AMS-UMI International
Joint Meeting 2024
Palermo, July 23–26, 2024

Algebraic Coding Theory
Special Session B28

Matteo Bonini
Aalborg University, DENMARK

Gretchen L. Matthews
Virginia Tech, USA

Ferdinando Zullo
Università degli Studi della Campania *Luigi Vanvitelli*, ITALY

This special session will focus on the interactions between algebraic coding theory, combinatorics and algebraic geometry. These research areas developed together, each of them playing a crucial role in the advancement of the other. In this session we will explore many different settings, involving Hamming metric codes, rank-metric codes, subspace codes and subfield metric codes, with a wide variety of tools from graph theory, additive combinatorics and finite geometry.

For more information visit `https://matteobonini11.wixsite.com/actumiams2024`.

Schedule and Abstracts

July 25, 2024

11:30–11:50 Matteo Bonini (Aalborg University) - Introductory talk
Abstract. I will give a introductory talk for this session.

12:00–12:45 Daniele Bartoli (University of Perugia) - Scattered spaces, polynomials, and MRD codes
Abstract.

Linear sets find widespread use across diverse mathematical domains, such as Finite Geometry and Coding Theory. Among these, scattered linear sets hold particular significance. This presentation will delve into recent findings concerning exceptional scattered polynomials, scattered sequences, MRD codes, and their interplay with algebraic geometry over finite fields. In many instances, these results have been achieved through insightful polynomial characterizations of the underlying entities.

References

[1] D. Bartoli, A. Cossidente, G. Marino, F. Pavese. *On cutting blocking sets and their codes*, Forum Mathematicum **34**(2), (2022) 347–368.

[2] D. Bartoli, G. Zini, F. Zullo. *Linear maximum rank distance codes of exceptional type*, IEEE Transactions on Information Theory **69**(6), (2023) 3627–3636.

[3] D. Bartoli, G. Marino, A. Neri. *New MRD codes from linear cutting blocking sets*, Annali di Matematica Pura e Applicata **202**, (2023) 115–142.

[4] D. Bartoli, M. Giulietti, G. Zini, *The classification of exceptional scattered polynomials of odd degree*, submitted.

[5] D. Bartoli, G. Marino, A. Neri, L. Vicino, *Exceptional scattered sequences*, submitted.

[6] D. Bartoli, M. Borello, G. Marino, *Saturating linear sets of minimal rank*, Finite Fields and Their Applications **95**, (2024) 102390.

[7] D. Bartoli, G. Longobardi, G. Marino, M. Timpanella, *Scattered trinomials of* $\mathbb{F}_{q^6}[X]$ *in even characteristic*, submitted.

14:30–14:50 Marco Timpanella (University of Perugia) - On Weierstrass semigroups and good AG codes

Abstract.

Ideas from algebraic geometry became useful in coding theory after Goppa's construction [3]. He had the beautiful idea of associating to a curve $\mathcal{X}$ defined over $\mathbb{F}_q$, the finite field with q elements, a code C. This code, called Algebraic-Geometric (AG) code, is constructed from two divisors D and G on $\mathcal{X}$, where one of them, say D, is the sum of n distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$. It turns out that the minimum distance d of C satisfies

$$d \geq n - \deg(G).$$

This is one of the main features of Goppa's construction.

In the theory of Algebraic-Geometric codes, Weierstrass semigroups are crucial for defining bounds on the minimum distance, as well as for defining improvements on the dimension. To ensure good performance, the divisors defining such codes have to be carefully chosen, exploiting the rich combinatorial and algebraic properties of curves. We present some recent examples of the application of Weierstrass semigroups to the construction of AG codes.

References

[1] P. Beelen, N. Tutas, *A generalization of the Weierstrass semigroup*, Journal of Pure and Applied Algebra, vol. 207 (2006), 243–260.

[2] C. Carvalho, F. Torres, *On Goppa codes and Weierstrass gaps at several points*, Designs, Codes, Cryptography, vol. 35 (2005), 211–225.

[3] V. D. Goppa, *A new class of linear correcting codes*, Problemy Peredachi Informatsii, vol. 3 (1970), 24–30.

