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

The Etzion-Silberstein Conjecture over Large Fields

Anina Gruica

Affiliation: Eindhoven University of Technology
The Netherlands

Abstract

In 2000 it was discovered that using coding theory strategies at the intermediate nodes of a network gives substantial gains in information throughput. With this discovery the field of *network coding* was born, which deals with the efficiency and reliability of transmission of information over networks. Not long after, network coding started to attract the interest of the mathematics' community, when in 2008 Kötter and Kschischang proposed rank-metric and subspace codes as a solution to the problem of error amplification in networks. Ever since, rank-metric and subspace codes have been a thriving research topic.

The main objects of interest in this abstract are matrix spaces endowed with the rank distance. More concretely, in the sequel we let m and n be integers with $m \geq n \geq 2$, we let q be a prime power and we denote by $\mathbb{F}_q$ the finite field of q elements. A (**linear rank-metric**) **code** is a nonzero $\mathbb{F}_q$-linear subspace $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$. Its **minimum distance** is the integer

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

In this extended abstract, we briefly survey some recent results on a special class of rank-metric codes, called Ferrers diagram codes. For $n \in \mathbb{N}$ we let $[n] := \{1,\dots,n\}$. An $n \times m$ **Ferrers diagram** $\mathscr{F}$ is a subset of $[n] \times [m]$ with the following properties:

(i) $(1,1) \in \mathscr{F}$ and $(n,m) \in \mathscr{F}$;
(ii) if $(i,j) \in \mathscr{F}$ and $j < m$, then $(j, j+1) \in \mathscr{F}$ (right-aligned);
(iii) if $(i,j) \in \mathscr{F}$ and $i > 1$, then $(i-1, j) \in \mathscr{F}$ (top-aligned).

We identify a Ferrers diagram $\mathscr{F}$ with $[c_1,\dots,c_m]$, where $c_j = |\{(i,j)\colon 1 \leq i \leq n, (i,j) \in \mathscr{F}\}|$. A Ferrers diagram $\mathscr{F} = [c_1,\dots,c_m]$ can be visualized as a collection of top-aligned and right-aligned dots where the j-th column has

c_j dots. Just like for matrices, we index the rows from top to bottom and the columns from left to right (see Figure 1 for an example).

Let $\mathbb{F}_q[\mathscr{F}]$ be the space of matrices in $\mathbb{F}_q^{n\times m}$ with support in $\mathscr{F}$. Then if $\mathscr{C} \leq \mathbb{F}_q[\mathscr{F}]$, we say that $\mathscr{C}$ is a **Ferrers diagram code** of **shape** $\mathscr{F}$. Ferrers diagram codes are used for the so-called multilevel construction, a general machinery to produce subspace codes proposed by Etzion and Silberstein in [3]. The multilevel construction produces subspace codes by combining several rank-metric codes with special properties and more precisely, it relies on the existence of Ferrers diagram codes of minimum distance lower bounded by a given d. The cardinality of the resulting subspace code increases with the dimension of the underlying Ferrers diagram codes. Therefore it is very natural to ask how large these linear spaces can be.

In [3] an upper bound for the dimension of a Ferrers diagram code of shape $\mathscr{F}$ and with a given rank distance d was given. To this day, it is not clear whether this upper bound, which from now on we denote by $\kappa(\mathscr{F},d)$, is sharp for all pairs $(\mathscr{F},d)$ and all q. We refer to codes attaining this bound as **maximal Ferrers diagram codes**. Showing the existence of maximal Ferrers diagram codes is an open problem that has been studied extensively and several cases have been established [3, 2, 4] by giving constructions of such codes.

In this talk, we show how to approach this open problem from a more combinatorial and asymptotic viewpoint. The technique we concentrate on is based on graph theory and was first developed in [5] in order to show that MRD codes are sparse as $q \to +\infty$. In our approach we look at maximal Ferrers diagram codes of shape $\mathscr{F}$ and minimum distance d as those $\kappa(\mathscr{F},d)$-dimensional spaces in $\mathbb{F}_q[\mathscr{F}]$ which do not contain any nonzero matrix $M \in \mathbb{F}_q[\mathscr{F}]$ with $\mathrm{rk}(M) \leq d-1$. Using this idea, we can then regard maximal Ferrers diagram codes as the isolated vertices of a bipartite graph having strong regularity properties. Using ideas from statistics that compare the mean and average of a discrete, uniform distribution, we get estimates on the number of these isolated vertices.

As a first application of the bounds on the maximal Ferrers diagram codes coming from the graph theory machinery we are interested in probability considerations: Given a pair $(\mathscr{F},d)$, what is the probability that a uniformly random Ferrers diagram code in $\mathbb{F}_q[\mathscr{F}]$ of dimension $\kappa(\mathscr{F},d)$ has minimum distance d as q tends to infinity? In [1] evidence was given that the answer to this question highly depends on the number of points on the diagonals of a Ferrers diagram. More precisely, for $1 \leq r \leq n+m-1$ we define the **r-th diagonal** as $D_r = \{(i,j)\colon i-j = n-r\} \subseteq [n]\times[m]$.

Example 0.1. Let $\mathscr{F} = [1,3,3,4,6,6]$. We have $|D_i \cap \mathscr{F}| = i$ for $1 \leq i \leq 6$,

$|D_7 \cap \mathscr{F}| = 2$ and $|D_i \cap \mathscr{F}| = 0$ for $8 \leq i \leq 11$.

