OpeRa 2024 – Caserta

Open Problems on Rank-Metric Codes

Founded by Programme Cassini and COMBINE

Supported by

OpeRa 2024-Caserta©, 2024

Contents

About

OpeRa 2024

OpeRa 2024 is a workshop dedicated to the latest advancements in rank-metric code theory, covering various aspects of the field.
This event is designed for researchers in rank-metric codes, both experienced and young, as well as those familiar with the subject but still not active on it who are interested in exploring new problems. It offers a platform to discover fresh perspectives and potential collaborations in the realm of rank-metric codes.

Organizing and Scientific Committee

Martino Borello	(University Paris 8 - LAGA)	co-chair
Julien Lavauzelle	(University Paris 8 - LAGA)	
Olga Polverino	(University of Campania "Luigi Vanvitelli")	
Ferdinando Zullo	(University of Campania "Luigi Vanvitelli")	co-chair

Local Organizing Committee

Chiara Castello	(University of Campania "Luigi Vanvitelli")
Giovanni Longobardi	(University of Naples Federico II)
Vito Napolitano	(University of Campania "Luigi Vanvitelli")
Paolo Santonastaso	(University of Campania "Luigi Vanvitelli")
Martin Scotti	(University Paris 8 - LAGA)

Timetable

CT: Contributed Talk, IS: Invited Speaker.

Wednesday, February 14th

9:00	**Organizers Welcome and Introduction**		
9:20–10:30	IS	**Alessandro Neri** Ghent University	Ferrers diagram rank-metric codes
10:30–11:00	**Coffee Break**		
11:00–12.10	IS	**Magali Bardet** University of Rouen Normandy	Algebraic attacks for the Rank Decoding Problem
12:10–14.00	**Lunch Break**		
14:00–15.10	IS	**Daniele Bartoli** University of Perugia	Recent results on scattered spaces and MRD codes
15:10–15:40	**Coffee Break**		
15:40-16.05	CT	**Valentin Suder** University of Rouen Normandy	(Near) Constant-Rank Codes and (A)PN functions
16:05-16:30	CT	**Alessandro Giannoni** University of Perugia	Exceptional and indecomposable scattered sequences of order $m > 2$
16:30–16:55	CT	**Francesco Ghiandoni** University of Perugia	On 3-dimensional MRD codes
16:55–17:20	CT	**Giovanni Giuseppe Grimaldi** University of Naples	Non-linear MRD codes from cones over exterior sets

Thursday, February 15th

9:20–10:30	IS	**Pierre Loidreau** University of Rennes 1 and DGA	How to design a McEliece like encryption scheme in rank metric?
10:30–11:00	**Coffee Break**		
11:00–11:25	CT	**Hugo Sauerbier Couvée** Technical University of Munich	How (not) to decode in the rank metric
11:25–11:50	CT	**Rakhi Pratihar** Inria Saclay Centre	Decoding rank metric Reed-Muller codes
11:50–12:25	CT	**Valentina Astore** University of Trento	Castelnuovo-Mumford Regularity in the Rank Metric
Afternoon	**Social Trip**		
Evening	**Social Dinner**		

Friday, Febraury 16th

9:20 – 10:30	IS	**Eimear Byrne** University College Dublin	Zeroes of the Zeta Polynomial of a Rank-Metric Code
10:30–11:00	**Coffee**		
11:00-12:10	IS	**Gianira N. Alfarano** VUB, UCD	The critical problem for rank-metric codes
12:45–14:00	**Lunch Break**		
14:00-15:10	IS	**Giuseppe Marino** University of Naples	Cutting blocking sets, saturating linear sets and rank-metric codes
15:10–15:50	**Coffee Break**		
15:40–16:05	CT	**Somi Gupta** University of Naples	A geometric characterization of known maximum scattered linear sets of $\mathrm{PG}(1, q^n)$
16:05–16:30	CT	**Elena Berardini** CNRS; University of Bordeaux	Algebraic Geometry codes in the sum-rank metric
16:30–16:55	CT	**Antonina P. Khramova** Eindhoven University of Technology	Eigenvalue bounds for sum-rank-metric codes

The Critical Problem for Rank-Metric Codes

Gianira N. Alfarano

IS

Vrije Universiteit Brussel, Belgium & University College Dublin, Ireland

(joint work with Eimear Byrne)

Keywords: Critical problem, rank-metric codes, q-polymatroids

In classical combinatorics, polymatroids have been introduced as an extension of the concept of matroids. There are many known connections between linear codes and matroids and many invariants in coding theory which are also matroid invariants. q-Matroids and q-polymatroids have been defined as the q-analogue of matroids and polymatroids. These objects gained a lot of interest among an increasing number of researchers, especially in the last few years, due to their connection with rank-metric codes. In particular, in [4] it has been shown that to an $\mathbb{F}_q$-linear rank metric code $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ it can be associated a q-polymatroid $M_\mathcal{C}$ and when $\mathcal{C}$ is also $\mathbb{F}_{q^m}$-linear, $M_\mathcal{C}$ is, in fact, a q-matroid; see also [3].

In this talk we will illustrate the solution of the q-analogue of the celebrated Critical Problem, proposed by Crapo and Rota in [2]. We will make use of the characteristic polynomial of a q-polymatroid as a basic tool for this result. Finally, we will provide the coding theoretic interpretation and we will *partially* solve it for *maximum rank distance (MRD)* codes. This talk is based on a joint work with Eimear Byrne; see [1].

