ALGEBRAIC METHODS IN CODING THEORY AND COMMUNICATION

Elisa Gorla (University of Neuchatel),
Marcus Greferath (University College Dublin),
Hiram H. López Valdez (Cleveland State University),
Felice Manganiello (Clemson University).

April 25–April 29, 2022

Starting with the seminal work of Claude Shannon in the 1940's, coding theory has been a flourishing subject for research collaborations between mathematicians, computer scientists and electrical engineers. Research problems in coding theory have evolved in the years to answer important practical questions from real world applications. This workshop brought together researchers from different backgrounds in order to foster interdisciplinary collaborations that push forward the research in coding theory and communication.

The workshop focused on five prominent directions in contemporary coding theory and its applications. *Locally recoverable codes* (LRCs) allow the recovery of a codeword symbol's erasure when one only has access to a small set of codeword symbols. These codes are of great current interest, in part due to their applicability to problems arising from distributed storage. *Rank-metric codes* are codes from a metric space defined by the rank function. The seminal papers on these codes are from the 1980s but it is in the last few decades that they received major interest by the international research community because of their applications to network coding and code-based cryptography. *Code-based Cryptography* put problems from coding theory at the core of advanced cryptosystems capable of withstanding attacks from quantum computers. The public-key cryptosystems used nowadays have been proven weak against quantum attacks, making this area one of the most important application in coding theory of the last few years. *Network Coding* seeks answers to problems of maximization of information flow over networks. These answers often require the establishment of new communication schemes, relying on mathematical structures that have not been used in this context before. In recent years, a new set of problems with local features arises from practical communication problems. For example, with the need of storing more and more data on different servers, the challenge of recovering information by contacting as few servers as possible arises. *Algebraic coding theory* tackles classical communication problems, such as error-free communication between a source and a receiver over noisy channels, using a wide range of tools from algebra, algebraic geometry, and probability theory. More recently, coding theory has found applications to emerging challenges in communication. Data communication changed as our digital lives which became more and more interconnected.

One of the first meetings with a focus on coding theory that brought together multidisciplinary researchers from many countries took place in Oberwolfach, Germany, in 2007. This workshop was followed by Dagstuhl meetings, which took place in Germany in 2011, 2013, 2016, 2018. A BIRS meeting took place in Canada in 2015. Another multidisciplinary meeting on coding theory was held in 2019 in Oberwolfach. Most of these workshops focused on the present-day challenges in coding theory arising from Big Data, Multimedia Streaming, Networks, Distributed Storage, and Security. One important consequence of having such a series of meetings is that they contributed to increasing the scientific interaction between mathematicians and researchers in more applied areas of coding theory. The workshop on "Algebraic Methods in Coding Theory

and Communication" is the first one hosted at the CMO.

1 Overview of the Field

The workshop focused on five central and timely themes in mathematical coding theory: locally recoverable codes, rank-metric codes, code-based cryptography, network coding, and algebraic coding theory. While remarkable connections have emerged among these five apriori unrelated research directions, they have not been yet explored to the full extent of their depth.

In the sequel, $\mathcal{C}$ denotes a linear $(n,k)_q$-code, i.e. a linear k-dimensional subspace of $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field with q elements.

Locally recoverable codes

Distributed storage systems have been widely used in recent times for many different purposes. In this context, one of the most common scenarios that needs to be addressed is related to the failure of one of the servers to return to the user the requested data. Whether this is because of the need for many parties to access the same files, or simply because the server's hardware needs to be replaced, the question of how to recover lost information in an "optimal" way is one that will only continue to increase in importance in our data-driven world.

How to recover lost data?

One solution to this problem is k-fold replication, also known as a repetition code. For example, suppose that we have a piece of data that contains four bits, such as 0100. We could repeat this data twice more and obtain the encoded word 010001000100. Then, if one symbol is lost, we could look at the other two copies to see what the original entry was.

But this encoding, in general, requires way too much overhead; the relatively small threefold replication described above requires an overhead of 200%. Threefold replication is also only able to recover two erasures, i.e., there are some patterns of three erasures for which some of the data can no longer be recovered. For example, if an erasure occurs at the same place in all of the three copies, then recovery of the erased symbol will be impossible. The natural question to ask is then, how could one decrease the storage space needed for the encoded information, while retaining (or improving) the erasure recovery capability. This is the main focus of the field of coding theory and the goal of coding theory for distributed storage.

In computer science applications, the main goal is to construct systems that deal with the most common scenario in an optimal way, but can still deal with the worst case scenario. It turns out that the most common scenario is actually the failure of a node, as in the one-node erasure example here:

$$(1,0,1,1,0,0,0,1) \longrightarrow (1,*,1,1,0,0,0,1)$$

If one wants to repair just a single erasure, in general they have to look at many other components of a codeword where the erasures occurred. For example, for the $(14,10)_q$ Reed Solomon code, to repair a single node failure we need to look at 10 other components of the vector we are repairing because we need to reconstruct entirely the evaluation polynomial. This means that we need to access data 10 times the size of the data we wish to repair. The aim of locally recoverable codes is to correct small volumes of erasures in an optimal way, with respect to the number of nodes that have to be accessed to recover the lost information.

