Rank-Metric Lattices

Giuseppe Cotardo[*]

Department of Mathematics
Virginia Tech
Virginia, U.S.A.

gcotardo@vt.edu

Alberto Ravagnani[†]

Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, the Netherlands

a.ravagnani@tue.nl

Abstract

We introduce the class of rank-metric geometric lattices and initiate the study of their structural properties. Rank-metric lattices can be seen as the q-analogues of higher-weight Dowling lattices, defined by Dowling himself in 1971. We fully characterize the supersolvable rank-metric lattices and compute their characteristic polynomials. We then concentrate on small rank-metric lattices whose characteristic polynomial we cannot compute, and provide a formula for them under a polynomiality assumption on their Whitney numbers of the first kind. The proof relies on computational results and on the theory of vector rank-metric codes, which we review in this paper from the perspective of rank-metric lattices. More precisely, we introduce the notion of lattice-rank weights of a rank-metric code and investigate their properties as combinatorial invariants and as code distinguishers for inequivalent codes.

Mathematics Subject Classifications: 05A15, 06C10, 94B99

1 Introduction

This paper initiates the study of *rank-metric lattices* and of their connection with the invariant theory of rank-metric codes. We define a rank-metric lattice as the combinatorial subgeometry of $\mathbb{F}_{q^m}^n$ whose atoms are the projective points corresponding to vectors having small rank (defined later).

Rank-metric lattices can be seen as the q-analogues of a family of lattices that have been studied since the seventies, namely higher-weight Dowling lattices. These were

---

introduced by Dowling himself [21, 22] in connection with the main problem of classical coding theory, i.e., computing the largest dimension of an error-correcting code in the Hamming metric with given length and correction capability. This question connects with the famous conjecture by Segre on the largest size of an arc in a projective space over a finite field [34]. Higher-weight Dowling lattices have been studied by various authors [21, 22, 8, 9, 28, 10, 24, 38, 33, 11], yet the techniques for computing their characteristic polynomial are to date unknown.

Computing the characteristic polynomials of rank-metric lattices is equivalent to counting/estimating the number of rank-metric codes with given length and correction capability, a line of research that is becoming increasingly important in contemporary coding theory; see e.g. [2, 16, 25, 31].

The first member of the family of rank-metric lattices is precisely the q-analogue of the first member of the family of higher-weight Dowling lattices. Indeed, the former is (isomorphic to) the lattice of subspaces of $\mathbb{F}_q^n$, and the latter is the lattice of subsets of $\{1, \ldots, n\}$. It is natural to ask to which extent this analogy holds. In this paper, we show that divergences in the behavior of q-analogous lattices already appear when examining the second family members. For example, while the second higher-Weight Dowling lattices is supersolvable (it is known as the q-analogue of the partition lattice), the second rank-metric lattice is not. In fact, in Section 4 of this paper we provide a complete characterization of the modular elements of rank-metric lattices, and determine all the supersolvable ones. The proof techniques follow to some extent Bonin's approach [9], but there are important technical differences in the arguments, which almost never translate from higher-weight Dowling lattices to rank-metric lattices (we will explain why).

In Section 5 we compute the characteristic polynomial of some rank-metric lattices, and establish general properties of their roots by combining the characterization of modular elements mentioned above with Stanley's modular factorization theorem [35]. A small rank-metric lattices whose characteristic polynomial we cannot compute is the one generated by vectors in $\mathbb{F}_{q^4}^4$ of rank at most 2. Using a computational approach based on coding theory, in Section 6 we provide a closed formula for its characteristic polynomial under the assumption that its second Whitney number is a polynomial in q. The formula we obtain is compatible with all the other properties of rank-metric lattices we establish throughout the paper.

In Section 7 we consider applications of rank-metric lattices to the invariant theory of (vector) rank-metric codes. We show how rank-metric lattices can be used to define new distinguishers for this class of codes. We start from the observation that the elements of the first rank-metric lattice are exactly the *optimal rank-metric anticodes* defined in [32] in connection with a class of invariants for (vector) rank-metric codes, namely the *generalized vector rank weights*; see [29]. In this paper, we extend the definition of [32] to "higher weight" rank-metric lattices. We then classify some families of rank-metric codes that show interesting extremality properties with respect to these notions and study the concepts *lattice weight distribution* and *lattice binomial moments* in this context.

2 Posets and Lattices

In this section we recall some definitions and results on posets and lattices that we will need throughout the paper. A standard reference for this part is [37, Chapter 3]. The reader who is already familiar with lattice theory can skip this section.

In the sequel, $(\mathscr{P}, \leqslant)$ denotes a finite poset. We say that $(\mathscr{P}, \leqslant)$ is **trivial** if the cardinality of $\mathscr{P}$ is 1. We sometimes abuse notation and simply write $\mathscr{P}$ for $(\mathscr{P}, \leqslant)$. Moreover, for $s, t \in \mathscr{P}$ we write $s < t$ for $s \leqslant t$ and $s \neq t$.

Definition 1. Elements $s, t \in \mathscr{P}$ are **comparable** if $s \leqslant t$ or $t \leqslant s$. We say that t **covers** s (or that s **is covered** by t) if $s < t$ and there is no element $u \in \mathscr{P}$ such that $s < u < t$. The notation is $s \lessdot t$.

Definition 2. The **join** of $s, t \in \mathscr{P}$, should it exist, is the element $u \in \mathscr{P}$ that satisfies $s \leqslant u$, $t \leqslant u$, and $u \leqslant v$ for all $v \in \mathscr{P}$ with $s \leqslant v$ and $t \leqslant v$. Dually, the **meet** of $s, t \in \mathscr{P}$, should it exist, is the element $u \in \mathscr{P}$ that satisfies $u \leqslant s$, $u \leqslant t$, and $v \leqslant u$ for all $v \in \mathscr{P}$ with $v \leqslant s$ and $v \leqslant t$. The poset $\mathscr{P}$ has **minimum element** $0 \in \mathscr{P}$ if $0 \leqslant s$ for all $s \in \mathscr{P}$. Dually, it has **maximum element** $1 \in \mathscr{P}$ if $s \leqslant 1$ for all $s \in \mathscr{P}$.

Notation 3. It is easy to check that the join (resp., the meet) of $s, t \in \mathscr{P}$, should it exist, is unique and we denote it by $s \vee t$ (resp., by $s \wedge t$). The minimum (resp., the maximum) element of $\mathscr{P}$, should it exist, is unique and it is denoted by $0_{\mathscr{P}}$ (resp., by $1_{\mathscr{P}}$), or by 0 (resp., 1) if the poset is clear from context.

Definition 4. The **Möbius function** of $\mathscr{P}$ is defined recursively by $\mu_{\mathscr{P}}(s, t) = 1$ if $s = t$, $\mu_{\mathscr{P}}(s, t) = -\sum_{s \leqslant u < t} \mu_{\mathscr{P}}(s, u)$ if $s < t$, and $\mu_{\mathscr{P}}(s, t) = 0$ otherwise. We sometimes write $\mu_{\mathscr{P}}(t)$ for $\mu_{\mathscr{P}}(0, t)$, when $\mathscr{P}$ has minimum element 0.

The following result is a cornerstone of combinatorics.

Proposition 5 (Möbius Inversion Formula)**.** *Let $\mathbb{K}$ be a field and let $f : \mathscr{P} \longrightarrow \mathbb{K}$ be a function. Define $g : \mathscr{P} \longrightarrow \mathbb{K}$ by $g(t) = \sum_{s \leqslant t} f(s)$ for all $t \in \mathscr{P}$. Then*

$$f(t) = \sum_{s \leqslant t} \mu_{\mathscr{P}}(s, t) \, g(s) \quad \text{for all } t \in \mathscr{P}.$$

Chains play a crucial role in determining the structure of a poset. They are defined as follows.

Definition 6. A **chain** in $\mathscr{P}$ is a non-empty subset $C \subseteq \mathscr{P}$ such that every $s, t \in C$ are comparable. We say that C is **maximal** if there is no chain in $\mathscr{P}$ that strictly contains C. We say that $\mathscr{P}$ is **graded** if all maximal chains in $\mathscr{P}$ have the same cardinality.

We will also need the following concepts.

Definition 7. Suppose that $\mathscr{P}$ is graded and with minimum element 0. The **rank function** $\rho_{\mathscr{P}} : \mathscr{P} \to \mathbb{Z}$ of $\mathscr{P}$ is uniquely defined by $\rho_{\mathscr{P}}(0) = 0$ and $\rho_{\mathscr{P}}(t) = \rho_{\mathscr{P}}(s) + 1$ whenever $s, t \in \mathscr{P}$ and $s \lessdot t$. In this case we call $\rho_{\mathscr{P}}(s)$ the **rank** of s and the elements $s \in \mathscr{P}$ with $\rho_{\mathscr{P}}(s) = 1$ are called **atoms** of $\mathscr{P}$. We denote the set of atoms of $\mathscr{P}$ by $\mathrm{At}(\mathscr{P}) \subseteq \mathscr{P}$. We call $\mathscr{P}$ **semimodular** if it is graded and

$$\rho_{\mathscr{P}}(s \wedge t) + \rho_{\mathscr{P}}(s \vee t) \leqslant \rho_{\mathscr{P}}(s) + \rho_{\mathscr{P}}(t) \quad \text{for all } s, t \in \mathscr{P}. \tag{1}$$

An element $t \in \mathscr{P}$ is called **modular** if equality holds in (1) for all $s \in \mathscr{P}$.

In this paper, we focus on the following special family of posets, called *lattices*. Standard examples of posets (such as the poset of subsets of a finite set and the poset of linear subspaces of a space over a finite field) are in fact lattices.

Definition 8. A **finite lattice** $(\mathscr{L}, \leqslant)$ is a finite poset where every $s, t \in \mathscr{L}$ have a join and a meet. In this case, join and meet can be seen as commutative and associative operations $\vee, \wedge : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$. In particular, the **join** (resp., the **meet**) of a non-empty subset $S \subseteq \mathscr{L}$ is well-defined as the join (resp., the meet) of its elements and denoted by $\vee S$ (resp., by $\wedge S$). Furthermore, $\mathscr{L}$ has a minimum and maximum element ($0_{\mathscr{L}}$ and $1_{\mathscr{L}}$, resp.). Finally, if $\mathscr{L}$ is graded then the **rank** of $\mathscr{L}$ is $\mathrm{rk}(\mathscr{L}) = \rho_{\mathscr{L}}(1_{\mathscr{L}})$.

One of the most studied combinatorial invariants of a lattice is its characteristic polynomial, defined as follows.

Definition 9. Let $\mathscr{L}$ be a finite graded lattice with rank function ρ and Möbius function μ. The **characteristic polynomial** of $\mathscr{L}$ is the element of $\mathbb{Z}[\lambda]$ defined as

$$\chi(\mathscr{L}; \lambda) := \sum_{s \in \mathscr{L}} \mu(s) \lambda^{\mathrm{rk}(\mathscr{L}) - \rho(s)} = \sum_{i=0}^{\mathrm{rk}(\mathscr{L})} w_i(\mathscr{L}) \lambda^{\mathrm{rk}(\mathscr{L}) - i},$$

where

$$w_i(\mathscr{L}) = \sum_{\substack{s \in \mathscr{L} \\ \rho(s) = i}} \mu(s)$$

is the i-**th Whitney number of the first kind** of $\mathscr{L}$. The i-**th Whitney number of the second kind** of $\mathscr{L}$, denoted by $W_i(\mathscr{L})$, is the number of elements of $\mathscr{L}$ of rank i.

Computing the characteristic polynomial of a lattice is a standard problem in combinatorics. For some lattices, this problem is more "approachable" than for others.

Definition 10. A **geometric lattice** is a finite lattice $(\mathscr{L}, \leqslant)$ which is semimodular and **atomistic**, i.e., every element $s \in \mathscr{L}$ is the join of a set of atoms of $\mathscr{L}$.

In [35, 36], Stanley identified a class of geometric lattices whose characteristic polynomial has a precise combinatorial significance. They can be defined as follows.

Definition 11. A geometric lattice $\mathscr{L}$ is called **supersolvable** if $\mathscr{L}$ has a maximal chain made of modular elements.

The following result is known as Stanley's modular factorization Theorem. It gives a sufficient condition for the characteristic polynomial of a geometric lattices to have a factor.