References

[1] G.N. Alfarano, E. Byrne. *The Critical Theorem for q-Polymatroids*. *submitted*.

[2] H. Crapo, G.-C. Rota, *On the foundations of combinatorial theory: Combinatorial geometries*. MIT Press, 1970.

[3] R. Jurrius, R. Pellikaan, *Defining the q-Analogue of a Matroid*. The Electronic Journal of Combinatorics, (2018)

[4] E. Gorla, R. Jurrius, H. López, A. Ravagnani. *Rank-metric codes and q-polymatroids*. Journal of Algebraic Combinatorics, **52**(1), 1–19 (2020).

Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium.
University College Dublin, School of Mathematics and Statistics, Science Centre Belfield Dublin 4.
email: `gianira.alfarano@ucd.ie`

Algebraic attacks for the Rank Decoding Problem

Magali Bardet
University of Rouen Normandy, France

IS

The Rank Decoding problem (RD) is at the core of rank-based cryptography. Cryptosystems such as ROLLO and RQC, which made it to the second round of the NIST Post-Quantum Standardization Process, as well as the Durandal signature scheme, rely on it or its variants. This problem can also be seen as a structured version of MinRank, which is ubiquitous in multivariate cryptography. In this talk, I will present several algebraic modelings for this problem, and analyze the complexity of solving them to get an upper bound on the complexity of these algebraic approaches.

Univ Rouen Normandie, LITIS UR 4108, F-76000 Rouen, France
email: `magali.bardet@univ-rouen.fr`

Recent results on scattered spaces and MRD codes

Daniele Bartoli
IS
University of Perugia, Italy

Keywords: Scattered linear sets, MRD codes

Linear sets have numerous applications in various areas of mathematics, including Finite Geometry and Coding Theory. Among them, scattered linear sets play a special role. In this talk, I will present recent results related to exceptional scattered polynomials, scattered sequences, MRD codes, and their connection with algebraic geometry over finite fields.

References

[1] D. Bartoli, A. Cossidente, G. Marino, F. Pavese. *On cutting blocking sets and their codes*. Forum Mathematicum 34(2), 347–368 (2022).
[2] D. Bartoli, G. Zini, F. Zullo. *Linear maximum rank distance codes of exceptional type*. IEEE Transactions on Information Theory 69(6), 3627–3636 (2023).
[3] D. Bartoli, G. Marino, A. Neri. *New MRD codes from linear cutting blocking sets*. Annali di Matematica Pura e Applicata 202, 115–142 (2023).
[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*, submitted.
[7] D. Bartoli, G. Longobardi, G. Marino, M. Timpanella. *Scattered trinomials of $\mathbb{F}_{q^6}[X]$ in even characteristic*, submitted.

University of Perugia, Department of Mathematics and Informatics, via Vanvitelli 1, 06123 Perugia
email: `daniele.bartoli@unipg.it`

Zeroes of the Zeta Polynomial of a Rank-Metric Code

Eimear Byrne

IS

University College Dublin, Ireland

Keywords: Zeta polynomial, Riemann hypothesis, rank-metric code

The zeta polynomial of an $\mathbb{F}_q$-$[n,k,d]$ code $\mathcal{C}$ is the unique polynomial $P_{\mathcal{C}}(T)$ of degree at most $n-d$ such that:

$$\frac{P_{\mathcal{C}}(T)}{(1-T)(1-qT)}((x-y)T+y)^n = \cdots + \frac{A_{\mathcal{C}}(x,y)-x^n}{q-1}T^{n-d} + \cdots \tag{1}$$

where $A_{\mathcal{C}}(x,y)$ is the Hamming-weight enumerator of $\mathcal{C}$. The theory of zeta polynomials for linear codes was introduced and studied by Duursma in a series of papers [4,3,5] and is inspired by the theory of Hasse-Weil zeta functions of algebraic curves. A survey and related open problems can be read in [6].

A q-analogue of this result appeared in [1]: the zeta polynomial of an $\mathbb{F}_q$-$[n \times m, k, d]$ rank-metric code $\mathcal{C}$ is the unique polynomial of degree at most $n-d$ such that:

$$\frac{P_{\mathcal{C}}(T)}{(1-T)(1-q^mT)}\sum_{r=0}^{n}\begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{j=0}^{r}(x-q^jy)y^{n-r}T^r = \cdots + \frac{A_{\mathcal{C}}(x,y)-x^n}{q^m-1}T^{n-d} + \cdots \tag{2}$$

where $A_{\mathcal{C}}(x,y)$ is the rank-weight enumerator of $\mathcal{C}$. Observe that (1) is obtained from (2) as $q \longrightarrow 1$.

The zeta polynomial $P_{\mathcal{C}}(T) = \sum_{j=0}^{n-d} = p_0 + \cdots p_{n-d}T^{n-d}$ is the unique polynomial such that $A_{\mathcal{C}}(x,y) = \sum_{i=0}^{n-d} p_i M_{n,d+i}(x,y)$, where $M_{n,d+i}(x,y)$ is the weight enumerator of an MDS code in the case of the Hamming metric and is the weight enumerator of an MRD code in the case of the rank metric. In particular, Singleton-extremal weight enumerators have constant zeta polynomial. The zeta polynomial can also be defined in terms of the *binomial moments* of a code and so encodes information on the dimensions of its shortened subcodes.