This leads to the following definition. A locally recoverable code $\mathcal{C}$ with locality r is a linear code $\mathcal{C}$ such that, if one erases one component of any $v \in \mathcal{C}$, this component can be recovered by accessing at most r other components of v. The number r of nodes we must call on to recover a single erasure is referred to as the locality of the code.

The concept of locality in error-correcting codes was introduced in the early 2010s [7, 8, 14] due to its applications to cloud storage and distributed storage systems. In the introductory talk on locally recovered codes, the speaker covered material from [1, 2, 3, 9, 10, 11, 12, 13, 15]. In particular, the Cadambe-Mazumdar bound, classical locally recoverable codes and hierarchical locally recoverable codes were discussed. The speaker then focussed on the construction of Tamo-Barg of LRCs as subcodes of Reed-Solomon codes and extended on the Tamo-Barg work using Galois theory to construct optimal codes with large parameters. Part of the research on Tamo-Barg LRCs is currently focused on expanding the Galois Theoretical connection in [9], as for example in [4, 5, 6] and extending the connection to larger classes of LRCs.

Rank-Metric Codes

Rank-metric codes are linear spaces of matrices over a finite field, in which every non-zero matrix has rank bounded from below by a given integer d. They were introduced by Delsarte in 1978 and more recently rediscovered in various contexts within pure and applied mathematics. In 2008, rank-metric codes were proposed as a solution to the problem of error amplification in coded communication networks. This novel application renewed the interest in the general theory of rank-metric codes, which are to date a central them in coding theory.

A current open problem in the theory of rank-metric codes asks to compute the asymptotic density of Maximum-Rank-Distance (MRD) codes, i.e., of those rank-metric codes that meet the Singleton bound with equality. Unlike MDS codes (which can be seen as the analogues of MRD codes for the Hamming metric), MRD codes were shown to be sparse over large fields. In other words, a uniformly random rank-metric code is MRD with probability that goes to zero as the size q of the underlying field grows.

Computing the "exact" asymptotic behaviour of the density function of MRD codes is currently a wide open problem in coding theory, closely linked to the theory of geometric lattices, to graph theory, and to the theory of finite semifields. The talk on rank-metric codes at the Algebraic Methods in Coding Theory and Communication workshop offered an overview of the mathematical theory of rank-metric codes, with a focus on the density questions just described.

Code-Based Cryptograhy

We consider public-key cryptosystems, where some sender, say Alice, wants to send an encrypted message to a receiver, say Bob. The cryptosystem is asymmetric, in the sense that Bob publishes a *public key* and secretly stores a *private key*, such that Alice (and everyone else) can use the public key to encrypt her message, and only Bob can decrypt the message by using his private key. For the system to be secure, an attacker should not be able to decrypt the encrypted message without the knowledge of the private key. This is done by using some "hard" mathematical problem. Currently used cryptosystems rely on one of the following three hard problems for the encryption: integer factorization, discrete logarithm problem, and elliptic curve discrete logarithm problem.

We say that a problem is "hard" for cryptographic purposes if no polynomial-time algorithm to solve it is known. For the three above problems, this is true for conventional computers. However, on quantum computers, there is a known algorithm that solves these problems in polynomial time. This algorithm is known as *Shor's algorithm*; it was originally formulated for integer factorization, but can be adapted to solve discrete logarithm problems, as well. This means that new algorithms are necessary for the future, to ensure secure secret communication in the time of quantum computers. The science of algorithms withstanding Shor's algorithm is called *post-quantum cryptography*.

At the time of writing, there are five main streams of post-quantum cryptography: code-based cryptography, lattice-based cryptography, hash-based cryptography, multivariate cryptography, and supersingular elliptic curve isogeny cryptography. Within *code based cryptography*, there are two main general cryptosystems which are based on error-correcting codes – the McEliece [16] and the Niederreiter system [17]. Both of these have variants, depending on which type of code one wants to use. Since both are equivalent from a security point of view we focus on the McEliece system. For implementation purposes however, and for the construction of digital signatures, the Niederreiter system is of great interest, as well.

Originally, the McEliece cryptosystem was introduced using binary Goppa codes. We will now describe the underlying ideas in its general form, using an arbitrary linear block code. Bob chooses a code $\mathcal{C}$ with generator matrix G and an efficient decoding algorithm. Moreover, he needs a disguising function ϕ that is a near-isometry, i.e., a function on the vectors that changes the weight by at most a given value. Then the private key is G and the public key is $\phi(G)$ together with the error correction capability of the code generated by $\phi(G)$, say $\hat{t}$. Alice chooses a random error vector e of weight at most $\hat{t}$ and encrypts her message m as

$$c = m\ \phi(G) + e.$$

Bob computes $\phi^{-1}(c)$ and then decodes in the secret code $\mathcal{C}$ to recover m. An attacker is unable to recover m without knowing ϕ, respectively the secret code $\mathcal{C}$. As a brute-force attack, he can try to decode in the

public code $\phi(\mathcal{C})$, but this code has no discernible structure, hence no efficient decoding algorithm: Decoding in such a "random" code is known to be a difficult problem.

