Abstract

The geometric counterpart of maximum rank metric codes

Ferdinando Zullo

Dipartimento di Matematica e Fisica
Università degli Studi della Campania "Luigi Vanvitelli", Italy

The set of $m \times n$ matrices $\mathbb{F}_q^{m\times n}$ 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*. The *minimum distance* of $\mathcal{C}$ is defined as

$$d(C) = \min_{A,B\in\mathcal{C},\ A\neq B}\{d(A,B)\}.$$

When $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m\times n}$, we say that $\mathcal{C}$ is an $\mathbb{F}_q$-*linear rank metric code* and the *dimension* $\dim_q(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$.

The Singleton bound for an $m\times n$ rank metric code $\mathcal{C}$ with minimum rank distance d, proved by P. Delsarte in [3] and by E. Gabidulin in [4], is

$$\#\mathcal{C} \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}.$$

If this bound is achieved, then $\mathcal{C}$ is called an *MRD-code*. Such codes have received great attention in recent years for their applications in cryptography and coding theory.

J. Sheekey in [6] opened a new perspective in the theory of MRD-codes: he proved that scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1,q^n)$ of maximum rank n yield $\mathbb{F}_q$–linear MRD-codes with dimension $2n$ and minimum distance $n-1$.

More generally, a linear set can be defined as follows. Let $V = V(r,q^n)$, $\Lambda = \mathrm{PG}(V,\mathbb{F}_{q^n}) = \mathrm{PG}(r-1,q^n)$, $q=p^h$ for some prime p. A pointset L of Λ is an $\mathbb{F}_q$-*linear set* of Λ of rank k if L consists of the points defined by the vectors of an $\mathbb{F}_q$-subspace U of V of dimension k, i.e.

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

For the number of points of an $\mathbb{F}_q$-linear set of rank k the following bound holds

$$|L_U| \leq \frac{q^k-1}{q-1},$$

and the $\mathbb{F}_q$-linear sets achieving this bound are called *scattered*, see [1]. Equivalently, it is possible to define scattered linear sets through the definition of the weight of a point. Let $\Omega = \mathrm{PG}(W,\mathbb{F}_{q^n})$ be a subspace of Λ and let L_U be an $\mathbb{F}_q$-linear set of Λ, then if $\dim_{\mathbb{F}_q}(W\cap U) = i$, we say that Ω has *weight* i in L_U, and we write $w_{L_U}(\Lambda) = i$. Hence, a scattered $\mathbb{F}_q$-linear set can be defined as an $\mathbb{F}_q$-linear set with the property that all of its points have weight one. In [2] the scattered property has been generalized by replacing points with subspaces of fixed dimension. More precisely, the $\mathbb{F}_q$-linear sets of Λ with the property that

$$w_{L_U}(\Omega) \leq h$$

for each $(h-1)$-subspace Ω of Λ and $\langle L_U\rangle_{\mathbb{F}_{q^n}} = \Lambda$ are called *h-scattered $\mathbb{F}_q$-linear sets*. It turns out that h-scattered $\mathbb{F}_q$-linear sets are scattered linear sets. Also, 1-scattered $\mathbb{F}_q$-linear sets coincide with the classical scattered linear sets generating the whole space defined above. The case $h = r - 1$ was also considered in [5, 7]. In [2] it was proved that for any h the rank of a h-scattered $\mathbb{F}_q$-linear set is bounded by $rn/(h+1)$ and examples of h-scattered linear sets whose rank attain this bound were given.

In this talk we will give a gentle introduction to the theory of h-scattered linear sets and we will deal with their connection with MRD-codes, extending the connection established in [6].

Joint work with Bence Csajbók, Giuseppe Marino, Vito Napolitano, Olga Polverino and Giovanni Zini.

References

[1] A. Blokhuis and M. Lavrauw: Scattered spaces with respect to a spread in $\mathrm{PG}(n, q)$, *Geom. Dedicata* **81** (2000), 231–243.

[2] B. Csajbók, G. Marino, O. Polverino and F. Zullo: Generalising the scattered property of subspaces, *Combinatorica* **41(2)** (2021): 237–262.

[3] P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.

[4] E. Gabidulin: Theory of codes with maximum rank distance, *Problems Inform. Transmission*, **21(3)** (1985), 3–16.

[5] G. Lunardon: MRD-codes and linear sets, *J. Combin. Theory Ser. A* **149** (2017), 1–20.

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

[7] J. Sheekey and G. Van de Voorde: Rank-metric codes, linear sets and their duality, *Des. Codes Cryptogr.* **88** (2020), 655-675.