The complex roots of the zeta polynomial of an algebraic curve over $\mathbb{F}_q$ all have absolute value $1/\sqrt{q}$ and in this sense such polynomials satisfy the Riemann hypothesis (RH). For a (formally) self-dual code over $\mathbb{F}_{q^m}$, the reciprocal zeroes of $P_{\mathcal{C}}(T)$ occur in pairs $\{\alpha, q^m/\alpha\}$ and occur as conjugate pairs if and only if both have absolute value $1/\sqrt{q^m}$. One can ask if RH is satisfied by the zeta polynomial associated with a self-dual weight enumerator. The answer to this question in general is negative, but then one may consider the question of classifying those weight enumerators for which RH does hold. In the Hamming metric, there are several results already known; see e.g. [2,3,7,8] and the references therein. In particular, some infinite families of extremal self-dual codes satisfy RH and many negative cases have been considered.

On the other hand, in the case of rank-metric codes, the question is virtually unexplored. There are some examples of self-dual codes whose zeta polynomial is the same as that of an algebraic curve and hence RH then holds. In the Hamming metric case, heuristics indicate that codes with high minimum distance with weight distributions close to the average tend to satisfy RH. It is unknown to what extent the rank-metric weight enumerators behave similarly to their Hamming weight counterparts.

References

[1] I. Blanco-Chacón, E. Byrne, I. M. Duursma, J. Sheekey. *Rank metric codes and zeta functions*. Designs, Codes and Cryptography, 86(8):1767–1792 (2018).

[2] K. Chinen, Y. Imamura. *On the Riemann hypothesis for self-dual weight enumerators of genera three and four*. SUT Journal of Mathematics, 57(1):55–75 (2021).

[3] I. M. Duursma. *From weight enumerators to zeta functions*. Discrete Appl. Math., 111(1-2):55–73 (2001).

[4] I. M. Duursma. *A Riemann hypothesis analogue for self-dual codes*. In Codes and association Schemes, volume 56 of AMS DIMACs Series, 115–124 (2001).

[5] *I. M. Duursma. Combinatorics of the two-variable zeta function*. In Finite fields and applications, volume 2948 of Lecture Notes in Comput. Sci., 109–136. Springer, Berlin (2004).

[6] D. Joyner, J. L. Kim. *The Riemann Hypothesis and Coding Theory*, 71–121. Birkhäuser Boston, Boston, MA (2011).

[7] D. C. Kim, J. Y. Hyun. *A Riemann hypothesis analogue for near-MDS codes*. Disc. Appl. Math., 160(16):2440–2444 (2012).

[8] S. Nishimura. *On a Riemann hypothesis analogue for self-dual weight enumerators of genus less than 3.* Disc. Appl. Math., 156(1):2532–2358 (2008).

School of Mathematics and Statistics, University College Dublin, Ireland
email: ebyrne@ucd.ie

How to design a McEliece like encryption scheme in rank metric ?

Pierre Loidreau

IS

DGA and IRMAR, Université de Rennes, France

Post-Quantum cryptography is a very active actual research field. The standardisation process initiated by the NIST has initiated a second phase with the continuing study of KEM and digital signature proposals. Among all potential cryptographic solutions, the ones basing their security on problems of decoding in rank metric are of promising interest. Such solutions have a better size/security trade-off than the ones based on decoding in Hamming metric.

The so-called unstructured solutions (not implying algebraic properties such as quasi-cyclicity for codes in the security analysis) are of particular interest, since the confidence in the security of structured solutions is not so great. Namely, national agencies such as BSI in Germany and ANSSI in France recommend to use unstructured solutions. In code-based cryptography for reasonable implementation parameters, this leaves essentially McEliece like architecture instantiated with unstructured families of codes. In this talk we see how we can design such systems whose security relies on rank metric problems with a proper security analysis enabling to propose parameters for a given security target. Our talk will be mostly based on [3], [2] and [1].

References

[1] N. Aragon, V. Dyseryn, P. Gaborit, P. Loidreau, J. Renner, A. Wachter-Zeh. *LowMS: a new rank metric code-based KEM without ideal structure*. IACR Cryptol. ePrint Arch., 1596 (2022).

[2] P. Briaud, P. Loidreau. *Cryptanalysis of Rank-Metric Schemes Based on Distorted Gabidulin Codes*. In T. Johansson and D. Smith-Tone, editors, 14th International Workshop, PQCrypto 2023, volume 14154 of LNCS, 38–56 (2023).

[3] P. Loidreau. *A new rank metric codes based encryption scheme*. In PQCrypto 2017, volume 10346 of LNCS, pages 3–17. Springer, 2017.

Batiment 22 IRMAR - Université de Rennes 1, Campus de Beaulieu 35042, Rennes Cedex, France
email: `pierre.loidreau@univ-rennes.fr`

Cutting blocking sets, saturating linear sets and rank-metric codes

Giuseppe Marino

University of Naples Federico II, Italy

IS

Keywords: cutting blocking sets, saturating linear sets, rank-metric codes

Let $\Lambda = \mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$, $q = p^h$, p prime, V a vector space of dimension r over $\mathbb{F}_{q^n}$, and let L be a set of points of Λ. The set L is said to be an $\mathbb{F}_q$-*linear* set of Λ of rank k if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V of dimension k.
An $\mathbb{F}_q$–linear set L_U of Λ of rank k is *scattered* if it has maximum size $q^{k-1} + q^{k-2} + \cdots + q + 1$. Also, in such a case U is said to be a *scattered* subspace. Scattered linear sets have a lot of applications in Galois Geometry, one of which is related to rank-metric codes.
In this talk I will present some constructions of scattered subspaces producing new maximum rank-metric codes ([2]) and shortest minimal rank metric codes ([3]). The last part of the talk will be devoted to shortest saturating linear sets which are related to the covering problem in the rank metric ([1]). Finally, open problems will be discussed.

