coding and Cryptography (WCC)*, Bergen, Norway, Apr. 2013.

[264] R. Trombetti and F. Zullo, "On the list decodability of rank metric codes," *IEEE Transactions on Information Theory*, vol. 66, no. 9, 2020, pp. 5379–5386.

[265] S. P. Vadhan, "Pseudorandomness," in *Foundation and Trends in Theoretical Computer Science*, 2011.

[266] A. Wachter, V. R. Sidorenko, M. Bossert, and V. V. Zyablov, "On (partial) unit memory codes based on Gabidulin codes," *Problems of Information Transmission*, vol. 47, no. 2, 2011, pp. 117–129.

[267] A. Wachter-Zeh, S. Puchinger, and J. Renner, "Repairing the Faure-Loidreau public-key cryptosystem," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2426–2430, 2018. DOI: 10.1109/ISIT.2018.8437561.

[268] A. Wachter-Zeh, "Bounds on list decoding of rank-metric codes," *IEEE Transactions on Information Theory*, vol. 59, no. 11, 2013, pp. 7268–7277. DOI: 10.1109/TIT.2013.2274653.

[269] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko, "Fast decoding of Gabidulin codes," *Des. Codes Cryptogr.*, vol. 66, no. 1, Jan. 2013, pp. 57–73.

[270] A. Wachter-Zeh and V. Sidorenko, "Rank metric convolutional codes for random linear network coding," in *2012 International Symposium on Network Coding (NetCod)*, IEEE, pp. 1–6, 2012.

[271] A. Wachter-Zeh, M. Stinner, and V. Sidorenko, "Convolutional codes in rank metric with application to random network coding," *IEEE Transactions on Information Theory*, vol. 61, no. 6, 2015, pp. 3199–3213.

[272] A. Wachter-Zeh and A. Zeh, "List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques," *Designs, Codes and Cryptography*, vol. 73, no. 2, 2014, pp. 547–570. DOI: 10.1007/s10623-014-9953-5.

[273] Z.-X. Wan, *Geometry of matrices: in memory of professor LK Hua (1910–1985)*. World Scientific, 1996.

[274] H. Wang, C. Xing, and R. Safavi-Naini, "Linear authentication codes: bounds and constructions," *IEEE Transactions on Information Theory*, vol. 49, no. 4, 2003, pp. 866–872.

[275] C. Xing and C. Yuan, "A new class of rank-metric codes and their list decoding beyond the unique decoding radius," *IEEE Transactions on Information Theory*, vol. 64, no. 5, 2018, pp. 3394–3402.

[276] R. W. Yeung and N. Cai, "Network error correction, I: basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, 2006, pp. 19–35.

[277] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr, "The exact rate-memory tradeoff for caching with uncoded prefetching," *IEEE Transactions on Information Theory*, vol. 64, no. 2, Feb. 2018, pp. 1281–1296. DOI: 10.1109/TIT.2017.2785237.

[278] P. C. Yunnan, P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," *41st Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2003.

[279] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: a geometric approach to the noncoherent multiple-antenna channel," *IEEE Transactions on Information Theory*, vol. 48, no. 2, Feb. 2002, pp. 359–383. DOI: 10.1109/18.978730.