Theorem 12 (see [35, Theorem 2]). *Let $\mathscr{L}$ be a geometric lattice of rank n and let $t \in \mathscr{L}$ be a modular element. We have*

$$\chi(\mathscr{L}; \lambda) = \chi([0, t]; \lambda) \sum_{\substack{x \in \mathscr{L} \\ x \wedge t = 0}} \mu_{\mathscr{L}}(x) \lambda^{n - \rho_{\mathscr{L}}(x) - \rho_{\mathscr{L}}(t)}.$$

As a corollary of the previous theorem we finally obtain Stanley's decomposition result for the characteristic polynomial of a geometric supersolvable lattice. The corollary shows that the polynomial splits into linear factors, whose roots have a precise combinatorial significance; see also [36, Section 3].

Corollary 13. *Let $\mathscr{L}$ be a supersolvable geometric lattice of rank n and let $0 = t_0 \lessdot t_1 \lessdot \cdots \lessdot t_n = 1$ be a maximal chain of modular elements of $\mathscr{L}$. We have*

$$\chi(\mathscr{L}; \lambda) = \prod_{i=1}^{n} (\lambda - |\{a \in \mathrm{At}(\mathscr{L}) \mid a \leqslant t_i, \, a \not\leqslant t_{i-1}\}|).$$

Corollary 13 and its generalizations (see e.g. [26, 7]) are standard tools for computing the characteristic polynomial of geometric lattices. Unfortunately, not all geometric lattices are supersolvable, hence their characteristic polynomial has to be computed using other approaches. This will be the case of *rank-metric lattices*, which we introduce in the next section.

3 Rank-Metric Lattices

In this section we define the main combinatorial objects studied in this paper, namely *rank-metric lattices*. These can be seen as the q-analogue of the higher-weights Dowling lattices, which were introduced in 1971 by Dowling [21] and later investigated and generalized by several authors; see below for further details on this.

We will also illustrate the connection between rank-metric lattices and the problem of computing the number of rank-metric codes of given dimension and minimum distance lower bounded by a given integer d. The latter is a central problem in contemporary coding theory.

Notation 14. Throughout this paper, q is a prime power and n, m are integers with $n, m \geqslant 2$. We denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_{q^m}$ its extension of degree m. We let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{F}_q^n$. With a small abuse of notation we denote by $\{e_1, \ldots, e_n\}$ also the standard basis of $\mathbb{F}_{q^m}^n$. All dimensions in the sequel are computed over $\mathbb{F}_{q^m}$, unless otherwise stated. We denote by $\leqslant$ the inclusion of linear spaces, to emphasize the order structure.

We start by defining the *rank* of a vector with entries from the field extension $\mathbb{F}_{q^m}$.

Definition 15. The **rank** (**weight**) of a vector $v \in \mathbb{F}_{q^m}$ is the dimension over $\mathbb{F}_q$ of the $\mathbb{F}_q$-span of its entries. We denote it by $\mathrm{rk}(v)$.

The rank of a vector is closely related to that of a matrix. To see this, let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be an ordered $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. For a vector $v \in \mathbb{F}_{q^m}^n$ we let $\Gamma(v)$ be the $n \times m$ matrix with entries in $\mathbb{F}_q$ defined by

$$v_i =: \sum_{j=1}^{m} \Gamma(v)_{i,j} \gamma_j \quad \text{for all } i.$$

By definition, the map $\mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{n \times m}$ given by $v \longmapsto \Gamma(v)$ is an $\mathbb{F}_q$-isomorphism and we have $\mathrm{rk}(v) = \mathrm{rk}(\Gamma(v))$ for all bases Γ and for all $v \in \mathbb{F}_{q^m}^n$.

The following properties of the vector rank will be needed repeatedly. They easily follow from the connection between vector and matrix rank explained above.

Proposition 16. *The following hold.*

(1) $\mathrm{rk}(v) \geqslant 0$ *for all* $v \in \mathbb{F}_{q^m}^n$, *with equality if and only if* $v = 0$.

(2) $\mathrm{rk}(v) = \mathrm{rk}(\lambda v)$ *for all* $v \in \mathbb{F}_{q^m}^n$ *and* $\lambda \in \mathbb{F}_{q^m} \setminus \{0\}$.

(3) $\mathrm{rk}(v + w) \leqslant \mathrm{rk}(v) + \mathrm{rk}(w)$ *for all* $v, w \in \mathbb{F}_{q^m}^n$ *(triangular inequality).*

(4) $\mathrm{rk}(v + w) \geqslant \mathrm{rk}(v) - \mathrm{rk}(w)$ *for all* $v, w \in \mathbb{F}_{q^m}^n$.

We are now ready to introduce the class *rank-metric lattices*, whose elements are the $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$ having a basis of vectors with rank bounded from above, ordered by inclusion.

Definition 17. Let $i \in \{1, \ldots n\}$. The **rank-metric lattice** (**RML** in short) $\mathscr{L}_i(n, m; q)$ associated with the 4-tuple (i, n, m, q) is the geometric sublattice of $\mathscr{L}(\mathbb{F}_{q^m}^n)$ whose atoms are the 1-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$ generated by the vectors of rank at most i, that is,

$$\mathscr{L}_i(n, m; q) := \{\langle v_1, \ldots, v_\ell \rangle_{\mathbb{F}_{q^m}} : \ell \geqslant 1, \, v_1, \ldots, v_\ell \in T_i(n, m; q)\},$$

where $T_i(n, m; q) := \{v \in \mathbb{F}_{q^m}^n : \mathrm{rk}(v) \leqslant i\}$. The order is given by the inclusion of $\mathbb{F}_{q^m}$-linear subspaces of $\mathbb{F}_{q^m}^n$.

We will need the following observations, which we will use without explicitly referring to them.

Remark 18. It follows from the definitions that $\mathscr{L}_i(n, m; q)$ is a geometric lattice of rank n, where the rank function is given by the $\mathbb{F}_{q^m}$-dimension. Furthermore, for any $X, Y \in \mathscr{L}_i(n, m; q)$ we have $X \vee_i Y = X + Y$ (the ordinary sum of linear subspaces) and $X \wedge_i Y = \langle x \in X \cap Y : \mathrm{rk}(x) \leqslant i \rangle$, where $\vee_i$ and $\wedge_i$ denote the operations of join and meet in $\mathscr{L}_i(n, m; q)$, respectively. By definition we have that $\mathscr{L}_0(n, m; q)$ is the trivial lattice $\{0\}$ and that $\mathscr{L}_n(n, m; q) = \{X \leqslant \mathbb{F}_{q^m}^n\}$ is the lattice of $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$.

As already mentioned, rank-metric lattices can be seen as the q-analogues (or also rank-metric analogues) of a well-studied class of lattices, known under the name of *higher-weight Dowling lattices*. These combinatorial geometries were introduced by Dowling in connection with a fundamental problem in coding theory; see [21, 22]. Their theory and connections with the Critical Problem by Crapo and Rota was further explored by Zaslavsky [38], Bonin [8, 9], Kung [28], Brini [10], Games [24], Britz [11], and more recently by Ravagnani [33]. The techniques for computing the characteristic polynomials of these lattices for arbitrary parameters are currently unknown.

Definition 19. Let Q be a prime power. The **Hamming weight** of a vector $v \in \mathbb{F}_Q^n$ is $\mathrm{wt}^{\mathrm{H}}(v) := |\{i \in [n] : v_i \neq 0\}|$. For $i \in \{1, \dots, n\}$, the **higher-weight Dowling lattice** (**HWDL** in short) $\mathscr{H}_i(n; Q)$ associated to the 3-tuple (i, n, Q) is the geometric sublattice of $\mathscr{L}(\mathbb{F}_Q^n)$ whose atoms are the 1-dimensional $\mathbb{F}_Q$-subspaces of $\mathbb{F}_Q^n$ generated by vectors of Hamming weight at most i, that is

$$\mathscr{H}_i^{\mathrm{H}}(n; Q) := \{\langle v_1, \dots, v_n \rangle_{\mathbb{F}_Q} : \ell \geqslant 1, \, v_1, \dots, v_\ell \in T_i^{\mathrm{H}}(n; Q)\},$$

where $T_i^{\mathrm{H}}(n; Q) := \{v \in \mathbb{F}_Q^n : \mathrm{wt}^{\mathrm{H}}(v) \leqslant i\}$.

Computing the characteristic polynomial (or equivalently the Whitney numbers of the first kind) of higher-weight Dowling lattices would allow to solve a long-standing open problem in coding theory and finite geometry, namely the famous *Segre's conjecture*, known as the *MDS Conjecture* in the context of coding theory. More generally, computing the characteristic polynomial of higher-weight Dowling lattices would allow one to give formulas for the number of Hamming-metric codes having given dimension and minimum distance bounded from below by an integer d. The q-analogy between higher-weight Dowling lattices and rank-metric lattices "lifts" to an analogy between the corresponding questions about codes, as we now briefly illustrate.

Definition 20. A (**rank-metric**) **code** is an $\mathbb{F}_{q^m}$-linear subspace $C \leqslant \mathbb{F}_{q^m}^n$. The **minimum (rank) distance** of C is $d(C) := \min\{\mathrm{rk}(v) : v \in \mathbb{F}_{q^m}^n, v \neq 0\}$, where the zero code $\{0\}$ has minimum distance $\min\{n, m\} + 1$ by definition. In this context, n is called the **length** of C. The **dual** of C is the code $C^\perp := \{v \in \mathbb{F}_{q^m}^n : c \cdot v = 0 \text{ for all } c \in C\}$, where $\cdot$ denotes the standard inner product of vectors.

The *equivalence* between the problem of counting rank-metric codes with given dimension and minimum distance lower bounded by d and that of computing the Whitney numbers of rank-metric lattices is expressed by Theorem 23 below (the general version of the result is [33, Theorem 3.1]). In order to state it, we will need the following symbols and the notion of Gaussian binomial coefficients; see [1].

Notation 21. We let $w_j(i, n, m; q)$ be the j-th Whitney number of the second kind of the lattice $\mathscr{L}_i(n, m; q)$. We denote by $\alpha_k(i, n, m; q)$ the number of k-dimensional rank-metric codes $C \leqslant \mathbb{F}_{q^m}^n$ with $d(C) \geqslant i + 1$. The j-th Whitney number of the first kind of $\mathscr{L}_i(n, m; q)$ is denoted by $W_j(i, n, m; q)$.

Definition 22. Let a, b be integers and let Q be a prime power. The Q-binomial coefficients of a and b is

$$\begin{bmatrix} a \\ b \end{bmatrix}_Q = \begin{cases} 0 & \text{if } b < 0 \text{ or } 0 \leqslant a < b, \\ 1 & \text{if } b = 0 \text{ and } a \geqslant 0, \\ \displaystyle\prod_{i=0}^{b-1} \frac{Q^{a-i} - 1}{Q^{i+1} - 1} & \text{if } b > 0 \text{ and } a \geqslant b. \end{cases}$$

We can now state the rank-metric instance of [33, Theorem 3.1].

Theorem 23. *The following hold for any $j \in \{0, \dots, n\}$.*

(1) $w_j(i, n, m; q) = \displaystyle\sum_{k=0}^{j} \alpha_k(i, n, m; q) \begin{bmatrix} n - k \\ j - k \end{bmatrix}_{q^m} (-1)^{j-k} q^{m\binom{j-k}{2}}.$

(2) $\alpha_j(i, n, m; q) = \displaystyle\sum_{k=0}^{j} w_k(i, n, m; q) \begin{bmatrix} n - k \\ j - k \end{bmatrix}_{q^m}.$

A very natural question is for which values of j we have $\alpha_j(i, n, m; q) = 0$. A partial answer to this question is given by the following result, which follows from [20, Theorem 5.4].

Theorem 24 (rank-metric Singleton bound). *Let $1 \leqslant k \leqslant n$ and $1 \leqslant d \leqslant \min\{n, m\}$ be integers. Let $C \leqslant \mathbb{F}_{q^m}^n$ be a code of dimension $k \geqslant 1$ and minimum distance at least d. We have*

$$mk \leqslant \max\{n, m\}(\min\{n, m\} - d + 1).$$

Proof. Let Γ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\Gamma(v) : v \in C\}$ is an $\mathbb{F}_q$ linear space of matrices, of the same cardinality as C, in which every non-zero matrix has rank at least d. Therefore by [20, Theorem 5.4] we have that $|C| \leqslant \min\{q^{m(n-d+1)}, q^{n(m-d+1)}\}$. The desired bound follows from the fact that $|C| = q^{mk}$. $\qquad\square$

We conclude this section with the following lemma summarizing some well-known properties of Gaussian binomial coefficients. We will need them in various proofs later.