References

[1] D. Bartoli, M. Borello, G. Marino. *Saturating linear sets of minimal rank*, accepted on Finite Fields and Their Applications, arXiv:2306.17081v2.
[2] D. Bartoli, G. Marino, A. Neri. *New MRD codes from linear cutting blocking sets*. Annali di Matematica Pura ed Applicata 202, 115–142 (2023).
[3] S. Lia, G. Longobardi, G. Marino, R. Trombetti. *Short rank-metric codes and scattered subspaces*, accepted on SIAM Journal on Discrete Mathematics, arXiv:2306.01315.

University of Naples Federico II, Dipartimento di Matematica e Applicazioni "Renato Caccioppoli",
Via Cintia, Monte S. Angelo I-80126 Naples, Italy
email: `giuseppe.marino@unina.it`

Ferrers diagram rank-metric codes

Alessandro Neri

IS

Ghent University, Belgium

(joint work with Mima Stanojkovski)

Ferrers diagram rank-metric codes were first studied in 2009 by Etzion and Silberstein [1], motivated by the application of subspace codes in network coding, and arise from subspace codes entirely contained in a unique Schubert cell. In their work, the authors proposed a conjecture on the largest dimension of a space of matrices over a finite field whose nonzero elements are supported on a given Ferrers diagram and have all rank lower bounded by a fixed positive integer r. Since then, their conjecture has been proved only in some cases, mostly including an assumption on the field size being large enough, or some restriction on the minimum rank r depending on the Ferrers diagram. As of today, this conjecture still remains widely open.

In this talk I will give an overview of the main combinatorial and algebraic properties of Ferrers diagram rank-metric codes and on the state of art on the celebrated Etzion-Silberstein conjecture. Afterwards, I will illustrate a constructive proof of this conjecture for the class of MDS-constructible Ferrers diagrams, which does not depend on the minimum rank r and holds over every finite field. This was obtained in a recent joint work with Mima Stanojkovski [2].

References

[1] T. Etzion, N. Silberstein. *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams.* IEEE Transactions on Information Theory, 55.7:2909–2919 (2009).

[2] A. Neri, M. Stanojkovski. *A proof of the Etzion-Silberstein conjecture for monotone and MDS-constructible Ferrers diagrams.* preprint, (2023) arXiv:2306.16407.

Ghent University, Dept. of math.: analysis, logic and discrete math. Krijgslaan 281, building S8, 9000 Ghent, Belgium

email: `alessandro.neri@ugent.be`

Castelnuovo-Mumford Regularity in the Rank Metric

Valentina Astore **CT**
Università degli Studi di Trento, Italy
(joint work with Martino Borello, Marco Calderini and Flavio Salizzoni)

Keywords: Schur product, Castelnouvo-Mumford regularity, distinguisher

This talk centers on investigating the Castelnuovo-Mumford regularity in the context of linear rank-metric codes and its application to distinguish (generalized) Gabidulin codes from random ones. As mentioned in [3], the Castelnuovo-Mumford regularity is a property of the geometrical object linked to a Hamming code, specifically, the associated projective system. It can be computed by examining the first Schur power of the code for which the dimension stabilizes. In the case of linear rank-metric codes, we can examine the associated q-system and the Schur powers of the associated Hamming code (refer to [1] for the precise definition of these objects).
For codes defined over $\mathbb{F}_{q^m}$, our key observation is that the $(q+1)$-th Schur power marks the onset of distinguishability. This is achieved by generalizing some results from [2] on random codes and by considering the specific case of Gabidulin codes.
The presentation will feature our initial findings, numerous open questions, and the research directions we plan to pursue.

References

[1] G.N. Alfarano, M. Borello, A. Neri, A Ravagnani. *Linear cutting blocking sets and minimal codes in the rank metric*. Journal of Combinatorial Theory, Series A, 192, 105658 (2022).
[2] I. Cascudo, R. Cramer, D. Mirandola, G. Zémor. *Squares of random linear codes*. IEEE Transactions on Information Theory, 61(3), 1159-1173 (2015).
[3] H. Randriambololona. *On products and powers of linear codes under componentwise multiplication*. Contemporary mathematics 637, 3–78 (2015).

Università degli Studi di Trento, Via Sommarive, 14, 38123, Povo (TN)
email: `valentina.astore@studenti.unitn.it`

Algebraic Geometry codes in the sum-rank metric

Elena Berardini **CT**
CNRS; IMB, Université de Bordeaux, France
(joint work with Xavier Caruso)

Algebraic Geometry codes in the Hamming metric allow to overcome the main drawback of Reed–Solomon codes, which is that their length is bounded by the cardinality of the finite field we work on, while benefiting from good parameters. The counterpart of Reed–Solomon codes in the sum-rank metric are linearized Reed–Solomon codes [2]. They have optimal parameters but suffer from the same limitation as Reed–Solomon codes. However, in contrast with the situation of codes in the Hamming metric, no geometric construction has been proposed so far.