By increasing the length n of the code, one may make the decoding problem arbitrarily hard. However, this affects the efficiency and the key size of the cryptosystem. Generally, code based cryptography suffers from large key sizes; on the other hand, the encryption and decryption times are very fast compared to other cryptosystems. One of the main research goals in this area is hence to find codes and disguising functions that allow smaller key sizes than currently known variants.

One promising idea is to use rank-metric codes instead of traditional Hamming metric codes, since generic decoding algorithms in the rank metric are less efficient than in the Hamming metric [18]. Until recently, all proposed variants in the rank metric use the same family of rank-metric codes codes; their main difference is the respective disguising function. Many of these variants have however been broken, mostly due to structural attacks, which reconstruct the private key from the public key. Nevertheless, this remains an active and promising area of investigation and NIST - the US National Institute of Standard and Technology - has encouraged researchers to further explore the use of rank-metric codes in code-based cryptography.

Network coding

Traditional approaches to the design of communication networks treat information flow much like commodity flow [21, 22]: packets are *routed* along links in the network, much like cars on a highway. In case of contention (when two packets wish to occupy the same link at the same time), one of the packets must wait or be dropped. Network coding [23] arose out of the realization that information flow is not commodity flow and that packets transmitted in a communication network should *not* be treated like cars on the highway. Intermediate nodes in a network can, in principle, do more than just routing: they can, via some appropriate mapping, *combine* packets contending for the same link. Provided that the intended receivers obtain enough information to invert such combinations, greater throughput can sometimes be achieved than in networks that perform routing alone.

In *linearly* coded networks [24, 25], the packets are assumed to be vectors over a finite field $\mathbb{F}_q$, and intermediate nodes in the network may transmit (on their outgoing links) $\mathbb{F}_q$-linear combinations of packets that they receive (on their incoming links). In the case of *multicasting*, where a source wishes to communicate the same message to several sinks simultaneously, such linear network coding can achieve the multicast capacity of the network, provided that the field size q is sufficiently large [24, 25]. Moreover, for sufficiently large q, the multicast capacity can be achieved, with high probability, by a random choice of coding coefficients at each node, without knowledge of the network topology [26].

Lower bounds on q to guarantee that a linear network coding solution exists were explored in [25, 27]. An algorithm to find a linear solution for any network was given in [28]. Linear solvability of a network was connected to the representability of a matroid in [29, 30]. It was proven in [31] that the existence of a linear network coding solution over $\mathbb{F}_{q_0}$ does not imply such an existence for all $q > q_0$. They conjectured that if there a solution over $\mathbb{F}_{q_0}$ and $q_0 - 1$ is prime, then there is a solution for all $q > q_0$. In the non-multicast scenario, it was shown in [32] that non-linear solutions may exist while no linear solution exists. Solutions over smaller finite fields may also be obtained with vector Network Coding, explored in [33, 34]. Physical-Layer Network Coding was studied in [35, 36] and wireless Network Coding was studied in [37].

Because of the necessity to invert a system of equations at the receiver, network coding is sensitive to errors introduced in the received packets, either by noise or by an adversary. An error-correction model that depends on the graph and network code was developed in [38, 39]. Probabilistic error-correcting codes were given in [40]. A deterministic error-correcting code, but which depends on the network, was given in [41]. Error-correcting codes under an adversarial model without such requirements (thus compatible with random linear network coding) were first given in [42, 43] for *non-coherent communication* (in which the sink has no knowledge of the coding coefficients of the incoming links), and in [44] for *coherent communication*.

Due to the linear combinations performed at different nodes of the network, an adversary wiretapping some links of the network obtains the sent message (a vector) multiplied by some transfer matrix. Information-theoretical security in Network Coding was first studied in [45, 46]. A similar code construction but with smaller field sizes was later given in [47]. An algorithmic code construction for security was given in [48]. Coding schemes that provide perfect secrecy and zero-error communication, without knowledge or modification of the underlying linear network code, were first given in [49].

The works noted above make use of only *one shot* of the linearly-coded network. Correction of link errors in *multishot network coding* was first investigated in [50, 51]. However, using Maximum Rank Distance (MRD) code solutions require large field sizes (exponential in the code length and number of shots). Solutions based on Maximum Sum-Rank Distance codes [52, 53] require only polynomial field sizes in the code length and number of shots and were proposed in [54]. Later, several works studied the mathematical properties of codes in the sum-rank metric [55, 56, 57, 58, 59]. See [60] for a survey. Other approaches to error correction in multishot Network Coding include rank-metric convolutional codes [61, 62, 63, 64].