[4] G. Korchmáros, G. P. Nagy, M. Timpanella, *Codes and gap sequences of Hermitian curves*, IEEE Transactions on Information Theory, vol. 66 (2020), 3547-3554.

[5] G.L. Matthews, T.W. Michel, *One-Point Codes Using Places of Higher Degree*, IEEE Transactions on Information Theory, vol. 51 (2005), 1590-1593.

[6] L. Landi, M. Timpanella, L. Vicino, *Two-point AG codes from one of the Skabelund maximal curves*, IEEE Transactions on Information Theory, (2024).

[7] S. Lia, M. Timpanella, *AG codes from $\mathbb{F}_{q^7}$-rational points of the GK curve*, Applicable Algebra in Engineering, Communication and Computing, vol. 34 (2021), 629-648.

[8] M. Timpanella, *On AG codes from a generalization of the Deligne-Lustzig curve of Suzuki type*, Journal of Mathematical Cryptology (2024).

15:00–15:20 Giovanni Longobardi (University of Naples Federico II) - Towards the classification of maximum scattered linear sets of $\mathrm{PG}(1, q^5)$ and its implications in coding theory

Abstract.

It is known that every linear set of the projective space is either a subgeometry or can be obtained as a projection of a subgeometry [5]. In [2, 7, 4], it was described how the properties of the projection vertex reflect in those of the linear set, especially with regard to those contained in $\mathrm{PG}(1, q^n)$. If $n \leq 4$, this approach led to a complete classification of them, see [1, 3].

In this talk, using various techniques borrowed from linear algebra, projective geometry, algebraic geometry over finite fields and exploiting the above mentioned approach, I will provide a classification result for scattered linear sets of maximum size in $\mathrm{PG}(1, q^5)$.

Finally, using the connections between such linear sets and maximum rank distance codes (shortly MRD codes) established in [6], I will discuss the implications of relevant results for $\mathbb{F}_{q^5}$-linear MRD codes with length 5 and minimum distance $d = 4$.

References

[1] G. Bonoli, O. Polverino, *$\mathbb{F}_q$-linear blocking sets in* $\mathrm{PG}(2, q^4)$, Innov. Incidence Geom. **2** (2005).

[2] B. Csajbók, C. Zanella, *On scattered linear sets of pseudoregulus type in* $\mathrm{PG}(1,q^t)$, Finite Fields Their Appl. **41** (2016), 34-54.

[3] B. Csajbók, C. Zanella, *Maximum scattered* $\mathbb{F}_q$*-linear sets of* $\mathrm{PG}(1,q^4)$, Discrete Math. **341** (2018), 74-80.

[4] G.G. Grimaldi, S. Gupta, G. Longobardi, R. Trombetti, *A geometric characterization of known maximum scattered linear sets of* $\mathrm{PG}(1,q^n)$, preprint.

[5] G. Lunardon, O. Polverino, *Translation ovoids of orthogonal polar spaces,* , Forum Math. **16** (2004) 663-669.

[6] J. Sheekey, *A new family of linear maximum rank distance codes*, Adv. Math. Commun. **10** (3), (2016) 475- 488.

[7] C. Zanella, F. Zullo, *Vertex properties of maximum scattered linear sets of* $\mathrm{PG}(1,q^n)$, Discrete Math. **343** (2020).

15:30–15:50 Alain Couvreur (Inria & Laboratoire LIX, École Polytechnique) - On the decoding of Rank-metric Reed-Muller codes

Abstract.

In 2021, Augot, Couvreur, Lavauzelle and Neri [1] proposed a construction of rank metric analogues of Reed–Muller codes from twisted group algebras associated to a Galois extension. However, they did not provide an efficient decoding algorithm correcting up to half the minimum distance.

In this talk, we propose two approaches addressing this issue. On one hand, for extensions with Galois group $(\mathbb{Z}/2\mathbb{Z})^n$, we identify common features shared with binary Reed–Muller codes with in particular a recursive structure in the spirit of Plotkin's $(u \mid u+v)$ construction. These observations lead to a decoding algorithm correcting up to half the minimum distance with a high probability. On the other hand, for extensions whose Galois group are a product of two cyclic groups, we propose a completely new approach based on Dickson matrices permitting to correct any error pattern up to half the minimum distance.