In this talk, we will present the first geometric construction of sum-rank metric codes, which we called linearized Algebraic Geometry codes [1]. After introducing some background on codes in the sum-rank metric, we will develop the theory of Riemann–Roch spaces over Ore polynomial rings with coefficients in the function field of a curve, by exploiting the classical theory of divisors and Riemann-Roch spaces on algebraic curves. With this theory at hand, we will study the parameters of linearized Algebraic Geometry codes and give lower bounds for their dimension and minimum distance. Notably, we will show that our new codes exhibit quite good parameters, respecting a similar bound to Goppa's bound for Algebraic Geometry codes in the Hamming metric. Furthermore, our construction yields codes asymptotically better than the sum-rank version of the Gilbert–Varshamov bound.

References

[1] E. Berardini, X. Caruso. *Algebraic Geometry codes in the sum-rank metric*. arXiv preprint arXiv:2303.08903 (2023).

[2] U. Martínez-Peñas. *Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring*. Journal of Algebra 504, 587–612 (2018).

CNRS; IMB, Université de Bordeaux, 351, cours de la Libération, F 33 405 Talence, France
email: `elena.berardini@math.u-bordeaux.fr`

How (not) to decode in the rank metric

Hugo Sauerbier Couvée **CT**

Technical University of Munich, Germany

(joint work with Alberto Ravagnani, Antonia Wachter-Zeh and Violetta Weger)

Keywords: code-based cryptography, generic syndrome decoding, rank metric

Not only do rank-metric codes have an interesting mathematical theory, they also find important applications such as cryptography. Currently, the main challenge therein is the design of quantum-secure cryptosystems, where systems based on rank-metric codes are some of the major contenders for a new future standard. Although they promise superior performance to Hamming-based systems, the largest obstacle for being standardized is insufficient research on their security. The focus of this talk will therefore be the complexity of the Rank Syndrome Decoding Problem (RSDP), which many systems are based on.

In the Hamming metric, the syndrome decoding problem has been well investigated since Prange's algorithm in 1962. Since then, several improvements were made using diverse techniques, with the most important idea being to split a vector into vectors of smaller weight. For the rank metric, the fastest combinatorial algorithm solving the RSDP is analogous to Prange's algorithm, but improvements following similar ideas from the Hamming metric have not been found yet.

In this talk we will investigate connections between the rank metric and the Hamming metric, reduce decoding to an open problem in extremal combinatorics concerning anticodes, and introduce an adaptive framework that allows room for new improvements using geometrical tools.

Technical University of Munich, Chair of Coding and Cryptography, Theresienstrasse 90, 80333 Munich, Germany

email: `hugo.sauerbier-couvee@tum.de`

On 3-dimensional MRD codes

Francesco Ghiandoni **CT**
University of Florence - University of Perugia - INdAM, Italy
(joint work with Daniele Bartoli)

Keywords: Scattered polynomials, linearized polynomials, MRD codes, finite fields

In this talk I will present recent results on the classification of $\mathbb{F}_{q^n}$-linear MRD codes of dimension three. In particular, I will provide non-existence results for MRD codes $\mathcal{C} = \langle x^{q^t}, F(x), G(x)\rangle \subseteq \mathcal{L}_{n,q}$ of exceptional type, i.e. such that $\mathcal{C}$ is MRD over infinite many extensions of the field $\mathbb{F}_{q^n}$. These results partially address a conjecture in [1].

References

[1] D. Bartoli, G. Zini, F. Zullo. Linear Maximum Rank Distance Codes of Exceptional Type *IEEE Tran. Inf. Theory* 69(6), 3627–3636 (2023).

University of Perugia, Department of Mathematics and Informatics, via Vanvitelli 1, 06123 Perugia
email: `francesco.ghiandoni@unifi.it`

Exceptional and indecomposable scattered sequences of order $m > 2$

Alessandro Giannoni **CT**
University of Naples Federico II, Italy
(joint work with Daniele Bartoli and Giuseppe Marino)

Keywords: Scattered linear sets, Scattered sequences, Evasive subspaces, MRD codes

Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$. If the $\mathbb{F}_q$-subspace $U = \{(x, f(x)|\ x \in \mathbb{F}_{q^n}\}$ defines a scattered linear set, then we call f a scattered polynomial. Scattered sequences are a generalization of scattered polynomials and can be seen as the geometrical counterparts of exceptional MRD codes. The order of a scattered sequence denotes the number of variables of its polynomials. The aim of this talk is to present the first infinite family of indecomposable and exceptional scattered sequences of any order greater than two. The MRD codes associated to these sequences are also minimal.