Algebraic coding theory

Algebraic coding theory applies algebraic structures and techniques to problems arising in the point-to-point communication scenario. Evaluation codes, codes from algebraic geometry, and codes over rings are examples of algebraic codes.

Among the most exciting advances in this field is the invention of list-decoding algorithms for various classes of algebraic codes. Research in this area began with a landmark paper by Sudan, who proposed an algebraic list-decoding scheme for Reed-Solomon codes. List decoding algorithms yield, for a given received word, a list of codewords that have at most a given distance δ from the received word. The size of the list depends on the chosen distance δ and is usually short, if δ is close to the error correction capability of the code.

The methods within algebraic coding theory are mostly algebraic and make use of various properties of multivariate polynomials, or more generally, the properties of "well-behaved" functions in the function field of an irreducible variety. On the computational side, the field profit of the recent advances in the theory of Gröbner bases, which provide us with important tools for computing with polynomial equations.

In addition, relevant relationships are emerging between this topic and codes on graphs. One of the central questions is whether it is possible to match the superior performance of graph-based codes with list-decoding algorithms or, at least, with algorithms derived from list-decoding algorithms. Investigating such questions requires a good command of the computational side of algebra, as well as being well-versed in the more engineering-related aspects of the theory of codes on graph.

It is also relevant that the main works in coding theory from Mexico are in algebraic coding theory. In addition, in recent years Mexico has seen a surge of interest in coding theory and cryptography, partly due to the interest in these fields from the Mexican Space Agency.

2 Presentation Highlights

The following is the list of talks which were delivered at the workshop.

	Monday	Tuesday	Wednesday	Thursday	Friday
9:30-10:30	Micheli	Ravagnani	Horlemann	Martinez Peñas	Neri
11:00-12:00	Matthews	Guruswami	Gaborit	Soljanin	Carvalho
13:00-14:00	Sprintson	Barg	Lange	Byrne	Wood

Introduction to the theory of Locally Recoverable Codes
Giacomo Micheli, University of South Florida

Abstract: This talk provides an introduction to the theory of locally recoverable codes (LRCs). In particular, we cover the basics on LRCs (motivation, definition, and singleton bound) and survey recent advances, with particular emphasis on Tamo-Barg codes and their connection to Galois theory over global function fields.

Fractional decoding of codes from curves
Gretchen Matthews, Virginia Tech

Abstract: There has been much recent work on erasure recovery using either fewer symbols or less information from a received word. In particular, locally recoverable codes and linear exact repair schemes address these scenarios. In this talk, we consider a similar challenge for error correction. Decoding algorithms

for error-correcting codes typically take as input all symbols of a received word and attempt to determine the original codeword. Fractional decoding attempts to do so using only a portion of the information normally used in recovery. In this talk, we consider how this framework developed in earlier works by Tamo, Ye, and Barg and Santos may be applied to codes defined using curves. This is joint work with Aidan Murphy and Welington Santos.

Codes with Locality in the Rank and Subspace Metrics
Alex Sprintson, Texas A&M University

Abstract: We extend the notion of locality from the Hamming metric to the rank and subspace metrics. Our main contribution is to construct a class of array codes with locality constraints in the rank metric. Our motivation for constructing such codes stems from designing codes for efficient data recovery from correlated and/or mixed (i.e., complete and partial) failures in distributed storage systems. Specifically, the proposed local rank-metric codes can recover locally from 'crisscross errors and erasures', which affect a limited number of rows and/or columns of the storage system. We also derive a Singleton-like upper bound on the minimum rank distance of (linear) codes with 'rank-locality' constraints. Our proposed construction achieves this bound for a broad range of parameters. The construction builds upon Tamo and Barg's method for constructing locally repairable codes with optimal minimum Hamming distance. Finally, we construct a class of constant-dimension subspace codes (also known as Grassmannian codes) with locality constraints in the subspace metric. The key idea is to show that a Grassmannian code with locality can be easily constructed from a rank-metric code with locality by using the lifting method proposed by Silva et al. We present an application of such codes for distributed storage systems, wherein nodes are connected over a network that can introduce errors and erasures.

Rank-Metric Codes
Alberto Ravagnani, Eindhoven University of Technology

Abstract: A (linear) rank-metric codes is a vector space of matrices of given size over a finite field, in which the rank of any nonzero matrix is bounded from below by a given integer. Rank-metric codes were first studied for combinatorial interest by Delsarte in the seventies, and then by Cooperstein, Gabidulin, and Roth in various contexts. In 2008, Silva, Koetter and Kschischang discovered that rank-metric codes combined with linear network coding offer a solution to the problem of error amplification in communication networks. Since then, rank-metric codes have been a thriving research area within coding theory, electrical engineering, and discrete mathematics.

This talk offers an overview on the mathematical theory of rank-metric codes, from the problem of correcting errors in networks, to that of investigating the properties of certain combinatorial structures and their q-analogues.

