Contemporary algebraic and geometric techniques
in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

The Geometry of Minimal Codes

Gianira N. Alfarano

University of Zurich
Switzerland

Abstract

This talk deals with the geometric description of some special classes of codes endowed with the Hamming and the rank metric, namely *minimal codes*.

Let $\mathbb{F}_q$ be the finite field with q element and let k,n two positive integers. The **Hamming support** of a vector $v \in \mathbb{F}_q^n$ is $\sigma_{\mathrm{H}}(v) = \{i \mid v_i \neq 0\} \subseteq [n]$ and its **Hamming weight** is $\mathrm{wt}_{\mathrm{H}}(v) = |\sigma_{\mathrm{H}}(v)|$. An $[n,k]_q$ **code** is a nonzero $\mathbb{F}_q$-linear subspace $\mathscr{C} \subseteq \mathbb{F}_q^n$ of dimension k. Its elements are called **codewords**. The **minimum distance** of $\mathscr{C}$ is the integer $d(\mathscr{C}) = \min\{\mathrm{wt}_{\mathrm{H}}(c) \mid c \in \mathscr{C}, c \neq 0\}$ and its **maximum weight** is $\max\{\mathrm{wt}_{\mathrm{H}}(c) \mid c \in \mathscr{C}\}$. If $d = d(\mathscr{C})$ is known, we say that $\mathscr{C}$ is an $[n,k,d]_q$ code. A **generator matrix** $G \in \mathbb{F}_q^{k\times n}$ of $\mathscr{C}$ is a matrix such that $\mathrm{rowsp}(G) = \mathscr{C}$. Finally, codes $\mathscr{C}$ and $\mathscr{C}'$ are called (**monomially**) **equivalent** if there exists an $\mathbb{F}_q$-linear isometry $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $f(\mathscr{C}) = \mathscr{C}'$. Recall that an $[n,k]_q$ code $\mathscr{C}$ is **nondegenerate** if there is no $i \in [n]$ with $c_i = 0$ for all $c \in \mathscr{C}$.

Nondegenerate codes in the Hamming metric have a well-known geometric description; see also [4].

Definition. A **projective** $[n,k,d]_q$ **system** $\mathscr{P}$ is a finite set of n points (counted with multiplicity) of $\mathrm{PG}(k-1,q)$ that do not all lie on a hyperplane and such that

$$d = n - \max\{|H \cap \mathscr{P}| : H \subseteq \mathrm{PG}(k-1,q),\ \dim(H) = k-2\}.$$

Projective $[n,k,d]_q$ systems $\mathscr{P}$ and $\mathscr{P}'$ are **equivalent** if there exists $\phi \in \mathrm{PGL}(k-1,q)$ mapping $\mathscr{P}$ to $\mathscr{P}'$ which preserves the multiplicities of the points.

Theorem. There is a correspondence between the (monomial) equivalence classes of nondegenerate $[n,k,d]_q$ linear codes and the equivalence classes of projective $[n,k,d]_q$ systems.

The Hamming distance is not the only metric that is used in coding theory. In this talk, we are interested also in the rank metric, which is the one induced by the rank weight. In order to define it, we need to fix n and m positive integers.

For a vector $v \in \mathbb{F}_{q^m}^n$ and an ordered basis $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ of the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$, let $\Gamma(v) \in \mathbb{F}_q^{n\times m}$ be the matrix defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij}\gamma_j.$$

Note that $\Gamma(v)$ is constructed by simply transposing v and then expanding each entry over the basis Γ. The **support** of a vector $v \in \mathbb{F}_{q^m}^n$ is the column space of $\Gamma(v)$. It is denoted by $\sigma_\Gamma(v) \subseteq \mathbb{F}_q^n$.

In the sequel, for $v \in \mathbb{F}_{q^m}^n$ we let $\sigma^{\mathrm{rk}}(v) := \sigma_\Gamma(v)$ be the **rank support** of v, where Γ is *any* basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$. The support is well-defined and does not depend on the choice of basis Γ. The **rank** (**weight**) of a vector v is the $\mathbb{F}_q$-dimension of its support, denoted by $\mathrm{rk}(v)$.

Rank-metric codes and their fundamental parameters are defined as follows.

A **rank-metric code** is an $\mathbb{F}_{q^m}$-linear subspace $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$. Its elements are called **codewords**. The integer n is the **length** of the code. The **dimension** of $\mathscr{C}$ is the dimension as an $\mathbb{F}_{q^m}$-vector space and the **minimum rank distance** of a nonzero code $\mathscr{C}$ is

$$d^{\mathrm{rk}}(\mathscr{C}) := \min\{\mathrm{rk}(v) : v \in \mathscr{C}, v \neq 0\}.$$

We also define the minimum distance of the zero code to be $n+1$. We say that $\mathscr{C}$ is an $[n,k,d]_{q^m/q}$ code if it has length n, dimension k and minimum distance d. When the minimum distance is not known or is irrelevant, we write $[n,k]_{q^m/q}$. A **generator matrix** of an $[n,k]_{q^m/q}$ code is a matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ whose rows generate $\mathscr{C}$ as an $\mathbb{F}_{q^m}$-linear space. If the columns of G are linear independent over $\mathbb{F}_q$, then the code is said **nondegenerate**.