University of Naples Federico II, Dipartimento di Matematica e Applicazioni "Renato Caccioppoli",
Via Cintia, Monte S. Angelo I-80126 Napoli, Italy
email: `giannonialessandro22@gmail.com`

Non-linear MRD codes from cones over exterior sets

Giovanni Giuseppe Grimaldi **CT**
University of Naples Federico II, Italy
(joint work with Nicola Durante and Giovanni Longobardi)

Keywords: finite projective space, C_F^s-set, linear set, rank metric code, MRD-code

In the finite projective space $\mathrm{PG}(n-1,q^n)$, let $\mathcal{X}$ be a C_F^s-set of an $(n-k+1)$-dimensional subspace Λ with vertices A and B and $\Lambda^\star$ be a $(k-3)$-dimensional subspace skew with Λ. In [1], it is shown that $\mathcal{X}$ is a union of $\{A,B\}$ and $q-1$ pairwise disjoint scattered $\mathbb{F}_q$-linear sets of rank n, say $\mathcal{X}_a$ for any $a \in \mathbb{F}_q^*$. Moreover, the line AB can be partitioned in $\{A,B\}$ and $q-1$ scattered $\mathbb{F}_q$-linear sets of rank n, say J_a for any $a \in \mathbb{F}_q^*$. Denote by $\mathcal{K}(\Lambda^\star,\mathcal{E})$ the cone with vertex $\Lambda^\star$ and base the set

$$\mathcal{E} = (\mathcal{X} \setminus \bigcup_{a\in T} \mathcal{X}_a) \cup \bigcup_{a\in T} J_a,$$

with $1 \in T \subset \mathbb{F}_q^*$. Then $\mathcal{K}(\Lambda^\star,\mathcal{E})$ gives rise to a new family of non-linear $(n,n,q;d)$-MRD codes for any $n \geq 3$, $2 \leq d \leq n-1$ and $d = n-k+1$. This new class of codes contains properly those constructed by Donati and Durante [1], and any its element is not equivalent to non-linear MRD codes constructed by Otal and Özbudak in [2].

References

[1] G. Donati, N. Durante. *A generalization of the normal rational curve in* $\mathrm{PG}(d,q^n)$ *and its associated non-linear MRD codes*. Des. Codes Cryptogr. 86, 1175–1184 (2018).
[2] K. Otal, F. Özbudak. *Some new non-additive maximum rank distance codes*. Finite Fields and Their Applications 50, 293–303 (2018).

University of Naples Federico II, Dipartimento di Matematica e Applicazioni "Renato Caccioppoli",
Via Cintia, Monte S. Angelo, I-80126 Napoli, Italy
email: `giovannigiuseppe.grimaldi@unina.it`

Eigenvalue bounds for sum-rank-metric codes

Antonina P. Khramova **CT**

Eindhoven University of Technology, Netherlands

(joint work with Aida Abiad and Alberto Ravagnani)

Keywords: sum-rank-metric code, spectral graph theory, MSRD code

We consider the problem of deriving upper bounds on the parameters of sum-rank-metric codes, with a focus on their dimension and block length. The sum-rank metric is a combination of the Hamming and the rank metric, and most of the available techniques to investigate it seem to be unable to fully capture its hybrid nature.

In this paper, we introduce a new approach based on sum-rank-metric graphs, in which the vertices are tuples of matrices over a finite field, and where two such tuples are connected when their sum-rank distance is equal to one. We establish various structural properties of sum-rank-metric graphs, revealing the connection to rank-metric graphs, and combine them with eigenvalue techniques to obtain bounds on the cardinality of sum-rank-metric codes. The bounds we derive improve on the best known bounds for several choices of the parameters. The bounds are explicit for small values of minimum distance ($d = 3, 4$), and for larger values can be calculated using LP methods.

The spectral graph theory methods also allow us to establish new non-existence results for (possibly nonlinear) MSRD codes. The talk is based on joint work with Aida Abiad and Alberto Ravagnani.

Eindhoven University of Technology, Departament of Mathematics and Computer Science
Groene Loper, 3, 5612 AE Eindhoven
email: `a.khramova@tue.nl`

Decoding rank metric Reed-Muller codes

Rakhi Pratihar **CT**
Inria Saclay Centre, France
(joint work with Alain Couvreur)

For an arbitrary Galois extension fields $\mathbb{L}$ over $\mathbb{K}$ with Galois group G, a rank metric code can be seen as $\mathbb{L}$-subspace of the twisted group algebra $\mathbb{L}[G]$, or $\mathbb{K}$-subspace of $\mathbb{L}[G] \cong \mathbb{K}^{N\times N}$ where $|G| = N$. In 2021, Augot et al. [1] defined a rank analogue of Reed-Muller codes in the context of finite Galois extension fields. This class of codes is a multivariate version of the Gabidulin codes, which are defined for cyclic Galois extensions. In this talk, I present two different ways to decode these codes; one using G-Dickson matrices and the other by a rank analogue of Plotkin-type construction for binary Reed-Muller codes. Both of these methods improve the error correcting capacity obtained in the previously known decoding method using rank error-correcting pairs [2]. This is based on an ongoing work with Alain Couvreur.

References

[1] D. Augot, A. Couvreur, J. Lavauzelle, A. Neri, *Rank metric codes over arbitrary Galois extensions and rank analogues of Reed-Muller codes*, SIAM journal of applied algebra and geometry 5(2) (2021).
[2] U. Martínez-Peñas, R. Pellikaan, *Rank error-correcting pairs*, Designs Codes, and Cryptography 84 (2017).

Inria Saclay Centre, 1 rue Honoré d'Estienne d'Orves, Bâtiment Alan Turing, Campus de l'École polytechnique, 91120 Palaiseau, France
email: `rakhi.pratihar@inria.fr, pratihar.rakhi@gmail.com`

A geometric characterization of known maximum scattered linear sets of $\mathrm{PG}(1, q^n)$

Somi Gupta **CT**
University of Naples Federico II, Italy
(joint work with Giovanni Giuseppe Grimaldi, Giovanni Longobardi and Rocco Trombetti)

Keywords: linearized polynomial, finite projective space, linear set.