References

[1] D. Augot, A. Couvreur, A. Neri, J. Lavauzelle, *Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed-Muller codes*, SIAM J. Appl. Algebra Geom. 5(2), pp 165–199, 2021.

16:00–16:20 Martino Borello (University of Paris 8 - LAGA) - The geometry of intersecting codes: bounds and constructions

Abstract.

Intersecting codes are linear codes in which every pair of nonzero codewords has a non-trivially intersecting support. They are a classical subject in coding theory introduced in [4,5] and extensively explored in subsequent articles (see, e.g., [2,3,7]), primarily focusing on the binary case. In this context, such codes coincide with minimal codes, which have been intensively studied over the past 20 years. Intersecting and minimal codes find several practical applications: facilitating communication over AND channels, usage in secret sharing schemes, and connections to other structures such as frameproof codes [1] and $(2,1)$-separating systems [6].

In this talk, we primarily delve into the geometric interpretation of intersecting codes, a subject largely unexplored until now. It is well-known that a nondegenerate linear code can be associated with a set of points (with multiplicities) in a projective space, and some coding-theoretical properties can be understood geometrically. This perspective bridges MDS codes with problems in projective geometry (the renowned MDS conjecture was initially formulated as such in [8]), covering problems with saturating sets, minimal codes with strong blocking sets, and so forth. Intersecting codes correspond to sets of points not contained within any pair of hyperplanes. We term such sets as *non-2-cohyperplanar*. This geometric interpretation of intersecting codes not only aids in visualizing fundamental properties but also paves the way for the introduction of novel constructions.

References

[1] S. R. Blackburn. *Frameproof codes.* SIAM Journal on Discrete Mathematics, 16(3):499–510, 2003.

[2] G. D. Cohen and A. Lempel. *Linear intersecting codes.* Discrete Mathematics, 56:35–43, 1984.

[3] G. D. Cohen and G. Zemor. *Intersecting codes and independent families.* IEEE Transactions on Information Theory, 40(6):1872–1881, 1994.

[4] G. Katona and J. Srivastava. *Minimal 2-coverings of a finite affine space based on GF(2).* Journal of statistical planning and inference, 8(3):375–388, 1983.

[5] D. Miklós. *Linear binary codes with intersection properties.* Discrete Applied Mathematics, 9(2):187–196, 1984.

[6] H. Randriambololona. *(2, 1)-separating systems beyond the probabilistic bound.* Israel Journal of Mathematics, 195:171–186, 2013.

[7] C. T. Retter. *Intersecting goppa codes.* IEEE transactions on information theory, 35(4):822–828, 1989.

[8] B. Segre. *Curve razionali normali ek-archi negli spazi finiti.* Annali di Matematica Pura ed Applicata, 39:357–379, 1955.

17:00–17:20 Martin Scotti (University of Paris 8 - LAGA) - Intersecting codes and their applications to additive combinatorics and factorization theory

Abstract.

Intersecting codes are linear codes in which every pair of nonzero codewords has a non-trivially intersecting support. They are a classical subject in coding theory introduced in [4,5] and extensively explored in subsequent articles (see, e.g., [2,3,7]), primarily focusing on the binary case. In this context, such codes coincide with minimal codes, which have been intensively studied over the past 20 years. Intersecting and minimal codes find several practical applications: facilitating communication over AND channels, usage in secret sharing schemes, and connections to other structures such as frameproof codes [1] and $(2, 1)$-separating systems [6].

In this talk, building on a connection already explored in [8, 9], we explore the link between intersecting codes and the problem of the 2-wise Davenport constant: considering a sequence of elements from an elementary abelian group, it is possible to construct a matrix. Interpreting this matrix as the parity-check matrix of a code, we observe that codewords correspond to weighted zero-sum subsequences. The problem of determining the 2-wise Davenport constant is then equivalent to determining for which parameters intersecting codes exist. This allows us to deduce properties of the 2-wise Davenport constant from the properties of intersecting codes. Applying this knowledge to nonunique factorization theory in Dedekind rings, using the classical example of the ring of integers of an algebraic number field, we give some new bounds on the number of prime ideals in the factorization of the product of two irreducible elements.