Lemma 25. *Let a, b, c be integers, let Q be a prime power, and let x, y be rational numbers. The following hold.*

(1) $\begin{bmatrix} a \\ b \end{bmatrix}_Q \begin{bmatrix} b \\ c \end{bmatrix}_Q = \begin{bmatrix} a \\ c \end{bmatrix}_Q \begin{bmatrix} a - c \\ a - b \end{bmatrix}_Q.$

(2) $\begin{bmatrix} a + b \\ c \end{bmatrix}_Q = \displaystyle\sum_{j=0}^{c} Q^{j(b-c+j)} \begin{bmatrix} a \\ j \end{bmatrix}_Q \begin{bmatrix} b \\ c - j \end{bmatrix}_Q = \sum_{j=0}^{c} Q^{(c-j)(a-j)} \begin{bmatrix} a \\ j \end{bmatrix}_Q \begin{bmatrix} b \\ c - j \end{bmatrix}_Q.$

(3) $\displaystyle\sum_{j=0}^{c} \begin{bmatrix} c \\ j \end{bmatrix}_Q (-1)^j Q^{\binom{j}{2}} x^{c-j} y^j = \begin{cases} 0 & \text{if } c = 0, \\ \displaystyle\prod_{j=0}^{c-1} (x - Q^j y) & \text{if } c \geqslant 1. \end{cases}$

4 Supersolvability

As Stanley's modular factorization theorem shows, the characteristic polynomial of supersolvable geometric lattices is particularly easy to compute and completely determined by the combinatorial structure of the lattice's atoms; see Theorem 12. It is therefore very natural to ask which rank-metric lattices are supersolvable, a question that we answer completely in this section.

Continuing the analogy with the Hamming-metric case, we will first state which higher-weight Dowling lattices are supersolvable. These were fully characterized by Bonin in [9] and are very few, as the following result shows.

Theorem 26 (see [9]). *The only non-trivial supersolvable higher-weight Dowling lattices are* $\mathscr{H}_1(n;q)$, $\mathscr{H}_2(n;q)$, $\mathscr{H}_{n-1}(n;q)$ *for* $n \geqslant 2$, *and* $\mathscr{H}_n(n;q)$.

The rank-metric analogue of Theorem 26, to the proof of which this section is entirely devoted, is the following.

Theorem 27. *The lattice* $\mathscr{L}_i(n,m;q)$ *is supersolvable if and only if one of the following holds:*

(1) $i \in \{1, n-1, n\}$,

(2) $m \in \{2, \ldots, i\}$.

Note Theorem 27 shows that the parameter q does not play any role in determining whether or not $\mathscr{L}_i(n,m;q)$ is supersolvable.

Remark 28. The approaches developed in [9, 22] extends only in part from the Hamming to the rank metric, because of technical differences between the two metrics that arise in the proofs. In fact, while the second higher-weight Dowling lattice $\mathscr{H}_2(n;q)$ is supersolvable (it is known as the q-analogue of the partition lattice), the second rank-metric lattice $\mathscr{L}_2(n,m;q)$ is *not* supersolvable, as we will prove in this section. Our main result is a complete characterization of the modular elements of $\mathscr{L}_i(n,m;q)$, from which Theorem 27 follows easily. The proof of the characterization is split across a number of preliminary results, which we will combine at the end of the section.

We start with the rank-metric analogues of [9, Lemmas 1.2 and 1.4]. Their proofs extend easily from the Hamming-metric case.

Lemma 29. *Let* $X \in \mathscr{L}_i(n,m;q)$. *Then* X *is modular if and only if* $X \wedge_n Y = X \wedge_i Y$ *for all* $Y \in \mathscr{L}_i(n,m;q)$.

Proof. Recall that, by definition of modularity, X is a modular element of $\mathscr{L}_i(n,m;q)$ if and only if, for all $Y \in \mathscr{L}_i(n,m;q)$,

$$\dim(X \wedge_i Y) = \dim(X) + \dim(Y) - \dim(X \vee_i Y). \tag{2}$$

Since $X \vee_i Y = X \vee_n Y$, we have that the right hand side of (2) is $X \wedge_n Y$. It follows that X is modular in $\mathscr{L}_1(n,m;q)$ if and only if $\dim(X \wedge_i Y) = \dim(X \wedge_n Y)$. The statement now follows from the fact that $X \wedge_i Y \leqslant X \wedge_n Y$. □

Lemma 30. *Let X be a modular element of $\mathscr{L}_i(n, m; q)$ and let $x \in X \setminus T_i(n, m; q)$. If $y \in T_i(n, m; q)$ and $x + y \in T_i(n, m; q)$, then $y \in X$.*

Proof. We have $\mathrm{rk}(x) \geqslant i + 1$, $\mathrm{rk}(y) \leqslant i$, and $\mathrm{rk}(x + y) \leqslant i$. Define the lattice element $Y := \langle x + y, y \rangle_{\mathbb{F}_{q^m}} \in \mathscr{L}_i(n, m; q)$ and assume toward a contradiction that $y \notin X$. Since $y \in Y \setminus X$, we have $X \wedge_n Y = \langle x \rangle_{\mathbb{F}_{q^m}}$. Since $x \notin T_i(n, m; q)$, we have $X \wedge_i Y = \{0\}$. Therefore X is not modular by Lemma 29. $\qquad\square$

We will establish Theorem 27 in various steps and by treating the cases $i = 1$, $i = 2$, and $i \geqslant 3$ separately. While the general proof strategy is similar to that of [9], the technical details are different and heavily rely on the properties of the rank weight.

Proposition 31. *$\mathscr{L}_1(n, m; q)$ is isomorphic to the lattice of $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$. In particular, $\mathscr{L}_1(n, m; q)$ is a modular lattice.*

Proof. We will construct a poset isomorphism $f : (\mathscr{L}, \leqslant) \longrightarrow \mathscr{L}_1(n, m; q)$, where $(\mathscr{L}, \leqslant)$ is the lattice of $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ ordered by inclusion. Define $f(U) := \langle U \rangle_{\mathbb{F}_{q^m}} = U \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ for all $U \in \mathscr{L}$. It is easy to see that f is order preserving and injective. Therefore to conclude the proof it suffices to prove that f is surjective. To see this, let $X \in \mathscr{L}_1(n, m; q)$ and let $\{v_1, \ldots, v_j\}$ be an $\mathbb{F}_{q^m}$-basis of X made of vectors of rank 1. Write $v_\ell = \lambda_\ell w_\ell'$ for $\ell \in \{1, \ldots, j\}$, where $\lambda_\ell \in \mathbb{F}_{q^m} \setminus \{0\}$ and $w_\ell \in \mathbb{F}_q^n$. Then $X = U \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = f(U)$, where $U = \langle w_1, \ldots, w_j \rangle_{\mathbb{F}_q}$, concluding the proof. $\qquad\square$

Remark 32. The proof of Proposition 31 shows that the elements of $\mathscr{L}_1(n, m; q)$ are precisely those subspaces of $\mathbb{F}_{q^m}$ having a basis made of vectors with entries in $\mathbb{F}_q$. These are the optimal rank-metric anticodes; see [32, Section 4].

The following lemma summarizes some properties of the rank of a vector that will be crucial in our approach. These are mainly inherited from the correspondence between vector rank and matrix rank illustrated in Section 3. They will be applied in several instances throughout this section, without referring to them explicitly, to avoid making the exposition too cumbersome.

Lemma 33. *Let $v \in \mathbb{F}_{q^m}^n$ be a non-zero vector. Then $\mathrm{rk}(v)$ is the smallest r for which there exist rank-1 vectors $v_1, \ldots, v_r \in \mathbb{F}_{q^m}^n$ with $v = v_1 + \cdots + v_r$. Furthermore, any such rank-1 vectors $v_1, \ldots, v_r$ are linearly independent over $\mathbb{F}_{q^m}$. Finally, for every $S \subseteq \{1, \ldots, r\}$ we have that $\sum_{j \in S} v_j$ has rank $|S|$.*

Proof. The first part of the statement follows from the fact that $v \mapsto \Gamma(v)$ is a rank-preserving $\mathbb{F}_q$-linear isomorphism (for any basis Γ).

For the second part, suppose towards a contradiction that the rank-1 vectors $v_1, \ldots, v_r$ are not linearly independent over $\mathbb{F}_{q^m}$ and let $\lambda_1, \ldots, \lambda_{r-1} \in \mathbb{F}_{q^m}$ such that (without loss of generality) $v_r = \lambda_1 v_1 + \cdots + \lambda_{r-1} v_{r-1}$. We then have

$$v = v_1 + \cdots + v_r = (1 + \lambda_1)v_1 + \cdots + (1 + \lambda_{r-1})v_{r-1},$$

which implies $\mathrm{rk}(v) \leqslant r - 1$ by the triangular inequality; see Proposition 16. This is a contradiction.

In order to prove the last part of the statement, let $S \subseteq \{1, \ldots, r\}$ and $w := \sum_{j \in S} v_j$. Suppose towards a contradiction that $\mathrm{rk}(w) < |S|$. Define the vector $u := \sum_{j \notin S} v_j$ and observe that $\mathrm{rk}(u) \leqslant r - |S|$, since it is the sum of $r - |S|$ rank-1 vectors. By the triangle inequality we have

$$r = \mathrm{rk}(v) = \mathrm{rk}(w + u) \leqslant \mathrm{rk}(w) + \mathrm{rk}(u) < |S| + r - |S| = r,$$

which is a contradiction. $\qquad\square$

The following two lemmas are devoted to the case $i = 2$. Note that the proof techniques do not apply to the Hamming-metric case. In fact, the Hamming-metric analogues of the following two lemmas are false; see [22].

Lemma 34. *Let X be a modular element of $\mathscr{L}_2(n, m; q)$. If X contains an element of rank 3, then $X = \mathbb{F}_{q^m}^n$.*

Proof. Suppose that X has an element of rank 3, say x. By Lemma 33, there exist $x_1, x_2, x_3 \in \mathbb{F}_{q^m}^n$ of rank 1, linearly independent over $\mathbb{F}_{q^m}$, with $x = x_1 + x_2 + x_3$. Define $y := x_1 + x_2$ and note that $x - y = x_3$. We have $y, x_3 \in T_2(n, m; q)$, which implies that $y, x_3 \in X$, by Lemma 30. Analogously, $x_1, x_2 \in X$. If $n = 3$, then this immediately shows that $X = \mathbb{F}_{q^m}^3$, because x_1, x_2 and x_3 are linearly independent over $\mathbb{F}_{q^m}$.

We assume $n \geqslant 4$ in the remainder of the proof. We complete $\{x_1, x_2, x_3\}$ to a basis of $\mathbb{F}_{q^m}^n$ by selecting vectors $x_4, \ldots, x_n \in \mathbb{F}_{q^m}^n$ of rank 1 (observe that is always possible because the rank-1 vectors of $\mathbb{F}_{q^m}^n$ span $\mathbb{F}_{q^m}^n$). For all $j \in \{1, \ldots, n\}$, let $\lambda_j \in \mathbb{F}_{q^m} \setminus \{0\}$ such that $x_j = \lambda_j y_j$, for some $y_j \in \mathbb{F}_q^n \setminus \{0\}$. Note that the λ_j's exist because $\mathrm{rk}(x_j) = 1$ for all $j \in \{1, \ldots, n\}$. Define the vector $z := x_1 + x_2 - \lambda_1 y_4$, so that

$$z = x_1 + x_2 - \lambda_1 y_4 = \lambda_1(y_1 - y_4) + x_2, \qquad x - z = x_3 + \lambda_1 y_4.$$

It follows that $z, x - z \in T_2(n, m; q)$, since they are sum of at most two vectors of rank 1 as $y_1 - y_4 \in \mathbb{F}_q^n$, and therefore $z \in X$ by Lemma 30. Note that we can re-write x_4 as

$$x_4 = \lambda_4 y_4 = \lambda_1^{-1} \lambda_4 (y - z),$$

which is a linear combination of elements of X. Therefore $x_4 \in X$ as well. Analogously, one can prove that $x_5, \ldots, x_n \in X$, which in turn implies that $X = \mathbb{F}_{q^m}^n$. $\qquad\square$

Lemma 35. *Let $X \in \mathscr{L}_2(n, m; q) \setminus \{\mathbb{F}_{q^m}^n\}$. If X contains an element of rank 4, then X is not modular.*

Proof. Suppose that X has an element of rank 4, say x. By Lemma 33, there exist $x_1, x_2, x_3, x_4 \in \mathbb{F}_{q^m}^n$ of rank 1, linearly independent over $\mathbb{F}_{q^m}$, that sum to x. We examine two cases.

