Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *"Computer Algebra for Geometry and Combinatorics"*

How do we construct new maximum rank distance codes?

Ferdinando Zullo[1] [ferdinando.zullo@unicampania.it]

[1] Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Caserta, Italy

The set $\mathbb{F}_q^{m\times n}$ of $m \times n$ matrices over $\mathbb{F}_q$ is a metric space with rank metric distance defined by $d(A, B) = \mathrm{rk}(A - B)$ for $A, B \in \mathbb{F}_q^{m\times n}$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is called *rank metric code*.

These codes were introduced independently by Delsarte [3] and Gabidulin [4]. They also proved a Singleton-like bound for these codes which involves the parameters of the code. If this bound is achieved, then $\mathcal{C}$ is called a *maximum rank distance code*, or shortly *MRD-code*. Such codes have received great attention in recent years for their applications in cryptography and coding theory.

For many years only few different new constructions of MRD codes have been discussed. In 2016 twisted Gabidulin codes have been introduced by Sheekey, and then generalized by Lunardon, Trombetti and Zhou. Remarkably, in his paper Sheekey pointed out a connection between 2-dimensional $\mathbb{F}_{q^n}$-linear MRD codes and scattered linear sets of maximum rank in $\mathrm{PG}(1, q^n)$.

In this talk we will consider 2-dimensional $\mathbb{F}_{q^n}$-linear MRD codes and we will see how *Computer Algebra* plays an important role in this area, such as it can be used

- to find first some examples of MRD codes for fixed values of the parameters;
- to prove that certain rank metric codes are MRD codes.

This is based on the papers [1,2,5,6,7].

Keywords
Rank metric code, Linear set, MRD code

References

[1] D. BARTOLI, C. ZANELLA AND F. ZULLO, A new family of maximum scattered linear sets in $\mathrm{PG}(1, q^6)$. *Ars Mathematica Contemporanea* **19**(1), 125–145 (2020).
[2] B. CSAJBÓK, G. MARINO AND F. ZULLO, New maximum scattered linear sets of the

projective line. *Finite Fields and Their Applications* **54**, 133–150 (2018).
[3] P. DELSARTE, Bilinear forms over a finite field, with applications to coding theory. *Journal Combinatoria Theory Series A* **25**(3), 226-241 (1978).
[4] E. GABIDULIN, Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii* **21**(1), 3–16 (1985).
[5] G. MARINO, M. MONTANUCCI AND F. ZULLO, MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$. *Linear Algebra and its Applications* **591**, 99–114 (2020).
[6] A. NERI, P. SANTONASTASO AND F. ZULLO, Extending two families of maximum rank distance codes. *arxiv preprint*.
[7] C. ZANELLA AND F. ZULLO, Vertex properties of maximum scattered linear sets of PG$(1, q^n)$. *Discrete Mathematics* **343**(5), 111800 (2020).