Recent Progress on Binary Deletion-Correcting Codes
Venkatesan Guruswami, UC Berkeley

Abstract: In the worst-case (bit) deletion noise model, a subset of up to t arbitrarily chosen bits are deleted from a sequence of n codeword bits. Crucially, the locations of the deleted bits are not known to the receiver who receives a subsequence of the transmitted bit-string. The goal is to design codes of low redundancy that allow recovery of the deleted bits and the original codeword. The study of deletion-correcting codes itself is quite old, dating back to optimal single-deletion codes in the 1960s, and positive rate codes to correct $t = \Omega(n)$ deletions in the 1990s. However, many basic questions remained open and our understanding of deletion-correcting codes significantly lagged the vast literature concerning error-correcting codes to correct bit flips.

After a long hiatus, there has been notable progress on deletion-correcting codes in the last 6-7 years, covering regimes when the number of deletions t is a small constant, a small constant fraction of n, and a large proportion of n, as well as the list-decoding model. The talk will survey some of this progress.

High-rate storage codes on triangle-free graphs.
Alexander Barg, University of Maryland

Abstract: Consider an assignment of bits to the vertices of a connected graph $G(V, E)$ with the property that the value of each vertex is a function of the values of its neighbors. A collection of such assignments is called a storage code of length $|V|$ on G. If G contains many cliques, it is easy to construct storage codes of rate close to 1, so a natural problem is to construct high-rate codes on triangle-free graphs, where finding codes of rate $>$1/2 is a nontrivial task. Previously only isolated examples of storage codes of rate $\geq$ 1/2 on triangle-free graphs were given in the literature. The class of graphs that we consider is coset graphs of linear binary codes (Cayley graphs of the group $\mathbb{F}_2^r$). One of the main results of this work is an infinite family of linear storage codes with rate approaching 3/4. We also give a group of necessary conditions for such codes to have rate potentially close to 1 and state a number of open problems. Joint work with Gilles Zémor.

Code-Based Cryptography - An Overview
Anna-Lena Horlemann, University of St. Gallen

Abstract: We will introduce the basics of code-based crypto systems and give an overview of past and current developments. We will start with the original public key cryptosystems by McEliece and Niederreiter, discuss several variants in the Hamming and rank metric of these systems and talk about various tools for cryptanalyzing them. In the end we will mention results on using other metrics for these systems and some techniques for creating digital signatures from the syndrome decoding problem.

Recent advances on rank based cryptography
Philippe Gaborit, University of Limoges

Abstract: In this talk we survey recent results for rank-based cryptography: cryptosystems which are based on error-correcting codes embedded with the rank metric. These new results concern the LRPC cryptosystem and the RQC cryptosystems for which we propose a new approach which permits to decrease public key by roughly 30% and permits to obtain very efficient systems even in the case of proven 2^{-128} Decryption Failure Rate. We will also survey different type of signatures based on rank metric including the Durandal signature scheme. Overall these new results show the validity of rank metric based cryptography as a real alternative in post-quantum crypto.

Code-based cryptography for secure communication
Tanja Lange, Eindhoven University of Technology

Abstract: Code-based cryptography, in particular the McEliece cryptosystem with binary Goppa codes, is known as one of the most conservative choices in post-quantum cryptography. It is also known as a system that is impractical or cumbersome to use for Internet applications due to the large size of the public key. Among the candidates in the 3rd round of the NIST competition on post-quantum cryptography is also the system with the smallest ciphertext size, making it attractive in situations where keys are changed infrequently and ciphertext size matters.

This talk will present several recent applications of code-based cryptography in Internet applications.

Network Coding, Error Correction and Security
Umberto Martinez-Penas, University of Valladolid

Abstract: Maximum information flow over a communication network with one source and one sink can be characterized by the classical max-flow min-cut theorem. However, in the multicast scenario (one source and multiple sinks), maximum flow cannot always be achieved by routing only. In 2000, Ahlswede, Cai, Li and Yeung developed a technique, called Network Coding, that allows the source to send the maximum possible amount of information to all sinks simultaneously. In this talk, we provide an introduction to Network Coding, and then provide a survey on techniques for deterministic worst-case error correction and information-theoretical security under the model considered by Koetter, Kschischang and Silva. This model considers the underlying network topology and network code as a blackbox (i.e., no knowledge or modification of the network is needed) and is thus compatible with random linear Network Coding. We will go through the different coding results obtained in the past decade, including subspace coding, list-decoding and multishot network coding, among others. We will conclude with directions for future research.