- Suppose that $x_j \in X$ for some $j \in \{1, 2, 3, 4\}$. We have that $x - x_j$ is an element of X of rank 3 and therefore X cannot be modular by Lemma 34.

- Suppose $x_1, x_2, x_3, x_4 \notin X$ and assume towards a contradiction that X is modular. Define $y := x_1 + x_2$ and note that $y, x - y \in T_2(n, m; q)$. Therefore $y \in X$ by Lemma 30. For all $j \in \{1, 2, 3, 4\}$, take $\lambda_j \in \mathbb{F}_{q^m} \setminus \{0\}$ and $y_j \in \mathbb{F}_q^n \setminus \{0\}$ such that $x_j = \lambda_j y_j$, and define

$$z_1 := x_1 + x_2 + \lambda_3 y_1, \qquad z_2 := x_3 + x_4 - \lambda_3 y_1, \qquad Y := \langle z_1, z_2 \rangle_{\mathbb{F}_{q^m}}.$$

  Observe that

$$z_1 = (\lambda_1 + \lambda_3) y_1 + x_2, \qquad z_2 = \lambda_3 (y_3 - y_1) + x_4.$$

  Since $y_1, x_2, y_3 - y_1$ and x_4 all have rank at most 1, we have $Y \in \mathscr{L}_2(n, m; q)$. We have $z_1 \notin X$, otherwise $z_1 - y = \lambda_3 y_1 \in X$ and hence $\lambda_1 y_1 = x_1 \in X$ (since X is a linear space), which is false by assumption. Since $x = z_1 + z_2 \in Y$ and Y has dimension at most 2, we have $X \wedge_n Y = \langle x \rangle_{\mathbb{F}_q}$. On the other hand, $x \notin T_2(n, m; q)$ because $\mathrm{rk}(x) = 4$, and therefore $X \wedge_2 Y = \langle 0 \rangle_{\mathbb{F}_q}$. This implies that X is not modular by Lemma 29. $\qquad \square$

We next characterize the modular elements of the lattice $\mathscr{L}_i(n, m; q)$ for $i \geqslant 3$. Again, the proofs of the following four lemmas heavily use the properties of the rank weight stated in Lemma 33. We start with two results that, technically, only require $i \geqslant 2$, but that we will need in the case $i \geqslant 3$ only.

Lemma 36. *Let $i \geqslant 2$, $j \in \{1, \ldots, i\}$, and let X be a modular element of $\mathscr{L}_i(n, m; q)$. Let $x_1, \ldots, x_{i+j} \in \mathbb{F}_{q^m}^n$ be of rank 1. Suppose that $x := x_1 + \cdots + x_{i+j} \in X$ and that $\mathrm{rk}(x) \geqslant i + 1$. Then $x_s - x_p \in X$ for all $s, p \in \{1, \ldots, i + j\}$.*

Proof. The result is clear if $s = p$. We henceforth assume $s \neq p$, say $(s, p) = (1, 2)$ without loss of generality. Define $y := x_1 + x_3 + \cdots + x_{i+1}$ and $z := x_2 + x_3 + \cdots + x_{i+1}$. Observe that $y, z \in X$ by Lemma 30, since $x \in X \setminus T_i(n, m; q)$ and $z, y, x - y, x - z \in T_i(n, m; q)$, as they are sum of at most i vectors of rank 1 (we are using $j \leqslant i$ here). Finally, we have that $y - z = x_1 - x_2 \in X$ because it is sum of elements of X. $\qquad \square$

Lemma 37. *Let $i \geqslant 2$ and let X be a modular element of $\mathscr{L}_i(n, m; q)$. If X contains an element of rank strictly bigger than i, then it must contain an element of rank either $i + 1$ or $i + 2$.*

Proof. Since X contains an element of rank strictly bigger than i and the sum of two vectors of rank $\leqslant i$ has rank $\leqslant 2i$, X must contain an element x of rank $i + j$, for some $1 \leqslant j \leqslant i$. If $j \in \{1, 2\}$ then we are done. Now suppose $j \geqslant 3$ and write $x = x_1 + \cdots + x_{i+j}$, where $x_1, \ldots x_{i+j} \in \mathbb{F}_{q^m}^n$ have rank 1 and are linearly independent over $\mathbb{F}_{q^m}$. Let $y := x_1 + \cdots + x_i$ and observe $y, x - y \in T_i(n, m; q)$ by Lemma 33. Therefore by Lemma 30 we have that $y \in X$. Let $z_1 := x_{i+1} - x_{i+3}$ and $z_2 := x_{i+2} - x_{i+3}$. By Lemma 36 we have $z_1, z_2 \in X$, since X is modular. Now observe that

$$z := y + z_1 + z_2 = x_1 + \cdots + x_i + x_{i+1} + x_{i+2} - 2x_{i+3}$$

has rank $i + 1$, $i + 2$, or $i + 3$, since by Proposition 16 we have

$$i + 1 = \mathrm{rk}(x_1 + \cdots + x_{i+2}) - \mathrm{rk}(2x_{i+3}) \leqslant \mathrm{rk}(z) \leqslant i + 3,$$

where the last inequality from the fact that z is a sum of at most $i + 3$ vectors of rank 1. If z has rank $i + 1$ or $i + 2$ then we are done. If z has rank $i + 3$, then $y + z_1 \in X$ must have rank $i + 1$ or $i + 2$, since z_2 has rank 1 or 2 (we are using the triangular inequality again). Therefore in any case we have exhibited a vector of rank $i + 1$ or $i + 2$. $\square$

In the proofs of the following two lemmas we need the assumption $i \geqslant 3$. For completeness of the exposition we will stress when the assumption is technically used.

Lemma 38. *Let $i \geqslant 3$ and let X be a modular element of $\mathscr{L}_i(n, m; q)$. If X contains an element of rank $i + 2$, then it contains an element of rank $i + 1$.*

Proof. Let $x \in X$ be of rank $i + 2$ and write $x := x_1 + \cdots + x_{i+2}$ for some rank-1 elements $x_1, \ldots, x_{i+2} \in \mathbb{F}_{q^m}^n$ that are linearly independent over $\mathbb{F}_{q^m}$. Define $y := x_1 + \cdots + x_i$ and $z := x_1 + \cdots + x_{i-1}$. Notice that $y, z, x - y, x - z \in T_i(n, m; q)$ by Lemma 33 (here we use $i \geqslant 3$). Therefore, by Lemma 30, $y, z, x - y$ and $x - z$ are elements of X. Finally, we have that $x - y + z = x_1 + \cdots + x_{i-1} + x_{i+1} + x_{i+2}$ is an element of X of rank $i + 1$ by Lemma 33. $\square$

Lemma 39. *Let $i \geqslant 3$ and let X be a modular element of $\mathscr{L}_i(n, m; q)$. If X contains an element of rank $i + 1$, then $X = \mathbb{F}_{q^m}^n$.*

Proof. Suppose that X contains an element of rank $i + 1$, say x. Write $x = x_1 + \cdots + x_{i+1}$ for some $x_1, \ldots, x_{i+1} \in \mathbb{F}_{q^m}^n$ of rank 1 and linearly independent over $\mathbb{F}_{q^m}$. Note that for all $j \in \{1, \ldots, i + 1\}$ we have $x - x_j \in T_i(n, m; q)$. Therefore by Lemma 30 we have $x_j \in X$ for all j. We now complete $\{x_1, \ldots, x_{i+1}\}$ to a basis of $\mathbb{F}_{q^m}^n$ by selecting vectors $x_{i+2}, \ldots, x_n \in \mathbb{F}_{q^m}^n$ of rank 1 (this is always possible because the rank-1 vectors of $\mathbb{F}_{q^m}^n$ span $\mathbb{F}_{q^m}^n$). Thus $\langle x_1, \ldots, x_{i+1}, x_{i+2}, \ldots, x_n \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^n$. For $s \in \{i + 2, \ldots, n\}$, define the vector $z_s := x_1 + x_2 - x_s$ and notice that $z_s, x - z_s \in T_i(n, m; q)$ by construction (here is where the assumption $i \geqslant 3$ is technically needed). Lemma 30 implies that $z_s \in X$ and therefore $x_s \in X$, for all $s \in \{i + 2, \ldots, n\}$, since $x_1, x_2 \in X$ by the first part of the proof and X is a linear space. It follows that X contains a basis for $\mathbb{F}_{q^m}^n$ and therefore $X = \mathbb{F}_{q^m}^n$, as claimed. $\square$

We can finally characterize the modular elements of any lattice $\mathscr{L}_i(n, m; q)$ for $2 \leqslant i \leqslant n$. The following is the analogue of [9, Theorem 1.3]. Note that in the rank-metric context (and in sharp contrast to the Hamming-metric case) it also holds for $i = 2$.

Theorem 40. *For all $i \geqslant 2$, the modular elements of $\mathscr{L}_i(n, m; q)$ are the elements of the set $\{X \leqslant \mathbb{F}_{q^m}^n : X \subseteq T_i(n, m; q)\} \cup \{\mathbb{F}_{q^m}^n\}$.*

Proof. First of all we note that if $X \subseteq T_i(n, m; q)$, then $X \wedge_i Y \in \mathscr{L}_i(n, m; q)$ and therefore $X \wedge_i Y = X \wedge_n Y$, for all $Y \in \mathscr{L}_i(n, m; q)$. It follows that X is modular in $\mathscr{L}_i(n, m; q)$ by Lemma 29. Moreover, $\mathbb{F}_{q^m}^n$ is trivially modular.

In order to prove the other implication, suppose that X is a modular element of $\mathscr{L}_i(n, m; q)$ that contains a vector of rank strictly greater than i. By combining Lemmas 34 and 35 in the case $i = 2$ and Lemmas 37, 38 and 39 in the case $i \geqslant 3$, we conclude that $X = \mathbb{F}_{q^m}^n$. This establishes the theorem. $\qquad \square$

We are finally ready to establish Theorem 27.

Proof of Theorem 27. The supersolvability of the lattice $\mathscr{L}_1(n, m; q)$ immediately follows from the fact that $\mathscr{L}_1(n, m; q)$ is a modular lattice by Proposition 31. We assume $i \geqslant 2$ in the remainder of the proof. Let $\{e_1, \ldots, e_n\}$ be the canonical basis of $\mathbb{F}_{q^m}^n$. Consider the following maximal chain in $\mathscr{L}_i(n, m; q)$:

$$\langle 0 \rangle_{\mathbb{F}_{q^m}} \lessdot \langle e_1 \rangle_{\mathbb{F}_{q^m}} \lessdot \langle e_1, e_2 \rangle_{\mathbb{F}_{q^m}} \lessdot \cdots \lessdot \langle e_1, e_2, \ldots, e_n \rangle_{\mathbb{F}_{q^m}}. \tag{3}$$

For $1 \leqslant k \leqslant n$, all the elements of $\langle e_1, e_2, \ldots, e_k \rangle_{\mathbb{F}_{q^m}}$ have rank at most k by the triangular inequality. Moreover, Theorem 40 implies that if $i \in \{n-1, n\}$ or $m \in \{2, \ldots, i\}$, then all the element of the chain in (3) are modular. This shows that, by definition, $\mathscr{L}_i(n, m; q)$ is supersolvable in those cases.