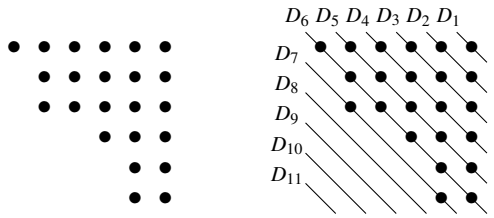

Figure 1: $\mathscr{F} = [1,3,3,4,6,6]$ and the points on the diagonals of $\mathscr{F}$.

If $\kappa(\mathscr{F},d) = \sum_{i=1}^{m} \max\{|D_i \cap \mathscr{F}| - d + 1, 0\}$ then we call the pair $(\mathscr{F},d)$ is called **MDS-constructible**. It was shown that if the pair $(\mathscr{F},d)$ is MDS-constructible, then maximal Ferrers diagram codes of shape $\mathscr{F}$ and minimum distance d are dense as $q \to +\infty$. The other implication was stated as an open question in [1, Open Problems (a)]. The terminology of MDS-constructibility comes from the fact that there exists a construction for codes of shape $\mathscr{F}$ and of minimum distance d and dimension $\kappa(\mathscr{F},d)$ using MDS codes. For establishing our result, we prove that the following is an equivalent definition of MDS-constructibility.

Lemma 0.2. The pair $(\mathscr{F},d)$ is MDS-constructible if and only if

$$\kappa(\mathscr{F},d) = \sum_{i=1}^{m+n-1} \max\{|D_i \cap \mathscr{F}| - d + 1, 0\}.$$

The RHS of Lemma 0.2 turns to be the right quantity to look at when deciding which Ferrers diagram codes are dense and which are sparse. The following is a generalization of [1, Corollary VI.13].

Theorem 0.3. Let $\mathscr{F}$ be an $n \times m$ Ferrers diagram let $2 \leq d \leq n$. The following hold:

(i) If $\kappa(\mathscr{F},d) = \sum_{i=1}^{n+m-1} \max\{|D_i \cap \mathscr{F}| - d + 1, 0\}$ then maximal $\mathscr{F}$-codes of minimum distance d are dense as $q \to +\infty$.

(ii) If $\kappa(\mathscr{F},d) \geq \sum_{i=1}^{n+m-1} \max\{|D_i \cap \mathscr{F}| - d + 1, 0\} + 2$ then maximal $\mathscr{F}$-codes of minimum distance d are sparse as $q \to +\infty$.

Moreover, if $\kappa(\mathscr{F},d) = \sum_{i=1}^{n+m-1} \max\{|D_i \cap \mathscr{F}| - d + 1, 0\} + 1$ then maximal $\mathscr{F}$-codes of minimum distance d are *not* dense as $q \to +\infty$.

Another interesting application of the graph theory tools is to show existence of maximal Ferrers diagram codes. Theorem 0.3 (i) shows that for large enough q, there exist maximal $\mathscr{F}$-codes of minimum distance d if $(\mathscr{F},d)$ is MDS-constructible. The lower bound we used in order to show

that Ferrers diagram codes are dense as $q \to +\infty$ for when $(\mathscr{F}, d)$ is MDS-constructible can be used to obtain the existence of certain maximal Ferrers diagram codes for field sizes that are smaller than those of known constructions.

The last part of this abstract is dedicated to MDS-constructible pairs $(\mathscr{F}, d)$. More precisely, for a fixed integer $2 \leq d \leq n$, we are interested in counting the number of $n \times m$ Ferrers diagrams $\mathscr{F}$ for which $(\mathscr{F}, d)$ is MDS-constructible. For $d = 2$ we obtain the following formula.

Theorem 0.4. The number of $n \times m$ Ferrers diagrams $\mathscr{F}$ for which $(\mathscr{F}, 2)$ is MDS-constructible is given by

$$\frac{m-n+1}{m}\binom{m+n-2}{n-1}.$$

From Theorem 0.4 it follows that for large m and fixed n, almost every Ferrers diagram has the property of being MDS-constructible with respect to $d = 2$. Interestingly, the number of $n \times n$ Ferrers diagrams for which the pair $(\mathscr{F}, 2)$ is MDS-constructible, given in Theorem 0.4, corresponds to the $(n-1)$th *Catalan number*; see e.g [6]. Catalan numbers have applications in various counting problems, often involving recursively defined objects. This result establishes a curious link between these numbers and the theory of rank-metric codes.

Keywords: rank metric, Ferrers diagram, density, Catalan numbers

References

[1] J. Antrobus and H. Gluesing-Luerssen, *Maximal Ferrers diagram codes: Constructions and genericity considerations*, IEEE Transactions on Information Theory **65** (2019), no. 10, 6204–6223.

[2] Tuvi Etzion, Elisa Gorla, Alberto Ravagnani, and Antonia Wachter-Zeh, *Optimal ferrers diagram rank-metric codes*, IEEE Transactions on Information Theory **62** (2016), no. 4, 1616–1630.

[3] Tuvi Etzion and Natalia Silberstein, *Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams*, IEEE Transactions on Information Theory **55** (2009), no. 7, 2909–2919.

[4] Elisa Gorla and Alberto Ravagnani, *Subspace codes from Ferrers diagrams*, Journal of Algebra and Its Applications **16** (2017), no. 07, 1750131.

[5] Anina Gruica and Alberto Ravagnani, *Common complements of linear subspaces and the sparseness of MRD codes*, arXiv preprint arXiv:2011.02993 (2020).

[6] R. Stanley, *Enumerative Combinatorics*, 2nd ed., vol. 1, Cambridge University Press, 2011.