Let n, t, r be positive integers such that $rn > t > r \geq 2$, and $V = \mathbb{F}_{q^n}^r$ be an r-dimensional vector space over $\mathbb{F}_{q^n}$; also, let $\mathrm{PG}(V, q^n) = \mathrm{PG}(r-1, q^n)$ be the underlying projective space. A subset of $\mathrm{PG}(r-1, q^n)$ is called a *linear set* L_U if its points are defined by non-zero elements of an $\mathbb{F}_q$-subspaces U of V. More precisely,

$$L_U = \{\langle u \rangle_{\mathbb{F}_{q^n}} : u \in U \setminus \{0\}\}.$$

If dim$_{\mathbb{F}_q}(U) = t$, then we say that L_U is a linear set of *rank* t.
In [2], Lunardon and Polverino showed that every linear set of rank t of $\mathrm{PG}(V, q^n)$ can be obtained as the projection of a canonical subgeometry $\Sigma \simeq \mathrm{PG}(t-1, q)$ of $\Sigma^* = \mathrm{PG}(t-1, q^n) \supset \mathrm{PG}(V, q^n)$ from a suitable subspace Γ of $\mathrm{PG}(t-1, q^n)$ such that $\Gamma \cap \Sigma = \emptyset$, onto $\mathrm{PG}(V, q^n)$. This subspace Γ is also called the *vertex* of the projection.
In this talk I will show a method to reconstruct, up to the action of the set-wise stabilizer of Σ in $\mathrm{PG}(t-1, q^n)$, the vertex Γ for a peculiar class of linear set of rank $t = n(r-1)$ in $\mathrm{PG}(r-1, q^n)$ called *evasive* linear sets, from $r-1$ imaginary points of $\mathrm{PG}(t-1, q^n)$ and their conjugates with respect to a collineation of $\mathrm{PG}(t-1, q^n)$ fixing pointwise the chosen subgeometry Σ.
Following the spirit of the work done by Csajbok and Zanella in [1] and later by Zanella and Zullo in [3], we also will focus on the case $r = 2$, and will exploit above mentioned results to characterize infinite families of linear sets of the projective line $\mathrm{PG}(1, q^n)$ introduced from 2018 onwards, through some properties of their projection vertices.

References

[1] B. Csajbók, C. Zanella. *On scattered linear sets of pseudoregulus type in* $\mathrm{PG}(1, q^t)$, Finite Fields Appl. 41, 34–54 (2016).
[2] G. Lunardon, O. Polverino. *Translation ovoids of orthogonal polar spaces*. Forum Math. 16, 663–669 (2004).
[3] C. Zanella, F. Zullo. *Vertex properties of maximum scattered linear sets of* $\mathrm{PG}(1, q^n)$. Discrete Mathematics 343(5) (2020).

University of Naples Federico II, Dipartimento di Matematica e Applicazioni "Renato Caccioppoli",
Via Cintia, Monte S. Angelo, I-80126 Napoli, Italy
email: `somi.gupta@unina.it`

(Near) Constant-Rank Codes and (A)PN functions

Valentin Suder

University of Rouen, France

CT

Keywords: PN/APN functions, constant-rank codes, MRD codes, DO-polynomials

In this talk, we will discuss PN and APN-ness of quadratic functions over finite fields from a rank-metric codes' perspective.

It is well understood that rank-metric codes, and in particular so called MRD codes, are in fact highly structured algebraic and geometric objects (e.g. presemifields [2]). These algebraic objects similarly coincide with the concept of Dembowski-Ostrom (DO) polynomials (i.e. homogeneous quadratic) that are Perfectly Nonlinear (PN) [1]. Although both of these links benefit from an extensive literature and research effort, it seems quite surprising that the direct relationship between rank-metric codes and quadratic functions falls into a blind spot.

On the other hand, the search for quadratic APN functions is of the utmost importance in symmetric cryptography on both practical and theoretic grounds.

In even characteristic, techniques based on the modification of the so-called Quadratic APN Matrices (QAM) [3,4] have led to finding a large number of new (i.e. inequivalent) quadratic APN functions. It appears that each of these QAM forms two distinct but interlaced rank-metric codes. The first of this code is constant-rank (i.e. have a 1-valued weight distribution) while the other has either a 1 or a 2-valued weight distribution depending on their length. These codes, their relationships and their generalisations (e.g. to odd characteristics) are the focus of our study.

References

[1] R.S. Coulter and M. Henderson. *Commutative presemifields and semifields*, Adv. Math. 217, 282-304 (2008).

[2] J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems. *Algebraic structures of MRD codes*, Adv. Math. Commun. 10, 499–510 (2016).

[3] Guobiao Weng, Yin Tan, Guang Gong. *On quadratic almost perfect nonlinear functions and their related algebraic object*, Workshop on Coding and Cryptography, WCC 2013.

[4] Yuyin Yu, Mingsheng Wang, Yongqiang Li. *A matrix approach for constructing quadratic APN functions* Workshop on Coding and Cryptography, WCC 2013.