A (**linear**, **rank-metric**) **isometry** of $\mathbb{F}_{q^m}^n$ is an $\mathbb{F}_{q^m}$-linear automorphism φ of $\mathbb{F}_{q^m}^n$ that preserves the rank weight, i.e., such that $\mathrm{rk}(v) = \mathrm{rk}(\varphi(v))$ for all $v \in \mathbb{F}_{q^m}^n$. It is known that the isometry group of $\mathbb{F}_{q^m}^n$, say $\mathscr{G}(q,m,n)$, is generated by the (nonzero) scalar multiplications of $\mathbb{F}_{q^m}$ and the linear group $\mathrm{GL}_n(q)$. More precisely, $\mathscr{G}(q,m,n) \cong \mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)$, which (right-)acts on $\mathbb{F}_{q^m}^n$ via

$$\begin{array}{rcl} (\mathbb{F}_{q^m}^* \times \mathrm{GL}_n(q)) \times \mathbb{F}_{q^m}^n & \longrightarrow & \mathbb{F}_{q^m}^n \\ ((\alpha, A), v) & \longmapsto & \alpha v A. \end{array}$$

As their Hamming-metric counterpart, also nondegenerate rank-metric codes have a geometric interpratation.

Definition. An $[n,k,d]_{q^m/q}$ **system** is an n-dimensional $\mathbb{F}_q$-space $U \subseteq \mathbb{F}_{q^m}^k$ with the properties that $\langle U \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$ and

$$d = n - \max\left\{\dim_{\mathbb{F}_q}(U \cap H) : H \text{ is an } \mathbb{F}_{q^m}\text{-hyperplane of } \mathbb{F}_{q^m}^k\right\}. \qquad (1)$$

When the parameters are not relevant, we simply call such an object a q-**system**.

Theorem. There is a 1-to-1 correspondence between equivalence classes of nondegenerate $[n,k,d]_{q^m/q}$ rank-metric codes and equivalence classes of $[n,k,d]_{q^m/q}$ systems.

The geometric interpretation of codes in the Hamming and rank metric gives one of the most fascinating applications in the theory of minimal codes. A code is minimal if all its codewords are **minimal**, i.e. their (rank or Hamming) support does not contain the support of any other linear independent codeword. The study of the minimal codewords of a linear code finds application in combinatorics, in the analysis of the Voronoi region for decoding purposes and in secret sharing schemes.

The aim of the talk is to explain the correspondence between nondegenerate minimal codes in the Hamming metric and *strong blocking sets* and the one between nondegenerate minimal codes in the rank metric and *linear cutting blocking sets*. While strong blocking sets have been studied in the past years also in relation to codes, linear cutting blocking sets have been introduced only recently in [3].

Cutting blocking sets are defined as follows.

Definition. Let r,N be positive integers with $r < N$. An r-blocking set $\mathscr{M}$ in $\mathrm{PG}(N,q)$ is **strong** if for every pair of $(N-r)$-flats Λ,Λ' of $\mathrm{PG}(N,q)$ we have

$$\mathscr{M} \cap \Lambda \subseteq \mathscr{M} \cap \Lambda' \iff \Lambda = \Lambda'.$$

Equivalently, an r-blocking set $\mathscr{M} \subseteq \mathrm{PG}(N,q)$ is strong if and only if for every $(N-r)$-dimensional subspace Λ of $\mathrm{PG}(N,q)$ we have $\langle \mathscr{M} \cap \Lambda \rangle = \Lambda$.

The correspondence described above between projective $[n,k,d]_q$ systems and nondegenerate $[n,k,d]_q$ linear codes extends to a correspondence between equivalence classes of $[n,k,d]_q$ minimal codes and equivalence classes of projective $[n,k,d]_q$ systems that are strong blocking sets.

In the rank metric case, the q-analogue of strong blocking set is given by *linear cutting blocking sets*, which are formally defined as follows.

Definition. A $[n,k]_{q^m/q}$ system U is called a **linear cutting blocking set** if for every $\mathbb{F}_{q^m}$-hyperplane H we have $\langle H \cap U \rangle_{\mathbb{F}_{q^m}} = H$.

Also in this case, we will show that the correspondence between nondegenerate rank-metric codes and q-systems extends to a correspondence between nondegenerate equivalence classes of minimal rank-metric codes and equivalence classes of linear cutting blocking sets.

The description of minimal rank-metric codes via the q-analogues of strong blocking sets allows us to establish a lower bound for their length. More precisely, we find that a minimal rank-metric code $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k must satisfy

$$n \geq k + m - 1. \tag{2}$$

We also show that a nondegenerate rank-metric code is minimal if and only if the associated Hamming-metric code is minimal (under the correspondence described earlier). This result naturally connects the theories of minimal codes in the two metrics and makes it possible to transfer/compare results across them.

A major, rather curious difference between minimal codes in the rank and in the Hamming metric appears to be in the role played by the field size q with respect to bounds and existence results. While in the Hamming metric the field size q is a crucial parameter (e.g., minimal codes do not exist for lengths that are too small compared to a suitable multiple of the field size), most of the bounds and existence results we can derive for minimal rank-metric codes do not depend on q, even when this quantity explicitly shows up in the computations.

References

[1] G. N. Alfarano, M. Borello, A. Neri. *A geometric characterization of minimal codes and their asymptotic performance.* Advances in Mathematics of Communications, 16.1 (2022).

[2] G. N. Alfarano, M. Borello, A. Neri, A. Ravagnani. *Three Combinatorial Perspectives on Minimal Codes* SIAM Journal on Discrete Mathematics, 36.1 (2022): 461-489.

[3] 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, 2022.

[4] M. A. Tsfasman and S. G. Vladut. *Algebraic-geometric codes*, volume 58 of Mathematics and its Applications (Soviet Series). Kluwer Academic Publishers Group, Dordrecht, 1991

Keywords: q-systems, rank-metric codes, minimal codes, linear cutting blocking sets