Multiple Concurrent (Local) Data Access with Codes
Emina Soljanin, Rutgers University

Abstract: Distributed storage systems strive to maximize the number of concurrent data access requests they can support with fixed resources. Replicating data objects according to their relative popularity and access volume helps achieve this goal. However, these quantities are often unpredictable. In emerging applications such as edge computing, even the expected numbers of users and their data interests extensively fluctuate, and data storage schemes should support such dynamics. Erasure-coding has emerged as an efficient and robust form of redundant storage. In erasure-coded models, data objects are elements of a finite field. Each node in the system stores one or more linear combinations of data objects. This talk asks 1) which data access rates an erasure-coded system can support and 2) which codes can support a specified region of access rates. We will address these questions by formulating them as some known and some new combinatorial optimization problems on graphs. We will explain connections with LRC and batch codes. This talk will also describe how, instead of a combinatorial, one can adopt a geometric approach to the problem.

q-Matroids, q-Polymatroids and Rank-Metric Codes
Eimear Byrne, University College Dublin

Abstract: There are many connections between linear codes and matroids and several coding theoretic invariants turn out to be matroid invariants. Following the development of the theory of rank-metric codes, q-matroids and q-polymatroids have become a topic of interest among an increasing number of researchers, especially in the last few years. This topic involves submodular functions defined on the lattice of subspaces of a vector space. In this talk, we'll look at some recent results of q-matroids and q-polymatroids and show the connections to rank metric codes. We will use the characteristic polynomial of a q-polymatroid as a basic tool for some of these results.

Geometric approaches to linear codes
Alessandro Neri, Max Planck Institute for Mathematics in the Sciences

Abstract: This talk will focus on the interactions between algebraic coding theory and finite geometry. We will explain in detail how these two mathematical areas are connected and in which way one can transform metric problems in coding theory to intersection problems in finite geometry, and vice versa. In particular, we will give an overview of such problems, from well-known results to more recent research directions.

Following footprints in coding theory: a collection of results.
Cicero Carvalho, Universidade Federal de Uberlândia

Abstract: In this talk, we intend to present the concept of footprint of an ideal, and a (certainly non-exhaustive) collection of recent results in coding theory obtained with the help of footprints and other tools from Gröbner basis theory.

Failures of the MacWilliams Identities
Jay A. Wood, Western Michigan University

Abstract: The Hamming weight enumerator can be viewed in two ways: (1) as counting the number of entries in a codeword that belong to particular subsets of a partition of the alphabet, or (2) using the value of the weight as the exponent in the enumerator. In generalizing beyond the Hamming weight enumerator, the counting interpretation has enjoyed great success. In contrast, the w-weight enumerator determined by a weight w often fails to satisfy the MacWilliams identities. We will describe some of these failures for well-known weights.

3 Broader Impacts, Structure and Challenges of the Hybrid Workshop

The hybrid format of the workshop allowed the organizers to reach out to a much larger audience than the limited number of otherwise in-person participants. Once informed about the decision by the CMO to go hybrid, the organizers decided to reshape the participation concept of the workshop. They decided to

reach out to participants from developing countries and to communities outside coding theory. The goal was to involve people with an interest in coding theory, who would not traditionally be invited to this type of workshop. In particular, we had several attendees from the SIAM Activity Group in Algebraic Geometry and attendees from developing countries working on coding theory or interested to learn more about this research area. The workshop had 205 confirmed members, out of which ten were in-person.

One of our goals was to include, to the extent possible, underrepresented minorities in STEM and have a broad representation of speakers of all genders and career stages. An early-career researcher gave each day an opening talk. The talk aimed to provide an introduction and a research background on one of the five topics. The early-career researchers have been able to showcase their expertise on the topics in front of a large audience. Established researchers presented the remaining two talks of each day with fundamental results on the research topic. Overall, 1/3 speakers were early-career researchers, and 1/3 of the speakers were women.

The organizers decided to limit to three the number of talks each day. This decision was motivated by the large audience attending from across the world and the fact that researchers connecting online likely had other duties at their institutions while attending the conference. Participants appreciated the lighter load. Nonetheless, an online gathering software was available for coffee breaks and for people to meet and collaborate throughout the week of the workshop.

References

[1] Edoardo Ballico and Chiara Marcolla. Higher hamming weights for locally recoverable codes on algebraic curves. *Finite Fields and Their Applications*, 40:61–72, 2016.

[2] Alexander Barg, Itzhak Tamo, and Serge Vlăduţ. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, 63(8):4928–4939, 2017.

[3] Viveck R Cadambe and Arya Mazumdar. Bounds on the size of locally recoverable codes. *IEEE transactions on information theory*, 61(11):5787–5794, 2015.

[4] Ruikai Chen and Sihem Mesnager. A function field approach toward good polynomials for optimal lrc codes. *arXiv preprint arXiv:2103.15443*, 2021.

[5] Ruikai Chen, Sihem Mesnager, and Chang-An Zhao. Good polynomials for optimal lrc of low locality. *Designs, Codes and Cryptography*, 89(7):1639–1660, 2021.

[6] Austin Dukes, Andrea Ferraguti, and Giacomo Micheli. Optimal selection for good polynomials of degree up to five. *Designs, Codes and Cryptography*, pages 1–10, 2022.