References

[1] S. R. Blackburn. *Frameproof codes.* SIAM Journal on Discrete Mathematics, 16(3):499–510, 2003.

[2] G. D. Cohen and A. Lempel. *Linear intersecting codes.* Discrete Mathematics, 56:35–43, 1984.

[3] G. D. Cohen and G. Zemor. *Intersecting codes and independent families.* IEEE Transactions on Information Theory, 40(6):1872–1881, 1994.

[4] G. Katona and J. Srivastava. *Minimal 2-coverings of a finite affine space based on GF(2).* Journal of statistical planning and inference, 8(3):375–388, 1983.

[5] D. Miklós. *Linear binary codes with intersection properties.* Discrete Applied Mathematics, 9(2):187–196, 1984.

[6] H. Randriambololona. *(2, 1)-separating systems beyond the probabilistic bound.* Israel Journal of Mathematics, 195:171–186, 2013.

[7] C. T. Retter. *Intersecting goppa codes.* IEEE transactions on information theory, 35(4):822–828, 1989.

[8] A. Plagne and W. Schmid *An application of coding theory to estimating Davenport constants.* Designs, Codes and Cryptography, 61:105–118, 2010.

[9] L. Marchan and O. Ordaz and I. Santos and W. Schmid *Multi-wise and constrained fully weighted Davenport constants and interactions with coding theory.* Journal of Combinatorial Theory, Series A, 135:237–267, 2015.

17:30–17:50 Eimear Byrne (University College Dublin) - Subfield-Metric Codes
Abstract.

Motivated by applications in quantum error correction, in [3] the authors introduced the subfield metric. Given positive $\lambda \in \mathbb{R}$, the λ-subfield weight wt_λ of an element x of the finite field $\mathbb{F}_{q^m}$ is 0 if $x = 0$, is 1 if $x \in \mathbb{F}_q^\times$, and takes the value λ otherwise. This weight assignment hence induces the partition $\mathbb{F}_{q^m}/\theta = \{\{0\}, \mathbb{F}_q^\times, \mathbb{F}_{q^m} \backslash \mathbb{F}_q\}$. It is extended additively to yield a weight function on $\mathbb{F}_{q^m}^n$, that is $\mathrm{wt}_\lambda(x) := \sum_{j=1}^n \mathrm{wt}_\lambda(x_j)$ for all $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. If $\lambda \geq 1/2$, it was shown in [3] that the induced distance function $\mathrm{d}_\lambda(x, y) := \mathrm{wt}_\lambda(x - y)$ for all $x, y \in \mathbb{F}_{q^m}^n$ is a distance function on $\mathbb{F}_{q^m}^n$. For applications in quantum error correction, the most interesting case appears to be $m = 2$ and $\lambda > 1$.

We show that the subfield metric satisfies the extension property and that this can be proved both by a direct argument and also by an application of a result of Dyshko and Wood (see [2, Theorem 5.1]).

Theorem 1. *Let C and D be a pair of $\mathbb{F}_{q^m}$-$[n, k]$ codes. Then C and D are isometric by an $\mathbb{F}_{q^m}$-linear map $\phi : C \longrightarrow D$ if and only if ϕ is the restriction to C of an $\mathbb{F}_q$-monomial transformation of $\mathbb{F}_{q^m}^n$.*

We next consider code optimality in relation to this metric. We describe a simple class of Plotkin-optimal codes. We obtain a duality result for linear codes for the subfield metric. We apply the methods of [1] to obtain explicit expressions for transform polynomials, which applied to the distance distribution of a subfield metric code, gives a linear programming bound. We demonstrate the effectiveness of this bound with some computations comparing its output to existing bounds in [3].

References

[1] E. Byrne, M. Greferath, and M. O'Sullivan, *The linear programming bound for codes over finite Frobenius rings.* Designs, Codes and Cryptography, 42(3):289–301, 2007.

[2] S. Dyshko and J. Wood, *MacWilliams extension property for arbitrary weights on linear codes over module alphabets.* Designs, Codes and Cryptography, 90(11):2683–2701, 2022.

[3] M. Grassl, A.-L. Horlemann, V. Weger, *The Subfield Metric and its Application to Quantum Error Correction*, Journal of Algebra and Its Applications, https://doi.org/10.1142/S021949882550063X, 2023.