We conclude the proof by showing that $\mathscr{L}_i(n, m; q)$ cannot be supersolvable if $m \geqslant i+1$ and $i \in \{2, \ldots, n-2\}$. We will do this by showing a much stronger fact: All the elements of $\mathscr{L}_i(n, m; q)$ of rank (i.e., dimension) $i + 1$ cannot be modular. To see this, let $X \in \mathscr{L}_i(n, m; q)$ have dimension $i + 1$ and let $G \leqslant \mathbb{F}_{q^m}^{(i+1) \times n}$ be the full-rank matrix in reduced row-echelon form whose rows are a basis for X. Let $\Gamma := \{\gamma_1, \ldots, \gamma_{i+1}\}$ be $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^m}$ (they exist because $m \geqslant i + 1$). One can easily check that $\sum_{s=1}^{i+1} \gamma_s G_s$ has rank at least $i + 1$. Therefore X cannot be modular by Theorem 40. $\qquad \square$

Table 1 illustrates Theorem 27 visually. For a fixed $n \geqslant 3$, it shows the "supersolvability region" of $\mathscr{L}_i(n, m; q)$.

		m						
		2	3	4	$\cdots$	j	$j+1$	$\cdots$
i	1	■	■	■	■	■	■	■
	2	■						
	3	■	■					
	$\vdots$	■	■	■				
	j	■	■	■	■	■		
	$\vdots$	■	■	■	■	■	■	
	$n-1$	■	■	■	■	■	■	■
	n	■	■	■	■	■	■	■

Table 1: The "region" of supersolvable rank-metric lattices for $n \geqslant 3$.

5 The Characteristic Polynomial of $\mathscr{L}_i(n,m;q)$

In this section we derive explicit formulas for the Whitney numbers of the first and second kind of some rank-metric lattices, including the supersolvable ones we characterized in Theorem 27. We also compute the *critical exponent* (defined later) of rank-metric lattices for some parameter sets. We start with the case $i = 1$.

Proposition 41. *The following hold.*

(1) $w_j(1,n,m;q) = (-1)^j q^{\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_q$ *for all* $j \in \{0,\dots,n\}$.

(2) $W_j(1,n,m;q) = \begin{bmatrix} n \\ j \end{bmatrix}_q$ *for all* $j \in \{0,\dots,n\}$.

(3) $\chi(\mathscr{L}_1(n,m;q);\lambda) = \sum_{j=0}^{n} (-1)^j q^{\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_q \lambda^{n-j} = \prod_{j=0}^{n-1}(\lambda - q^j).$

Proof. The first two formulas follow from Proposition 31 and the definitions of Whitney numbers of the first and second kind. The third formula follows from the definition of characteristic polynomial and Lemma 25. $\square$

We now treat the case $i = n$. The following result easily follows from the definitions and its proof is therefore omitted.

Proposition 42. *The following hold.*

(1) $w_j(n,n,m;q) = (-1)^j q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m}$ *for all* $j \in \{0,\dots,n\}$.

(2) $W_j(n,n,m;q) = \begin{bmatrix} n \\ j \end{bmatrix}_{q^m}$ *for all* $j \in \{0,\dots,n\}$.

(3) $\chi(\mathscr{L}_n(n,m;q);\lambda) = \sum_{j=0}^{n} (-1)^j q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m} \lambda^{n-j} = \prod_{j=0}^{n-1}(\lambda - q^{mj}).$

It is interesting to observe the very close "structural" analogy between Propositions 41 and 42, where the only difference is the presence of the factor m.

Since the rank of a vector $v \in \mathbb{F}_{q^m}^n$ cannot exceed m, the next result follows from Proposition 42.

Corollary 43. *Suppose that* $m \in \{2,\dots,i\}$. *The following hold.*

(1) $w_j(i,n,m;q) = (-1)^j q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m}$ *for all* $j \in \{0,\dots,n\}$.

(2) $W_j(i, n, m; q) = \begin{bmatrix} n \\ j \end{bmatrix}_{q^m}$ for all $j \in \{0, \ldots, n\}$.

(3) $\chi(\mathscr{L}_i(n, m; q); \lambda) = \sum_{j=0}^{n} (-1)^j q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m} \lambda^{n-j} = \prod_{j=0}^{n-1} (\lambda - q^{mj})$.

In the next result we study the case $i = n - 1$ under the assumption that $m \geqslant n$. We will use Stanley's modular factorization theorem.

Theorem 44. *If $n \leqslant m$, then*

$$\chi(\mathscr{L}_{n-1}(n, m; q); \lambda) = \left(\lambda - q^{(n-1)m} + \prod_{s=1}^{n-1} (q^m - q^s) \right) \prod_{j=0}^{n-2} (\lambda - q^{mj}).$$

Proof. By Corollary 13 and the proof of Theorem 27, we have

$\chi(\mathscr{L}_{n-1}(n, m; q); \lambda)$

$= \prod_{j=1}^{n} \left(\lambda - \left| \left\{ A \in \mathrm{At}(\mathscr{L}_i(n, m; q)) : A \leqslant \langle e_1, \ldots, e_j \rangle_{\mathbb{F}_{q^m}}, A \not\leqslant \langle e_1, \ldots, e_{j-1} \rangle_{\mathbb{F}_{q^m}} \right\} \right| \right)$, (4)

where we set the span over $\mathbb{F}_{q^m}$ of the empty set to be $\{0\}$. Therefore it remains to compute the quantities

$$a_j := \left| \left\{ A \in \mathrm{At}(\mathscr{L}_{n-1}(n, m; q)) : A \leqslant \langle e_1, \ldots, e_j \rangle_{\mathbb{F}_{q^m}}, A \not\leqslant \langle e_1, \ldots, e_{j-1} \rangle_{\mathbb{F}_{q^m}} \right\} \right|$$

for $j \in \{1, \ldots, n\}$. Observe that the atoms of $\mathscr{L}_i(n, m, q)$ below $\langle e_1, \ldots, e_j \rangle_{\mathbb{F}_{q^m}}$ but not below $\langle e_1, \ldots, e_{j-1} \rangle_{\mathbb{F}_{q^m}}$ are the 1-dimensional subspace of $\mathbb{F}_{q^m}^n$ generated by a vector of the form $(\star, \cdots, \star, 1, 0, \cdots, 0)$, where the 1 is in position j and the $\star$'s are arbitrary elements of $\mathbb{F}_{q^m}$. It follows that $a_j = q^{(j-1)m}$, for all $j \in \{1, \ldots, n-1\}$. Moreover,

$$a_n = q^{(n-1)m} - \left| \left\{ \langle x \rangle_{\mathbb{F}_{q^m}} \leqslant \mathbb{F}_{q^m}^n : \mathrm{rk}(x) = n \right\} \right| = q^{(n-1)m} - \prod_{s=1}^{n-1} (q^m - q^s).$$

Substituting these expressions into (4) gives the desired result. $\qquad \square$

We now extract from Theorem 44 some more explicit information about the Whitney numbers of $\mathscr{L}_{n-1}(n, m; q)$.

Corollary 45. *The following hold for $n \leqslant m$.*

(1) $w_0(n - 1, n, m; q) = 1$.

(2) $w_j(n - 1, n, m; q) = (-1)^j \left(q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m} - q^{m\binom{j-1}{2}} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix}_{q^m} \prod_{s=1}^{n-1} (q^m - q^s) \right)$ *for all* $j \in \{1, \ldots, n\}$.

(3) $W_0(n-1, n, m; q) = 1.$

(4) $W_1(n-1, n, m; q) = \begin{bmatrix} n \\ 1 \end{bmatrix}_{q^m} - \prod_{s=1}^{n-1}(q^m - q^s).$

(5) $W_j(n-1, n, m; q) = \begin{bmatrix} n \\ j \end{bmatrix}_{q^m}$ *for all* $j \in \{2, \ldots, n\}.$

Proof. Parts (1) and (3) follow from the definitions. Part (2) follows from Theorem 44, since by Lemma 25 we have

$$\chi(\mathscr{L}_{n-1}(n, m; q); \lambda)$$
$$= \prod_{j=0}^{n-1}(\lambda - q^{mj}) + \prod_{s=1}^{n-1}(q^m - q^s) \prod_{j=0}^{n-2}(\lambda - q^{mj})$$
$$= \sum_{j=0}^{n}(-1)^j q^{m\binom{j}{2}} \begin{bmatrix} n \\ j \end{bmatrix}_{q^m} \lambda^{n-j} + \prod_{s=1}^{n-1}(q^m - q^s) \sum_{j=1}^{n}(-1)^{j-1} q^{m\binom{j-1}{2}} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix}_{q^m} \lambda^{n-j}.$$

By the definition of Whitney numbers of the second kind we have

$$W_1(n-1, n, m; q) = \begin{bmatrix} n \\ 1 \end{bmatrix}_{q^m} - \left| \left\{ \langle x \rangle_{\mathbb{F}_{q^m}} \leqslant \mathbb{F}_{q^m}^n : \mathrm{rk}(x) = n \right\} \right|,$$

which implies (4). Finally, (5) follows from the observation that any subspace of $\mathbb{F}_{q^m}^n$ of dimension $j \geqslant 2$ has a basis of vectors of rank $\leqslant n - 1$. To see this, let $X \leqslant \mathbb{F}_{q^m}^n$ be of dimension $j \in \{2, \ldots, n\}$ and let $G \in \mathbb{F}_{q^m}^{j \times n}$ be the matrix in reduced row-echelon form whose rows form a basis of X. Every row of X has at least $j - 1$ zeroes. Therefore its rank is at most $n - j + 1 \geqslant n - 1$. $\square$

The following result is the q-analogue of [9, Theorem 3.3]. It computes some of the roots of the characteristic polynomial of rank-metric lattices, which is a standard question in lattice theory.

Proposition 46. *For all $i \in \{1, \ldots, n\}$, the characteristic polynomial of $\mathscr{L}_i(n, m; q)$ has the integers $1, q^m, \ldots, q^{(i-1)m}$ among its roots.*

Proof. Let $U_i := \langle e_1, \ldots, e_i \rangle_{\mathbb{F}_{q^m}}$. All the elements of U_i have rank less or equal than i. Therefore U_i is a modular element of $\mathscr{L}_i(n, m; q)$ by Theorem 40. As an application of Theorem 12 we obtain

$$\chi(\mathscr{L}_i(n, m; q); \lambda) = \chi([0, U_i]; \lambda) \sum_{\substack{X \in \mathscr{L}_i(n, m; q) \\ X \wedge U_i = 0}} \mu(0, X) \, \lambda^{n-i-\dim(X)}, \tag{5}$$

where μ is the Möbius function of $\mathscr{L}_i(n, m; q)$. The desired result now follows from the fact that the interval $[0, U_i]$ is the lattice of subspaces of U_i, whose characteristic polynomial

is

$$\chi([0, U_i]; \lambda) = \prod_{s=0}^{i-1} (\lambda - q^{sm});$$

see e.g. [37]. Combining this with (5) concludes the proof. □

The following example shows that converse of Corollary 13 does not hold in general. Recall that, by Proposition 31, the rank-metric lattice $\mathscr{L}_2(n, m; q)$ is *not* supersolvable.

Example 47. Let $q = 2$, $n = 4$, and $m = 3$. We have $\alpha_0(2, 4, 3; 2) = 1$. Observe that the maximum rank of an element of $\mathbb{F}_{2^3}^4$ is 3 and that

$$\alpha_1(2, 4, 3; 2) = \left| \left\{ \langle v \rangle_{\mathbb{F}_{2^3}} : v \in \mathbb{F}_{2^3}^4, \, \mathrm{rk}(v) = 3 \right\} \right| = \begin{bmatrix} 4 \\ 3 \end{bmatrix}_2 (2^3 - 2)(2^3 - 2^2) = 360.$$

We also have

$$\alpha_2(2, 4, 3; 2) = \left| \left\{ C \leqslant \mathbb{F}_{2^3}^4 : \dim(C) = 2, \, d(C) \geqslant 3 \right\} \right|.$$

On the other hand, by the rank-metric Singleton bound of Theorem 24 we have $6 \leqslant 4(3 - d + 1)$ for any 2-dimensional code of $\mathbb{F}_{2^3}^4$ of minimum distance d. This implies $d \leqslant 2$ and therefore $\alpha_2(2, 4, 3; 2) = 0$. A similar argument using again the rank-metric Singleton bound of Theorem 24 shows that $\alpha_3(2, 4, 3; 2) = \alpha_4(2, 4, 3; 2) = 0$. Finally, by applying Theorem 23 we obtain

$$(w_j(2, 4, 3; 2) : j \in \{0, \dots, 4\}) = (1, -225, 11680, -89280, 77824).$$

Therefore, by definition, we have $\chi(\mathscr{L}_2(4, 3; 2); \lambda) = \lambda^4 - 225\lambda^3 + 11680\lambda^2 - 89280\lambda + 77824$, whose factorization is $(\lambda - 1)(\lambda - 8)(\lambda - 64)(\lambda - 152)$. However, $\mathscr{L}_2(4, 3; 2)$ is not supersolvable by Theorem 27.