[7] Parikshit Gopalan, Cheng Huang, Bob Jenkins, and Sergey Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, 2014.

[8] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information theory*, 58(11):6925–6934, 2012.

[9] Giacomo Micheli. Constructions of locally recoverable codes which are optimal. *IEEE Transactions on Information Theory*, 66(1):167–175, 2019.

[10] Dimitris S Papailiopoulos, Alexandros G Dimakis, and Viveck R Cadambe. Repair optimal erasure codes through hadamard designs. *IEEE Transactions on Information Theory*, 59(5):3021–3037, 2013.

[11] N Prakash, Govinda M Kamath, V Lalitha, and P Vijay Kumar. Optimal linear codes with a local-error-correction property. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 2776–2780. IEEE, 2012.

[12] Natalia Silberstein, Ankit Singh Rawat, O Ozan Koyluoglu, and Sriram Vishwanath. Optimal locally repairable codes via rank-metric codes. In *2013 IEEE International Symposium on Information Theory*, pages 1819–1823. IEEE, 2013.

[13] Itzhak Tamo and Alexander Barg. Bounds on locally recoverable codes with multiple recovering sets. In *2014 IEEE International Symposium on Information Theory*, pages 691–695. IEEE, 2014.

[14] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[15] Itzhak Tamo, Dimitris S Papailiopoulos, and Alexandros G Dimakis. Optimal locally repairable codes and connections to matroid theory. *IEEE Transactions on Information Theory*, 62(12):6661–6671, 2016.

[16] McEliece, Robert J. *A Public-Key Cryptosystem Based On Algebraic Coding Theory*. DSN Progress Report. 44: 114–116, 1978.

[17] H. Niederreiter. *Knapsack-type cryptosystems and algebraic coding theory*. Problems of Control and Information Theory. Problemy Upravlenija i Teorii Informacii. 15: 159–166, 1986.

[18] P. Gaborit, O. Ruatta and J. Schrek. *On the Complexity of the Rank Syndrome Decoding Problem*, in IEEE Transactions on Information Theory, vol. 62, no. 2, pp. 1006-1019, Feb. 2016.

[19] Anna-Lena Horlemann-Trautmann, Kyle Marshall and Joachim Rosenthal. *Extension of Overbeck's Attack for Gabidulin Based Cryptosystems*. In Designs, Codes and Cryptography, vol. 86, no. 2, pages 319-340, 2017/2018.

[20] Anna-Lena Horlemann-Trautmann, Kyle Marshall and Joachim Rosenthal. *Considerations for Rank-based Cryptosystems.* In Information Theory Proceedings (ISIT), 2016 IEEE International Symposium on, Barcelona, Spain, July 2016.

[21] P. Elias, A. Feinstein, and C. Shannon. A note on the maximum flow through a network. *IRE Trans. Inform. Theory*, 2(4):117–119, 1956.

[22] L.R. Ford, and D. R. Fulkerson. Maximal flow through a network. *Canadian journal of Mathematics*, 8:399–404, 1956.

[23] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inform. Theory*, 46(4):1204–1216, 2000.

[24] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Trans. Inform. Theory*, 49(2):371–381, 2003.

[25] R. Kötter, and M. Médard. An algebraic approach to network coding. *IEEE/ACM Trans. Networking*, 11(5):782–795, 2003.

[26] 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 Trans. Inform. Theory*, 52(10):4413–4430, 2006.

[27] N. J. A. Harvey, D. R. Karger, and K. Murota. Deterministic network coding by matrix completion. Proc. 16th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA), 489–498, 2005.

[28] 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 Trans. Inform. Theory*, 51(6):1973–1982, 2005.

[29] R. Dougherty, C. Freiling, and K. Zeger. Network coding and matroid theory. *Proceedings of the IEEE*, 99(3):388–405, 2011.

[30] A. Kim, and M. Médard. Scalar-linear solvability of matroidal networks associated with representable matroids. 2010 6th Int. Symp. Turbo Codes & It. Inf. Proc., 452–456.

[31] Q. T. Sun, X. Yin, Z. Li, and K. Long. Multicast network coding and field sizes. *IEEE Trans. Inform. Theory*, 61(11):6182–6191, 2015.

[32] R. Dougherty, C. Freiling, and K. Zeger. Insufficiency of linear coding in network information flow. *IEEE Trans. Inform. Theory*, 51(8):2745–2759, 2005.

[33] Q. T. Sun, X. Yang, K. Long, X. Yin, and Z. Li. On vector linear solvability of multicast networks. *IEEE Trans. Inform. Theory*, 64(12):5096–5107, 2016.

[34] T. Etzion, and A. Wachter-Zeh. Vector Network Coding Based on Subspace Codes Outperforms Scalar Linear Network Coding. *IEEE Trans. Inform. Theory*, 64(4):2460–2473, 2018.

[35] S. Zhang, S. C. Liew, and P. P. Lam. Hot topic: Physical-layer network coding. In Proc. 12th ICMCN, 358–365, 2006.