18:00–18:20 Hsin-Po Wang (Apple Research Fellow, Simons Institute for the Theory of Computing) - How to Speak Tensor
Abstract.

Tensor is an algebraic operation that combined a set of vector spaces into a big vector space. It can be used out of trivial codes. In this talk, we will go over four creative applications: distributed storage, distributed matrix multiplication, local testability and quantum error correction.

July 26, 2024

11:30–11:50 Olgica Milenkovic (University of Illinois) - Can Coding Reduce Deduplication Fragmentation?
Abstract.

Data deduplication is the process of removing replicas of data chunks stored by different users on servers, and is one of the key features of modern Big Data storage devices. Despite the importance of the methods, prior theoretical works have not addressed one of the major drawbacks of deduplication: file fragmentation. Fragmentation arises when placing deduplicated data chunks of different user files in linear order in the chunk store, because neighboring chunks of the same file may be stored in sectors far apart on the store. The contributions of our work are three-fold. First, we describe a new model for file structures of the form of self-avoiding paths in graphs (such as sparse Hamiltonian path graphs, trees etc) and introduce the notation of *fragmentation level* and *jumping index*. The fragmentation level captures the worst-case "spread" of data chunks in a file when deduplicated and placed on the server. The jumping index, on the other hand, represents the worst-case number of jumps in the store that one has to make in order to retrieve a file. Second, we establish connections between the notion of the fragmentation level and bandwidth of the file graph, and introduce a new graph-theoretic problem that allows for a succinct characterization of the jumping index. Importantly, we suggest techniques for adding redundancy and coded chunks to the store that allow one to reduce the fragmentation level as well as the jumping index. The key ideas behind our approach are information-theoretic arguments regarding redundant chunk store fragmentation levels, as well as a new algorithms of *graph folding* and jumping index aggregation on trees.

12:00–12:45 Sihem Mesnager (Universities of Paris VIII and Sorbonne Paris Cité, LAGA, CNRS) - Functions-based codes: results and open problems
Abstract.

One of the leading research problems in coding theory is constructing new linear codes with appropriate parameters (functional in communication systems, consumer electronics and data storage systems), determining their weight distributions and studying their dual codes. This research also pays particular attention to applications.

This talk concentrates on linear codes. We aim to present results and open questions by selecting families of linear codes over finite fields with arbitrary characteristics (some of them are designed for (toward) specific intended applications). Specifically, the emphasis will be on linear codes created from functions over finite fields. We shall discuss the advantages and limitations.

14:30–14:50 Kathryn Haymaker (Villanova University) - New asymptotic bound for codes from hypergraphs
Abstract.

Let X be a finite set and $\binom{X}{r}$ the collection of all subsets of X with r elements. An *r-uniform hypergraph* $\mathcal{H}$ with vertex set X is a subset of $\binom{X}{r}$. A *Berge cycle of length k* in a hypergraph is a sequence of k distinct vertices $v_1, \ldots, v_k$ and k distinct edges $e_1, \ldots, e_k$ such that $\{v_i, v_{i+1}\} \subseteq e_i$. A hypergraph $\mathcal{H}$ has girth at least g if $\mathcal{H}$ has no Berge cycles of length k for every $2 \leq k \leq g-1$. Denote the family of Berge cycles of length at most $g-1$ as $\mathcal{C}_{<g}$, and notice that a hypergraph has girth at least g if and only if it is $\mathcal{C}_{<g}$-free. Given a family of r-uniform hypergraphs $\mathcal{F}$, the *Turán number* for $\mathcal{F}$ is the maximum number of edges in an r-uniform N-vertex hypergraph that is $\mathcal{F}$-free, denoted $\mathrm{ex}_r(N, \mathcal{F})$. The asymptotic behavior of these numbers in general is unknown.