Remark 48. The linear factor $\lambda - 64 = \lambda - 2^{2 \cdot 3}$ in the previous example might suggest that the characteristic polynomial of $\mathscr{L}_2(4, 3; 2)$ can be computed as in the proof of Theorem 44 via the chain

$$0 \lessdot \langle e_1 \rangle_{\mathbb{F}_{2^3}} \lessdot \langle e_1, e_2 \rangle_{\mathbb{F}_{2^3}} \lessdot \langle e_1, e_2, e_3 \rangle_{\mathbb{F}_{2^3}} \lessdot \mathbb{F}_{2^3}^4.$$

However, the proof of Lemma 34 shows that $\langle e_1, e_2, e_3 \rangle_{\mathbb{F}_{2^3}}$ is not modular. To see this in a more direct way, let $1, \alpha, \beta \in \mathbb{F}_{2^3}$ be linearly independent over $\mathbb{F}_2$. Define $x = e_1 + \alpha e_2 + \beta e_3$ and $z = e_1 + e_4 + \alpha e_2$. Let $U = \langle z, x + z \rangle_{\mathbb{F}_{2^3}}$. It is easy to check that $X \in \mathscr{L}_2(4, 3; 2)$. Moreover, $\langle e_1, e_2, e_3 \rangle_{\mathbb{F}_{2^3}} \cap U = \langle x \rangle$, because $z \in U \setminus \langle e_1, e_2, e_3 \rangle_{\mathbb{F}_{2^3}}$. This contradicts the definition of modularity for $\langle e_1, e_2, e_3 \rangle_{\mathbb{F}_{2^3}}$.

We now turn to the *critical exponent* of rank-metric lattices, which is one of the most important invariant of a combinatorial geometry. It was defined by Crapo and Rota in [17] and it measures the largest dimension of a linear space that *distinguishes*, i.e., avoids, a given collection of projective points. Computing the critical exponent of a combinatorial geometry is a hard problem in general, known under the name of *Critical Problem*; see [17].

In this paper, we give the definition of critical exponent directly in the context of rank-metric lattices.

Definition 49. The **critical exponent** of $\mathscr{L}_i(n, m; q)$ is

$$\mathrm{crit}(\mathscr{L}_i(n, m; q)) = n - \max\{k \in \mathbb{Z}_{\geqslant 0} : \alpha_k(i, n, m; q) \neq 0\},$$

where $\alpha_k(i, n, m; q)$ is defined in Notation 21.

In the next result we explicitly compute the value of the critical exponent for some parameter sets.

Theorem 50. *(1) If $n \leqslant m$, then $\mathrm{crit}(\mathscr{L}_i(n, m; q)) = i$.*

(2) If $n > m$, then $\mathrm{crit}(\mathscr{L}_i(n, m; q)) \geqslant ni/m$. Furthermore, $\mathrm{crit}(\mathscr{L}_i(n, m; q)) = ni/m$ if $m \mid ni$ and one of the following holds:

(a) $n = tm$ and $i = m - k$ for some nonnegative integers t, k;

(b) $n = mk/2$ for some nonnegative integer k, m even, and $i \in \{2, m - 2\}$;

(c) $n = 8$, $m = 6$, $i = 3$ and $q = 2^h$ with $h \equiv 1 \mod 6$;

(d) $n = 8$, $m = 4$, $i = 3$ and $q = 2^h$ for some odd nonnegative integer h.

Proof. We start observing that, by definition, we have

$$\max\{k \in \mathbb{Z}_{>0} : \alpha_k(i, n, m; q) \neq 0\}$$
$$= \max\{k \in \mathbb{Z}_{>0} : \exists C \leqslant \mathbb{F}_{q^m}^n \text{ s.t. } \dim(C) = k \text{ and } d(C) \geqslant i + 1\}$$
$$\leqslant \frac{\max\{n, m\}(\min\{n, m\} - i)}{m},$$

where the latter inequality follows from the rank-metric Singleton bound; see Theorem 24. Therefore, by the definition of critical exponent, we have

$$\mathrm{crit}(\mathscr{L}_i(n, m; q)) \geqslant n - \frac{\max\{n, m\}(\min\{n, m\} - i)}{m}, \tag{6}$$

where we have equality in (6) if and only if there exists a code $C \leqslant \mathbb{F}_{q^m}^n$ of dimension $\max\{n, m\}(\min\{n, m\} - i)/m$ and minimum distance at least $i + 1$. Again by the rank-metric Singleton bound (Theorem 24), this happens if and only if there exists a code $C \leqslant \mathbb{F}_{q^m}^n$ of dimension $\max\{n, m\}(\min\{n, m\} - i)/m$ and minimum distance exactly $i + 1$. In the remainder of the proof we describe some parameter sets for which the existence of such a code has been established.

If $m \geqslant n$ then the existence of a code $C \leqslant \mathbb{F}_{q^m}^n$ of dimension $n - i$ and minimum distance $i + 1$ has been established by Delsarte [20] for all i. If $m < n$, the existence is only known for some parameters, which have been conveniently collected in [30, Remark 2.3] and to which we refer (see also [4, 18, 5]). These correspond precisely to the parameters listed in the statement. $\square$

By combining Theorem 50 with [33, Corollary 3.4], we obtain a recursion for the Whitney numbers of the first kind of $\mathscr{L}_i(n, m; q)$ in some parameter ranges.

Proposition 51. *Let $j \in \{0, \ldots, n\}$. We have*

$$w_j(i, n, m; q) = -\sum_{s=0}^{j-1} w_s(i, n, m; q) \begin{bmatrix} n - s \\ j - s \end{bmatrix}_{q^m} \tag{7}$$

if $n \leqslant m$ and $n - i < j$, or if $n > m$ and $n(m - i)/m < j$.

6 On the Whitney Numbers of $\mathscr{L}_2(4, 4; q)$

In this section we concentrate on some "small" non-supersolvable rank-metric lattices whose characteristic polynomials we cannot compute by applying the results of Section 5, namely, lattices of the form $\mathscr{L}_2(4, 4; q)$. We give explicit formulas for their characteristic polynomials, *under the assumption* that their second Whitney numbers of the first kind are a polynomial in q. This technical assumption will allow us to follow a computational approach based on rank-metric codes, Theorem 23, and Lagrange interpolation.

Notation 52. In this section, $n = m = 4$. We denote by $M(q)$ the number of 2-dimensional MRD codes $C \leqslant \mathbb{F}_{q^4}^4$ to simplify the notation.

We start by observing the following.

Proposition 53. *We have:*

(1) $w_2(2, 4, 4; q) = q^4 \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q^4} - \begin{bmatrix} 3 \\ 1 \end{bmatrix}_{q^4} \sum_{j=3}^{4} \begin{bmatrix} 4 \\ j \end{bmatrix}_q \prod_{s=1}^{j-1} (q^4 - q^s) + M(q);$

(2) $W_2(2, 4, 4; q) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q^4} - M(q).$

Moreover, $w_2(2, 4, 4; q)$ is a polynomial in q if and only if $M(q)$ is a polynomial in q.

Proof. By Theorem 23, we have

$$w_2(2, 4, 4; q) = \sum_{k=0}^{2} \alpha_k(2, 4, 4; q) \begin{bmatrix} 4 - k \\ 2 - k \end{bmatrix}_{q^4} (-1)^{2-k} q^{4\binom{2-k}{2}}. \tag{8}$$

Furthermore:

- $\alpha_0(2, 4, 4; q) = 1$;

- $\alpha_1(2, 4, 4; q) = \sum_{j=3}^{4} \begin{bmatrix} 4 \\ j \end{bmatrix}_q \prod_{s=1}^{j-1} (q^4 - q^s)$;

- $\alpha_2(2, 4, 4; q) = M(q)$.

These expressions combined with (8) give the first part of the statement. For the second part, note that by Theorem 24 we have $d(C) \leqslant 3$ for all $C \leqslant \mathbb{F}_{q^4}^4$ of dimension 2. Therefore

$$W_2(2,4,4;q) = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q^4} - |\{C \leqslant \mathbb{F}_{q^4}^4 : d(C) > 2\}| = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q^4} - M(q).$$

The last part of the statement follows from Theorem 23 and the fact that $\alpha_3(2,4,4;q) = \alpha_4(2,4,4;q) = 0$ by Theorem 24. $\qquad\square$

The following observation will be crucial in our approach.

Lemma 54. *Let* $u, v \in \mathbb{F}_{2^4}^4$ *be vectors of rank 4. The number of 2-dimensional MRD codes* $C \leqslant \mathbb{F}_{2^4}^4$ *containing* u *is the same as the number of 2-dimensional MRD codes* $C \leqslant \mathbb{F}_{2^4}^4$ *containing* v.

Proof. Since the entries of u and v both span $\mathbb{F}_{q^4}$ over $\mathbb{F}_2$, for all $j \in \{1, \ldots, i\}$ there exist $a_{1,j}, \ldots a_{4,j} \in \mathbb{F}_2$ with $v_j = \sum_{i=1}^{4} u_i a_{i,j}$. Let A be the matrix whose (i,j) entry is $a_{i,j}$. Then A has size 4×4 and invertible. Moreover, $v = u \cdot A$. Therefore the mapping $\mathbb{F}_{q^4}^4 \to \mathbb{F}_{q^4}^4$ given by $x \mapsto x \cdot A$ is rank-preserving and thus induces a bijection between the 2-dimensional MRD codes $C \leqslant \mathbb{F}_{q^4}^4$ containing u and the 2-dimensional MRD codes $C \leqslant \mathbb{F}_{q^4}^4$ containing v. This establishes the lemma. $\qquad\square$

Notation 55. We let $\hat{M}(q)$ be the quantity defined by the previous lemma, that is, $\hat{M}(q)$ is the number of 2-dimensional MRD codes in $\mathbb{F}_{q^4}^4$ containing a *given* vector of rank 4.

The quantities $M(q)$ and $\hat{M}(q)$ are closely connected to each other, as the following result shows.

Proposition 56. *We have*

$$\hat{M}(q) = \frac{M(q)(q^3 - q^2 - q - 1)}{q^5(q-1)^3(q+1)(q^2+q+1)}.$$

Proof. We count the elements of the set

$$\Sigma := \{(C, v) : C \leqslant \mathbb{F}_{q^4}^4 \text{ is MRD}, \dim(C) = 2, v \in \mathbb{F}_{q^4}^4, \text{rk}(v) = 2\} \qquad (9)$$

in two ways. Since the number of rank-4 vectors in $\mathbb{F}_{q^4}^4$ is $(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3)$, by Lemma 54 we have

$$|\Sigma| = \hat{M}(q)(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3). \qquad (10)$$

Now fix a 2-dimensional MRD code C in $\mathbb{F}_{2^4}^4$ and recall for every such C the number of rank-4 vectors $v \in C$ is the same and is computed, for example, in [19, Corollary 28]. Therefore,

$$|\Sigma| = M(q)\left(q^8 - 1 - \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q (q^4-1)\right)$$
$$= M(q)\, q\,(q-1)\,(q+1)\,(q^2+1)\,(q^3-q^2-q-1). \qquad (11)$$

The statement follows from comparing (10) with (11). $\qquad\square$

We now start working under the assumption that $w_2(2, 4, 3; q)$ is a polynomial in q. By Proposition 53, this is equivalent to assuming that $M(q)$ is a polynomial in q.