[36] C. Feng, D. Silva, and F. R. Kschischang. An algebraic approach to physical-layer network coding. *IEEE Trans. Inform. Theory*, 59(11):7576–7596, 2013.

[37] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft. XORs in the air: Practical wireless network coding. In Proc. 2006 Conf. App., tech., arch., and prot. for comp. comm., 243–254, 2006.

[38] R. W. Yeung, and N. Cai. Network error correction, I: Basic concepts and upper bounds *Comm. Information & Systems*, 6(1):19–35, 2006.

[39] N. Cai, and R. W. Yeung. Network error correction, II: Lower bounds. *Comm. Information & Systems*, 6(1):37–54, 2006.

[40] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard. Resilient network coding in the presence of byzantine adversaries. IEEE INFOCOM 2007, 616–624, 2007.

[41] Z. Zhang. Linear network error correction codes in packet networks. *IEEE Trans. Inform. Theory*, 54(1):209–218, 2008.

[42] R. Koetter, and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[43] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Trans. Inform. Theory*, 54(9):3951–3967, 2008.

[44] D. Silva, and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Trans. Inform. Theory*, 55(12):5479–5490, 2009.

[45] N. Cai, and R. W. Yeung. Secure network coding. In *Proc. 2002 IEEE ISIT*, pages 323, 2002.

[46] N. Cai, and R. W. Yeung. Secure network coding on a wiretap network. *IEEE Trans. Inform. Theory*, 57(1):424–435, 2010.

[47] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio. On the capacity of secure network coding. In Proc. 42nd Allerton Conference, 63–68, 2004.

[48] S. El Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory*, 58(3):1361–1371, 2012.

[49] D. Silva, and F. R. Kschischang. Universal secure network coding via rank-metric codes. *IEEE Trans. Inform. Theory*, 57(2):1124–1135, 2011.

[50] R. W. Nóbrega and B. F. Uchôa-Filho. Multishot codes for network coding: Bounds and a multilevel construction. In *Proc. 2009 IEEE ISIT*, pages 428–432, 2009.

[51] R. W. Nóbrega, and B. F. Uchôa-Filho. Multishot codes for network coding using rank-metric codes. In *Proc. 2010 IEEE IWWNC*, pages 1–6, 2010.

[52] U. Martínez-Peñas Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504:587–612, 2018.

[53] U. Martínez-Peñas A general family of MSRD codes and PMDS codes with smaller field sizes from extended Moore matrices. *SIAM J. Disc. Math* (in press), 2022.

[54] U. Martínez-Peñas and F. R. Kschischang. Reliable and secure multishot network coding using linearized Reed–Solomon codes. *IEEE Trans. Info. Theory*, 65(8):4785–4803, 2019.

[55] E. Byrne, H. Gluesing-Luerssen, and A. Ravagnani. Fundamental properties of sum-rank-metric codes. *IEEE Trans. Info. Theory*, 67(10):6456–6475, 2021.

[56] U. Martínez-Peñas Theory of supports for linear codes endowed with the sum-rank metric. *Des. Codes Crypto.*, 87(10):2295–2320, 2019.

[57] E. Camps-Moreno, E. Gorla, C. Landolina, E. Lorenzo-García, U. Martínez-Peñas, and F. Salizzoni. Optimal Anticodes, MSRD Codes and Generalized Weights in the Sum-Rank Metric. *IEEE Trans. Info. Theory*, 67(10):6456–6475, 2021.

[58] H. Bartz, T. Jerkovits, S. Puchinger, and J. Rosenkilde. Fast decoding of codes in the rank, subspace, and sum-rank metric. *IEEE Trans. Info. Theory*, 67(8):5026–5050, 2021.

[59] S. Puchinger, J. Renner, and J. Rosenkilde. Generic decoding in the sum-rank metric. *IEEE Trans. Info. Theory* (in press), 2022.

[60] U. Martínez-Peñas, M. Shehadeh, and F. R. Kschischang. Codes in the Sum-Rank Metric: Fundamentals and Applications. *Found. Trends Commun. Inf. Theory*, 19(5):814–1031, 2022.

[61] A. Wachter, V. R. Sidorenko, M. Bossert, and V. V. Zyablov. On (partial) unit memory codes based on Gabidulin codes. *Prob. Info. Transmission*, 47(2):117–129, 2011.

[62] A. Wachter-Zeh, M. Stinner, and V. Sidorenko. Convolutional codes in rank metric with application to random network coding. *IEEE Trans. Info. Theory*, 61(6):3199–3213, 2015.

[63] R. Mahmood, A. Badr, and A. Khisti. Convolutional codes with maximum column sum rank for network streaming. *IEEE Trans. Info. Theory*, 62(6):3039–3052, 2016.

[64] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. MRD rank metric convolutional codes. In *Proc. 2017 IEEE ISIT*, 2766–2770, 2017.