Suppose that H is a parity check matrix for an $[n, k, d]_q$ code, of size $t \times N$ with entries in $\mathbb{F}_q$ for some prime power q. Taking $R = \mathbb{F}_q^t$ and $S = \mathbb{F}_q$, we present the following hypergraph construction. Let $r \geq 2$ be an integer. Let $\vec{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ be a vector whose entries are elements of S. For $R' \subset R$ and $A \subset R$, define $\mathcal{H}(A, \vec{\lambda})$ to be the r-uniform r-partite hypergraph with vertex set $\cup_{i=1}^{r}(R' \times \{i\})$ and edge set

$$\bigcup_{x \in R', a \in A} \{((x + \lambda_1 a, 1), ((x + \lambda_2 a, 2), (x + \lambda_3 a, 3), \ldots, (x + \lambda_r a, r))\}.$$

We show that a Berge cycle in $\mathcal{H}(A, \vec{\lambda})$ implies the existence of an equation in R whose coefficients are differences of the entries of $\vec{\lambda}$, satisfied by elements in A.

A series of code constructions by Dumer [2] establish the existence of linear codes of distance $d = 5$ and $d = 6$ with improved parameters in comparison with BCH codes.

In general we use H to denote a parity-check matrix for one of these codes. Let $A \subset \mathbb{F}_q^t$, where A is the set of columns of H. We define $\mathcal{H}_5 = \mathcal{H}(A, \vec{\lambda})$, where the elements of $\vec{\lambda}$ are a Sidon set in $\mathbb{F}_q$. Since a code of distance 6 (over a field with large enough q) can yield a hypergraph, we can apply results from hypergraphs to establish an asymptotic bound for codes.

The asymptotic sphere-packing bound for linear codes states that for any $[n, k, 6]_q$ code, $k \leq n - 2\log_q(n) - O(1)$, which for a fixed small distance like $d = 6$ is the best asymptotic bound known. To obtain Theorem 3, we employ the correspondence between codes and hypergraphs described above, and use a recent result of Conlon, Fox, Sudakov, and Zhao [1]:

Theorem 2 (Cor. 1.10, Ref. 1)**.** *For $r \geq 3$, every r-uniform hypergraph on N vertices with girth 6 has $o(n^{3/2})$ edges.*

Theorem 3. *If C is a linear $[n, k, 6]_q$ code, then $k \leq n - 2\log_q n - \omega(1)$, where $\omega(1)$ is a function that goes to infinity with n.*

This improves the asymptotic sphere packing bound for linear q-ary codes of distance 6.

References

[1] D. Conlon, J. Fox, B. Sudakov, and Y. Zhao. The regularity method for graphs with few 4-cycles. *Journal of the London Mathematical Society*, 104(5):2376–2401, 2021.

[2] I. Dumer. Nonbinary double-error-correcting codes designed by means of algebraic varieties. *IEEE Transactions on Information Theory*, 41(6):1657–1666, 1995.

15:00–15:20 Alessandro Neri (Ghent University) - Union-Closed Linear Codes

Abstract.

A family of subsets of a finite set is said to be *union-closed* if, for any pair of sets in the family, also their union belongs to the family. Union-closed families of sets have been investigated from a wide variety of mathematical points of view, due to the notorious long-standing conjecture which was proposed by Frankl 1979. Its statement is quite elementary:

> "*For every finite union-closed family of sets with at least two elements, there exists an element that belongs to at least half of the sets in the family.*"

In this talk we study union-closed sets families arising from the theory of error-correcting codes. More precisely, we deal with union-closed sets families which coincide with families of supports of linear codes over a finite field. This linearity enriches the corresponding union-closed sets family with interesting geometric and algebraic features, which we exploit to derive results on the combinatorial side.

15:30–15:50 Giuseppe Cotardo (Virginia Tech) - Rank-Metric Lattices and Finite Geometry

Abstract.

Rank-Metric Lattices (RML in short) were introduced in [1] as the q-analogue of Higher-Weight Dowling Lattices [3,4]. They are special families of geometric lattices whose elements are the $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$ having a basis of vectors with rank weight bounded from above, ordered by inclusion.

In this talk, we investigate the properties of RMLs from a finite geometry perspective. We compute the Whitney numbers of the first kind for some of these lattices, providing a recursive formula. In the second part of the talk, we present asymptotic results on the density of some classes of cardinality-optimal rank-metric codes.

References

[1] G. Cotardo, A. Ravagnani, *Rank-metric lattices*, The Electronic Journal of Combinatorics, P1–4, 2023.