The values of $\hat{M}(q)$ for some small values of q (we managed up to $q = 9$) can be computed using algebra software combined with an argument that we outline very briefly. We let α be a primitive element of $\mathbb{F}_{q^4}$ and $v := (1, \alpha, \alpha^2, \alpha^3)$ be a vector of rank 4. Then $\hat{M}(q)$ is the number of 2-dimensional MRD codes $C \leqslant \mathbb{F}_{q^4}^4$ containing v. We consider the code whose generator matrix is

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & A & B \end{pmatrix}$$

for some $A, B \in \mathbb{F}_{q^4}^4$ such that $\{1, A, B\}$ is a set of elements that are linearly independent over $\mathbb{F}_q$. Observe that the matrices

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & A & B \end{pmatrix}, \qquad \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & A' & B' \end{pmatrix}$$

generate the same code if and only if $A = A'$ and $B = B'$. Therefore to compute $\hat{M}(q)$ it suffices to count all the pairs (A, B) such that, for all non-zero $\gamma \in \mathbb{F}_{q^4}$,

$$(1, \alpha, \alpha^2, \alpha^3) + (0, \gamma, \gamma A, \gamma B)$$

has rank 3 or 4. This is equivalent to saying that, for all $i \in \{1, \dots, q^4 - 1\}$,

$$(1, \alpha, \alpha^2, \alpha^3) + \alpha^i(0, 1, A, B)$$

has rank 3 or 4. Using the matrix representation of vectors one can finally show that $\hat{M}(q)$ is the number of $(A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4) \in \mathbb{F}_q^8$ such that

$$I + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ A_1 & A_2 & A_3 & A_4 \\ B_1 & B_2 & B_3 & B_4 \end{pmatrix} \cdot M^i$$

has rank 3 or 4 for all $i \in \{1, \dots, q^4 - 1\}$, where M is the companion matrix of minimal polynomial of α over $\mathbb{F}_q$. By combining this computational approach with Proposition 56 we obtain the following result.

Lemma 57. *The values of $M(q)$ for $q \in \{2, 3, 4, 5, 7, 8\}$ are the following:*

- $M(2) = 1344$,
- $M(3) = 6368544$,
- $M(4) = 998645760$,
- $M(5) = 43710000000$,
- $M(7) = 11599543859904$,

- $M(8) = 103734668427264.$

Our next step is to use the previous values to interpolate $M(q)$ under the polynomiality assumption. The putative degree of $M(q)$ is too large (up to 16, as we will explain later) for this to be possible. We therefore proceed by constructing a polynomial of smaller degree which we can interpolate with the values computed in Lemma 57. We start by recalling the following folklore result from elementary algebra.

Lemma 58. *Let $P(x), Q(x) \in \mathbb{Z}[x]$ be polynomials. If $|\{a \in \mathbb{Z} \mid P(a)/Q(a) \in \mathbb{Z}\}| = +\infty$, then $Q(x)$ divides $P(x)$ in $\mathbb{Z}[x]$.*

By combining Lemma 58 with Proposition 56, we deduce that if $M(q)$ is a polynomial in q, then $\hat{M}(q)$ is a polynomial in q as well. Under these assumptions, write

$$M(q) = \frac{\hat{M}(q)\, q^5 (q-1)^3 (q+1)(q^2+q+1)}{q^3 - q^2 - q - 1}$$

and observe that $q^5(q^3-1)(q^2-1)(q-1)$ and $q^3 - q^2 - q - 1$ are coprime in $\mathbb{Z}[q]$, which implies that $q^3 - q^2 - q - 1$ divides $\hat{M}(q)$ as a polynomial. Therefore we may write $\hat{M}(q) = Z(q)(q^3 - q^2 - q - 1)$, for some $Z(q) \in \mathbb{Z}[q]$ of degree at most 5. The bound on the degree follows from the fact that

$$M(q) \leqslant \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q^4} = q^{16} + \text{lower order terms in } q,$$

which gives $\deg(M(q)) \leqslant 16$ and thus $\deg(\hat{M}(q)) \leqslant 8$. By definition, we have

$$Z(q) = \frac{M(q)}{q^5(q^3-1)(q^2-1)(q-1)}.$$

Since $Z(q)$ has degree at most 5, it can be interpolated using the 6 values for $M(q)$ computed in Lemma 57. The passages are elementary and the final outcome is

$$Z(q) = \frac{1}{2}\,(q^5 - q^4 - q^3 - q^2),$$

which in turn gives

$$M(q) = \frac{1}{2}\, q^7 (q^3 - 1)(q^2 - 1)(q - 1)(q^3 - q^2 - q - 1). \tag{12}$$

Finally, by applying Proposition 53 and Theorem 24, after lengthy computations one obtains the following result.

Theorem 59. *If $w_2(2, 4, 4; q)$ is a polynomial in q, then*

$$w_0(2, 4, 4; q) = 1,$$
$$w_1(2, 4, 4; q) = -\left(q^8 + q^7 + 2q^6 - q^3 + 1\right),$$
$$w_2(2, 4, 4; q) = \frac{1}{2}\left(q^{16} + 3q^{14} + q^{13} + 3q^{12} + q^{11} + q^{10} - q^9 + q^7 + 4q^6 - 2q^3\right),$$
$$w_3(2, 4, 4; q) = -\frac{1}{2}\left(q^{20} + 3q^{18} + q^{17} + 2q^{16} - q^{15} + 3q^{12} + 2q^{11} + q^{10} - q^9 - 2q^8 - q^7\right),$$
$$w_4(2, 4, 4; q) = \frac{1}{2}\left(q^{20} + 3q^{18} + q^{17} + q^{16} - q^{15} - 3q^{14} - q^{13} + q^{11}\right).$$

In particular, we have

$$\chi(\mathscr{L}_2(4, 4; q); \lambda) = (\lambda - 1)(\lambda - q^4)\Bigg(\lambda^2 - (q^8 + q^7 + 2q^6 - q^4 - q^3)\lambda$$
$$+ \frac{1}{2}\left(q^{16} + 3q^{14} + q^{13} + q^{12} - q^{11} - 3q^{10} - q^9 + q^7\right)\Bigg).$$

Remark 60. It is interesting to observe that the final formula of Theorem 59 is compatible with the modularity of $\langle e_1, e_2 \rangle_{\mathbb{F}_{q^4}}$ in $\mathscr{L}_2(4, 4; q)$, which implies that $(\lambda - 1)(\lambda - q^4)$ is always a factor of $\chi(\mathscr{L}_2(4, 4; q); \lambda)$ by Theorem 12. We could also computationally obtain the value of $M(9)$ and it coincides with the prediction made by Equation (12).

As an application of Theorem 59, we compute the characteristic polynomial of $\mathscr{L}_2(4, 4; q)$ for some values of q, under the assumption that its second Whitney number of the first kind is a polynomial in q. The final results are summarized in Table 2.

q	$\chi(\mathscr{L}_2(4, 4; q); \lambda)$
2	$(\lambda - 1)(\lambda - 16)(\lambda^2 - 488\lambda + 60736)$
3	$(\lambda - 1)(\lambda - 81)(\lambda^2 - 10098\lambda + 29574801)$
4	$(\lambda - 1)(\lambda - 256)(\lambda^2 - 89792\lambda + 2588286976)$
5	$(\lambda - 1)(\lambda - 625)(\lambda^2 - 499250\lambda + 86141640625)$
7	$(\lambda - 1)(\lambda - 2401)(\lambda^2 - 6820898\lambda + 17687732901601)$
8	$(\lambda - 1)(\lambda - 4096)(\lambda^2 - 19394048\lambda + 147637824126976)$
9	$(\lambda - 1)(\lambda - 6561)(\lambda^2 - 48885282\lambda + 962216318765601)$

Table 2: The characteristic polynomial of $\mathscr{L}_2(4, 4; q)$, under the assumption that its second Whitney number of the first kind is a polynomial in q. We display the unique factorization of the putative polynomial.

7   Lattice-Rank Weights of Rank-Metric Codes

In this section we show an application of rank-metric lattices to coding theory. We introduce new structural invariants (sometimes called *distinguishers*) for rank-metric codes based on rank-metric lattices. We call these invariants *lattice-rank weights* and show that they extend the *generalized vector rank weights* introduced in [32]. In our approach, the elements of the rank-metric lattice $\mathscr{L}_i(n, m; q)$ play the same role that optimal anticodes play in [32]. In fact, the elements of $\mathscr{L}_1(n, m; q)$ are precisely the optimal anticodes of [32].

In the second part of this section we then define the notions of *lattice binomial moments* and *lattice rank weight distribution* that are naturally associated with the invariants we introduce. We derive derive the corresponding *MacWilliams-type identities* and discuss some families of rank-metric codes that are extremal with respect to these new notions.

Notation 61. Throughout this section we work with fixed $n, m \geqslant 2$, which we generally don't remember in the notation to improve readability. We also fix a code $C \leqslant \mathbb{F}_{q^m}^n$ of dimension k and minimum distance d. All dimensions are computed over $\mathbb{F}_{q^m}$, unless otherwise stated.

We recall the notion of equivalent codes.

Definition 62. We say that the code $C, D \leqslant \mathbb{F}_{q^m}^n$ are **equivalent** if there exists an $\mathbb{F}_{q^m}$-linear map $\varphi : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ such that $\mathrm{rk}(v) = \mathrm{rk}(\varphi(v))$ for all $v \in \mathbb{F}_{q^m}^n$ and $\varphi(C) = D$.

Studying the invariants of codes is a natural way of investigating their structure. Several invariants are particularly relevant for applications due to their property of distinguishing between inequivalent codes. The latter problem is central not only in coding theory but also in some related research areas. For example, code distinguishers provide an attack tool in code-based cryptography. We propose the following invariants.

Definition 63. For $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$, the (i, j)-**th lattice-rank weight** of C is the number

$$\ell_j^{(i)}(C) := \min\{\dim(X) : X \in \mathscr{L}_i(n, m; q), \dim(C \cap X) \geqslant j\}.$$

The (i, j)-**th dual lattice-rank weight** of C is the number

$$\hat{\ell}_j^{(i)}(C) := \min\{\dim(X^\perp) : X \in \mathscr{L}_i(n, m; q), \dim(C \cap X) \geqslant j\}.$$

Remark 64. If $i \in \{1, n\}$ or $m \in \{2, \ldots, i\}$, then the dual of an element of $\mathscr{L}_i(n, m; q)$ is still an element of $\mathscr{L}_i(n, m; q)$. However, this property does not hold in general. Examples can be easily found.

For ease of notation, we write $\ell_j^{(i)}$, $\ell_j^{(i)\perp}$, $\hat{\ell}_j^{(i)}$ and $\ell_j^{(i)\perp}$ instead of $\ell_j^{(i)}(C)$, $\ell_j^{(i)}(C^\perp)$, $\hat{\ell}_j^{(i)}(C)$ and $\hat{\ell}_j^{(i)}(C^\perp)$ respectively.

We also recall the following definition of generalized rank-weights proposed in [29] and later characterized via anticodes in [32].

Definition 65. For $j \in \{1, \dots, k\}$, the j-**th generalized rank weight** of C is

$$m_j(C) := \min\{\dim(A) : A \in \mathcal{A}, \dim(A \cap C) \geqslant j\},$$

where $\mathcal{A}$ denotes the set of $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$ that have a basis made of vectors with entries in $\mathbb{F}_q$.

Again, we write m_j instead of $m_j(C)$. We have the following result which, in particular, shows that the lattice rank weights extend the generalized rank weights as a code invariant.

Theorem 66. *The following hold.*

(1) $\ell_j^{(1)} = m_j$ *for all* $j \in \{1, \dots, k\}$.

(2) $\ell_1^{(i)} = \lceil \frac{d}{i} \rceil$ *for all* $i \in \{1, \dots, n\}$.

(3) $\ell_j^{(i)} < \ell_{j+1}^{(i)}$ *for all* $i \in \{1, \dots, n\}$ *and* $j \in \{1, \dots, k-1\}$.

(4) $\ell_j^{(i+1)} \leqslant \ell_j^{(i)}$ *for all* $i \in \{1, \dots, n-1\}$ *and* $j \in \{1, \dots, k\}$.

(5) $\ell_j^{(i)} \leqslant n - k + j$ *for all* $i \in \{1, \dots, n\}$ *and* $j \in \{1, \dots, k\}$.

(6) $\ell_j^{(i)} \geqslant \lceil \frac{d}{i} \rceil + j - 1$ *for all* $i \in \{1, \dots, n\}$ *and* $j \in \{1, \dots, k\}$.