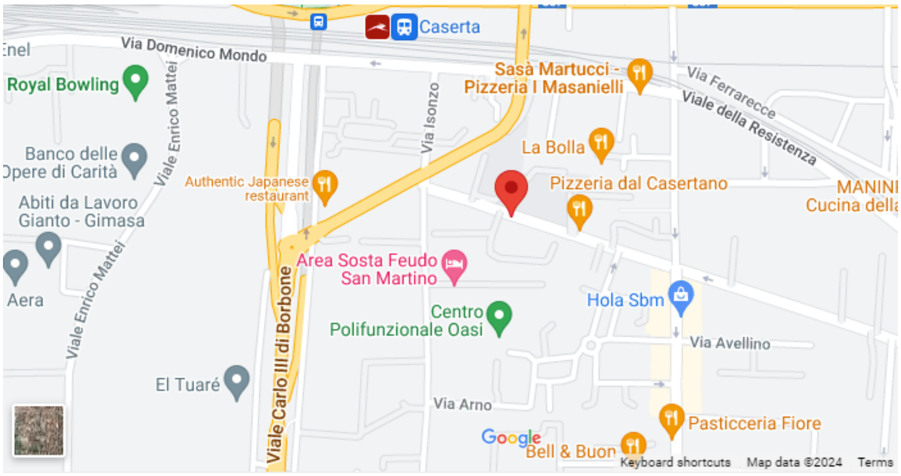
Univ Rouen Normandie, LITIS UR 4108, F-76000 Rouen, France
email: `valentin.suder@univ-rouen.fr`

List of Participants

Abiad, Aida	Eindhoven University of Technology
Alfarano, Gianira Nicoletta	Vrije Universiteit Brussel University College Dublin
Astore, Valentina	University of Trento
Bardet, Magali	University of Rouen Normandy
Bartoli, Daniele	University of Perugia
Berardini, Elena	CNRS; University of Bordeaux
Borello, Martino	University Paris 8 - LAGA
Broby, Daniel	Ulster University
Byrne, Eimear	University College Dublin
Castello, Chiara	University of Campania "Luigi Vanvitelli"
Degen, Sebastian	University of Bielefeld
Dionigi, Arianna	University of Perugia
Durante, Nicola	University of Naples Federico II
Franch, Ermes	University of Bergen
Ghiandoni, Francesco	University of Perugia
Giannoni, Alessandro	University of Perugia
Grimaldi, Giovanni Giuseppe	University of Naples Federico II
Gruica, Anina	Eindhoven University of Technology
Gupta, Somi	University of Naples Federico II
Jany, Benjamin	Eindhoven University of Technology
Khramova, Antonina	Eindhoven University of Technology
Li, Chunlei	University of Bergen
Longobardi, Giovanni	University of Naples Federico II
Loidreau, Pierre	University of Rennes 1 and DGA
Marino, Giuseppe	University of Naples Federico II
Mazzocca, Francesco	University of Campania "Luigi Vanvitelli"
Musharraf, Usman	University of Campania "Luigi Vanvitelli"
Napolitano, Vito	University of Campania "Luigi Vanvitelli"
Neri, Alessandro	Ghent University
Polverino, Olga	University of Campania "Luigi Vanvitelli"
Pratihar, Rakhi	Inria Saclay Centre
Santonastaso, Paolo	University of Campania "Luigi Vanvitelli"
Sauerbier Couvée, Hugo	Technical University of Munich
Scotti, Martin	University Paris 8 - LAGA
Suder, Valentin	University of Rouen Normandy
Toesca, Beatrice	University of Zurich
Trombetti, Rocco	University of Naples Federico II
Weger, Violetta	Technical University of Munich Eindhoven University of Technology
Zappatore, Ilaria	University of Limoges
Zini, Giovanni	University of Modena and Reggio Emilia
Zullo, Ferdinando	University of Campania "Luigi Vanvitelli"

Useful Information

Talks will take place at the **Department of Mathematics** & **Physics** of **University of Campania "Luigi Vanvitelli"** in the **Room A**.



Recommended Accommodations in Caserta: Suggested hotels and B& B's located in the city center, within walking distance from the railway station: Villa Maria Cristina, Royal Hotel, Hotel dei Cavalieri, B&B Il Cavaliere, Roof Garden House [Before booking, contact Ferdinando Zullo at `ferdinando.zullo@unicampania.it`].

Please note that Caserta attracts approximately one million visitors each year. Due to limited room availability, we strongly recommend making your reservation as early as possible to ensure the best choice of available hotels.

For those interested in very affordable rooms near the Reggia, you have the opportunity to explore options at SNA Caserta. For more information, please contact Paolo Santonastaso at `paolo.santonastaso@unicampania.it`.

How to Reach Caserta

If you are planning the trip to Caserta and are looking for the best way to reach the city, here are some options to consider

by Plane: If you are arriving from other cities or countries, the most convenient way to reach Caserta is through Naples' Capodichino International Airport. From here, you have several options to continue your journey to Caserta. Another option is to fly to Rome, from where you can either take direct trains to Caserta or make a transfer in Naples.

by Bus: From Capodichino Airport, there is a shuttle service available that will take you directly to Caserta. Be sure to check the shuttle schedules to plan your trip accordingly.

By Train: A convenient and fast option to reach Caserta is by taking the train from Naples, specifically from Piazza Garibaldi Station. However, please note that Piazza Garibaldi Station is not directly connected to Capodichino Airport. You can use a shuttle service that connects the airport to the train station. Trains to Caserta are frequent, and the journey takes about 40 minutes.

We hope this information helps you plan your trip to Caserta. Safe travels!