[2] B. Csajbók, C. Zanella, *Maximum scattered* $\mathbb{F}_q$*-linear sets of* $\mathrm{PG}(1, q^4)$, Discrete Mathematics, 341(1), pp. 74–80, 2018.

[3] T. A. Dowling, *Codes, Packings and the critical problem*, Atti del Convegno di Geometria Combinatoria e sue Applicazioni, pp. 209–224, 1971.

[4] T. A. Dowling, *A q-analog of the partition lattice*, A Survey of Combinatorial Theory, pp. 101–115. 1973.

[5] S. E. Payne, *A complete determination of translation ovoids in finite Desarguian planes*, Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, 51(5), pp. 328–331, 1971.

[6] A. Ravagnani, *Whitney numbers of combinatorial geometries and higher-weight Dowling lattices*, SIAM Journal on Applied Algebra and Geometry, 6(2), pp. 156–189, 2022.

16:00–16:20 Julia Shapiro (Virginia Tech) - Capacity of Adversarial Networks in the Multishot Regime

Abstract.

Adversarial network coding studies the transmission of data over networks affected by adversarial noise. In this realm, the noise is modeled by an omniscient adversary who is restricted to corrupting a proper subset of the network edges. In [4], Ravagnani and Kschischang established a combinatorial framework for adversarial networks. The study was recently furthered by Beemer, Kilic and Ravagnani [1,2], with particular focus on the one-shot capacity: a measure of the maximum number of symbols that can be transmitted in one use of the network without errors.

In this talk, we present recent results on the capacity of networks in multiple transmission rounds. We also discuss scenarios where there is a gain in capacity in using a network multiple times for communication versus using the network once and extend bounds from the one-shot capacity regime to the multishot regime.

References

[1] A. Beemer, A. Kılıç, A. Ravagnani, *Network decoding against restricted adversaries*, IFAC-PapersOnLine, vol. 55, pp. 236–241, 2022, doi:10.1016/j.ifacol.2022.11.058.

[2] A. Beemer, A. Kılıç, A. Ravagnani, *Network decoding*, in IEEE Transactions on Information Theory, vol. 69, no. 6, pp. 3708– 3730, June 2023, doi: 10.1109/TIT.2023.3241409.

[3] G. Cotardo, G. L. Matthews, A. Ravagnani, J. Shapiro, *Multishot adversarial network decoding*, 2023 59th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2023, pp. 1–8, doi: 10.1109/Allerton58177.2023.10313407.

[4] F. Kschichang, A. Ravagnani, *Adversarial network coding*, in IEEE Transactions on Information Theory, vol. 65, no. 1, pp. 198–219, Jan. 2019, doi: 10.1109/TIT.2018.2865936.

17:00–17:20 Olga Polverino (University of Campania) - Full weight spectrum cyclic subspace codes

Abstract.

For a linear Hamming metric code $\mathcal{C}$ of length n over $\mathbb{F}_q$, we define the weight set as

$$w(\mathcal{C}) = \{w(c) \colon c \in \mathcal{C} \setminus \{0\}\}.$$

It is easy to see that $|w(\mathcal{C})| \leq n$. The codes attaining the equality in the above bound were called **full weight spectrum** codes; see [1].

In this talk we will focus on the analog class of codes in the framework of cyclic subspace codes. Subspace codes gained a lot of attention especially because they may be used in random linear network coding for correction of errors and erasures. Let denote by $\mathcal{G}_q(n, k)$ the Grassmaniann

of all the $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$ of dimension k, equipped with the subspace distance introduced in [2]. A **one-orbit cyclic subspace code** $\mathcal{C}$ is a subspace code in $\mathcal{G}_q(n,k)$ such that

$$\mathcal{C} = \{\alpha U \colon \alpha \in \mathbb{F}_{q^n} \setminus \{0\}\}$$

for some $U \in \mathcal{G}_q(n,k)$. In this framework, defined $\omega_i = |\{\alpha U \colon \alpha \in \mathbb{F}_{q^n}^*, d(U, \alpha U) = i\}|$, the weight set of the code is

$$w(\mathcal{C}) = \{\omega_i \, : \, i \in \mathbb{N} \text{ and} \, \omega_i > 0\}.$$

One can easily check that the size of such a weight set is at most k. Similarly to the Hamming metric case, we define **full weight spectrum** codes those codes $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ such that $|w(\mathcal{C})| = k$. In this talk, we will see examples and characterization results of full weight spectrum one-orbit cyclic subspace codes.

References

[1] T.L. Alderson, *A note on full weight spectrum codes*, Trans. Comb., 8 n. 3 (2019), 15–22.

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

17:30–17:50 Gianira N. Alfarano (University College Dublin) - Constant Dimension Subspace Codes in Schubert Varieties

Abstract.

In [1], Ahlswede et al. came out with the idea that in network communication nodes can combine the inputs received and forward the new messages. This networking technique is known nowadays as *network coding*: transmitted data are encoded and decoded in order to increase network throughput, reduce delays and make the network robust. In the seminal paper [3], Kötter and Kschischang introduced the concept of transmitting information over a network encoded in subspaces. A **constant dimension subspace code** is a set of subspaces with fixed dimension of a given vector space over a finite field. In this context, the source sends a (basis of a) vector subspace and the receiver gathers a (basis of a) vector subspace possibly affected by noise. An important parameter to measure the error-correction capacity is the minimum distance of a (constant dimension) subspace code, which is the minimum among the subspace distances of any two distinct subspaces in the code.

In this talk, we consider constant dimension subspace codes restricted to Schubert varieties, which means that we allow as codewords only subspaces with a particular shape. We are interested in finding the largest size of a constant dimension subspace code with prescribed minimum distance value in some Schubert varieties. We will present the general problem, that turns out to have a natural description as a problem of incidence geometry. When the prescribed minimum distance is the largest possible, we provide a construction of maximum size constant dimension subspace codes which uses the notion of *linear sets* in projective geometry.

The talk is based on the recent paper [2].

References

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

[2] G.N. Alfarano, J. Rosenthal, B. Toesca, *Constant Dimension Subspace Codes in Schubert Varieties*, preprint 2024.

[3] R. Köetter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information theory, 54(8):3579–3591, 2008.

18:00–18:20 Chiara Castello (University of Campania) - On generalized Sidon spaces

Abstract.

Since [3], subspace codes have gained a strong interest due to their use for the error correction in random network coding. The first class of subspace codes was the one of cyclic subspace codes, originally introduced in [2]. We will focus on one-orbit cyclic subspace codes, i.e. given an $\mathbb{F}_q$-subspace S of $\mathbb{F}_{q^n}$, the one-orbit cyclic subspace code defined by S is

$$\mathrm{Orb}(S) = \{\alpha S \colon \alpha \in \mathbb{F}_{q^n}^*\} \subseteq \mathcal{G}_q(n,k),$$

where $\alpha S = \{\alpha s \colon s \in S\}$ and $\mathcal{G}_q(n,k)$ is the Grassmannian of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^n}$. In [4] Roth, Raviv and Tamo pointed out the connection between one-orbit cyclic subspace codes and Sidon spaces. They have been introduced in [1] by Bachoc, Serra and Zémor as the q-analogue of Sidon sets, classical combinatorial objects introduced by Simon Szidon. The authors of [4] also introduced the notion of r-Sidon spaces, as an extension of Sidon spaces, which may be seen as the q-analogue of B_r-sets, a generalization of classical Sidon sets.
In this work we will investigate one-orbit cyclic subspace codes, through some properties of Sidon spaces and r-Sidon spaces, providing upper and lower bounds on the possible dimension of their *r-span* and showing explicit constructions in the case in which the upper bound is achieved.

References

[1] C. Bachoc, O. Serra and G. Zémor, An analogue of Vosper's theorem for extension fields, Math. Proc. Cambridge Philos. Soc., 163(3), 423–452, 2017.

[2] T. Etzion and A. Vardy, Error-correcting codes in projective space, IEEE Trans. Inform. Theory, 57(2), 1165-1173, 2011.

[3] R. Koetter and F. R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inform. Theory, 54, 3579–3591, 2008.

[4] R. M. Roth, N. Raviv and I. Tamo, Construction of Sidon spaces with applications to coding, IEEE Trans. Inform. Theory, 64(6), 4412–4422, 2018.

E–mail: ferdinando.zullo@unicampania.it.