Proof. We establish the various properties separately.

(1) Proposition 31 implies that the elements of $\mathscr{L}_1(n, m; q)$ are precisely the $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^n$ with a basis made of vectors with entries in $\mathbb{F}_q$. The statement follows from Remark 32 and Definition 65.

(2) Every $v \in C$ can be expressed as the sum of no less than $\lceil \mathrm{rk}(v)/i \rceil$ element of rank less or equal then i. Hence we have

$$\ell_1^{(i)} = \min\{\dim(X) : X \in \mathscr{L}_i(n, m; q), \dim(C \cap X) \geqslant 1\}$$
$$= \min\left\{ \left\lceil \frac{\mathrm{rk}(v)}{i} \right\rceil : v \in C \right\} = \left\lceil \frac{d}{i} \right\rceil.$$

(3) Let $X \in \mathscr{L}_i(n, m; q)$ such that $\dim(X \cap C) \geqslant j + 1$ and $\dim(X) = \ell_j^{(i)}$. Take an element $Y \in \mathscr{L}_i(n, m; q)$ such that $Y \leqslant X$ and $\dim(Y) = \dim(X) - 1 = \ell_j^{(i)} - 1$. We will prove that $\dim(Y \cap C) \geqslant j$. Note that, since $Y \leqslant X$, we have $Y \cap C = Y \cap (X \cap C)$ and $Y + (X \cap C) \leqslant X$. Therefore,

$$\dim(Y \cap C) = \dim(Y \cap (X \cap C))$$
$$= \dim(Y) + \dim(X \cap C) - \dim(Y + (X \cap C))$$
$$\geqslant \dim(Y) + \dim(X \cap C) - \dim(X)$$
$$= \ell_j^{(i)} - 1 + j + 1 - \ell_j^{(i)},$$

which implies $\dim(Y \cap C) \geqslant j$ and concludes the proof.

(4) The property follows from the definition of (i,j)-th lattice-rank weight.

(5) By (3) and the fact that $\dim(X) \leqslant n$ for any $X \in \mathscr{L}_i(n,m;q)$, we have an increasing chain $\ell_j^{(i)} < \ell_{j+1}^{(i)} < \cdots < \ell_k^{(i)} \leqslant n$. It follows that $\ell_j^{(i)} + k - j \leqslant n$.

(6) By (2) and (3) we have the decreasing chain $\ell_j^{(i)} > \ell_{j-1}^{(i)} > \cdots > \ell_1^{(i)} = \lceil \frac{d}{i} \rceil$. It follows that $\ell_j^{(i)} \geqslant \ell_1^{(i)} + j - 1$.

This concludes the proof. $\qquad\qquad\square$

Remark 67. Observe that, by part (2) of Theorem 66, we have that $\ell_1^{(i)} = 1$ for all $i \geqslant d$. This shows that $\ell_1^{(i)} = \ell_1^{(i+1)}$ for $i \geqslant d$ and therefore the bound in part (4) of Theorem 66 is sometimes met with equality if $j = 1$. Notice that the same bound can be met with equality also for $j \neq 1$. Consider, for example, $C := \langle e_1, e_2 \rangle_{\mathbb{F}_{q^m}} \leqslant \mathbb{F}_{q^m}^n$. It is not difficult to check that $\ell_1^{(i)} = 1$ and $\ell_2^{(i)} = 2$ for all $i \in \{1, \ldots, n\}$, which shows that $\ell_2^{(i)} = \ell_2^{(i+1)}$ for all $i \in \{1, \ldots, n\}$.

In the following example we show that lattice-rank weights can distinguish between inequivalent codes when the "fundamental" codes parameters (length, dimension, minimum distance, and generalized weights) don't.

Example 68. Let α be the primitive element of $\mathbb{F}_{2^4}$ with $\alpha^4 + \alpha + 1 = 0$ and consider the codes

$$C := \left\langle (1,0,\alpha^5,\alpha), (0,1,\alpha^{14},\alpha^{13}) \right\rangle, \qquad D := \left\langle (1,0,\alpha^6,\alpha^{10}), (0,1,\alpha^7,\alpha^3) \right\rangle,$$

where all the spans in this example are over $\mathbb{F}_{2^4}$. The following hold.

(1) $\mathrm{rk}((1,0,\alpha^5,\alpha)) = \mathrm{rk}((0,1,\alpha^{14},\alpha^{13})) = \mathrm{rk}((1,0,\alpha^6,\alpha^{10})) = \mathrm{rk}((0,1,\alpha^7,\alpha^3)) = 3$

(2) $\ell_1^{(1)}(C) = 2$. This value is attained, for example, by the space $\langle (1,1,0,0), (0,0,1,1) \rangle$ of $\mathscr{L}_1(4,4;2)$, whose intersection with C is $\langle (1,1,\alpha^{12},\alpha^{12}) \rangle$.

(3) $\ell_1^{(1)}(D) = 2$. This value is attained, for example, by the space $\langle (1,0,1,1), (0,1,0,1) \rangle$ of $\mathscr{L}_1(4,4;2)$, whose intersection with C is $\langle (1,\alpha^6,1,\alpha^{13}) \rangle$.

(4) $\ell_2^{(1)}(C) = \ell_2^{(1)}(D) = 4$. This means that the only element of $\mathscr{L}_1(4,4;2)$ that intersects C and D in a subspace of dimension at least 2 is the full space $\mathbb{F}_{2^4}^4$.

Therefore, by Theorem 66, C and D have the same "fundamental" code parameters. On the other hand, the following hold.

(5) $\ell_1^{(2)}(C) = 1$. This value is attained, for example, by the element $\langle (1,\alpha^6,0,1) \rangle$ of $\mathscr{L}_2(4,4;2)$.

(6) $\ell_1^{(2)}(D) = 1$. This value is attained, for example, by the element $\langle (1,\alpha^6,1,\alpha^{13}) \rangle$ of $\mathscr{L}_2(4,4;2)$.

(7) $\ell_2^{(2)}(C) = 2$. This is because $C \in \mathscr{L}_2(4,4;2)$, since $C = \langle (1,1,\alpha^{12},\alpha^{12}), (1,\alpha^6,0,1) \rangle$.

(8) $\ell_2^{(2)}(D) = 3$. This is because $D \notin \mathscr{L}_2(4,4;2)$ and the smallest element of $\mathscr{L}_2(4,4;2)$ containing D is $\langle (1,0,0,\alpha^{11}), (0,1,0,\alpha^{14}), (0,0,1,\alpha^8) \rangle$.

This allows us to conclude that C and D are inequivalent codes, even though they share the same generalized rank weights.

We now introduce the notions of *weight distribution* and *binomial moments* associated to the lattice-rank weights of a code. We show that partial information about the former provides partial information about the latter. These two notions capture structural properties of the underlying code that have been investigated before in the coding theory literature; see, for example, [23, 6, 14, 13]. In particular, the binomial moments have been used to define and study the *zeta function* of codes; see [23] for the Hamming metric and [6, 15] for the rank metric.

In the context outlined above, we also derive the MacWilliams identities for rank-metric codes associated to the lattice-rank weights. These identities provide a connection between the invariants of a code and those of its dual.

Definition 69. Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$. The (i,j)-**th lattice-rank distribution** of C is define as the integer vector whose $(u+1)$-th component, for $u \in \{0, \ldots, n\}$, is

$$A_{j,u}^{(i)}(C) := \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X) = u}} A_{j,X}^{(i)}(C),$$

where, for $X \in \mathscr{L}_i(n,m;q)$,

$$A_{j,X}^{(i)}(C) := |\{D \leqslant C \cap X : \dim(D) = j \text{ and } \nexists Y \in \mathscr{L}_i(n,m;q) \text{ s.t. } D \leqslant Y < X\}|.$$

Definition 70. Let $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, k\}$ and $u \in \{0, \ldots, n\}$. The (i,j,u)-**th lattice binomial moment** of C is defined as

$$B_{j,u}^{(i)}(C) := \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X) = u}} B_{j,X}(C),$$

where

$$B_{j,X}(C) = \begin{bmatrix} \dim(C \cap X) \\ j \end{bmatrix}_{q^m} \quad \text{for all } X \in \mathscr{L}_i(n,m;q).$$

To further simplify the notation, in the sequel we will write $A_{j,u}^{(i)}$ and $B_{j,u}^{(i)}$ instead of $A_{j,u}^{(i)}(C)$ and $B_{j,u}^{(i)}(C)$, respectively. The following result shows that $B_{j,u}^{(i)}$ is fully determined by the code parameters, for u in some intervals.

Proposition 71. *We have*

$$B_{j,u}^{(i)} = \begin{cases} 0 & \text{if } u < \ell_j^{(i)}, \\ \begin{bmatrix} k + u - n \\ j \end{bmatrix}_{q^m} |\{X \in \mathscr{L}_i(n,m;q) : \dim(X) = u\}| & \text{if } u > n - \hat{\ell}_1^{(i)\perp}. \end{cases}$$

Proof. If $u < \ell_j^{(i)}$, then for all $X \in \mathscr{L}_i(n, m; q)$ such that $\dim(X) = u$ we have

$$\begin{bmatrix} \dim(C \cap X) \\ j \end{bmatrix}_{q^m} = 0.$$

On the other hand, if $n - u < \hat{\ell}_1^{(i)\perp}$ then $C^\perp \cap X^\perp = \{0\}$ and the following holds:

$$
\begin{aligned}
B_{j,u}^{(i)}(C) &= \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X)=u}} \begin{bmatrix} \dim(C \cap X) \\ j \end{bmatrix}_{q^m} \\
&= \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X)=u}} \begin{bmatrix} n - \dim(C^\perp + X^\perp) \\ j \end{bmatrix}_{q^m} \\
&= \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X)=u}} \begin{bmatrix} \dim(C^\perp \cap X^\perp) + k + u - n \\ j \end{bmatrix}_{q^m} \\
&= \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X)=u}} \begin{bmatrix} k + u - n \\ j \end{bmatrix}_{q^m} \\
&= \begin{bmatrix} k + u - n \\ j \end{bmatrix}_{q^m} |\{X \in \mathscr{L}_i(n, m; q) : \dim(X) = u\}|.
\end{aligned}
$$

This concludes the proof. $\square$

Remark 72. We have that $B_{j,u}^{(i)} = A_{j,u}^{(i)} = 0$ for all $u < \ell_j^{(i)}$.

The following result shows the relation between the invariants we just defined. Its proof is similar to the one of [13, Theorem 6.4] and therefore we omit it.

Theorem 73. *Let* $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, k\}$ *and* $u, v \in \{0, \ldots, n\}$. *Define*

$$f_i(u, v) = |\{(X, Y) \in \mathscr{L}_i(n, m; q) \times \mathscr{L}_i(n, m; q) : Y \leqslant X, \dim(X) = u, \dim(Y) = v\}|$$

and denote by $\mu^{(i)}$ *the Möbius function of the lattice* $\mathscr{L}_i(n, m; q)$. *The following hold.*

(1) $B_{j,u}^{(i)} = \sum_{v=0}^{u} A_{j,v}^{(i)} f_i(u, v).$

(2) $A_{j,v}^{(i)} = \sum_{u=0}^{v} \mu^{(i)}(u, v) B_{j,u}^{(i)} f_i(v, u).$

The following can be seen as the MacWilliam identities for lattice-rank weights. We derive them passing through the lattice binomial moments. Using Theorem 73, an analogous result can be derived for the lattice-rank distribution. MacWilliam-types identities in this form have already been established in the coding theory literature in several contexts. The proof of this result is similar to the one of [13, Theorem 6.7] and we therefore omit it.

Theorem 74. *The following holds for all $i, j \in \{1, \ldots, k\}$ and $u \in \{1, \ldots, n\}$.*

$$B_{j,u}^{(i)} = \sum_{p=0}^{i} q^{mp(k+u-n-i+p)} \begin{bmatrix} k + u - n \\ i - p \end{bmatrix}_{q^m} \sum_{\substack{X \in \mathscr{L}_i(n,m;q) \\ \dim(X) = u}} \begin{bmatrix} \dim(C^\perp \cap X^\perp) \\ j \end{bmatrix}_{q^m}.$$

We conclude this section by characterizing some classes of rank-metric codes that exhibit interesting rigidity properties with respect to lattice-rank weights. The following is the vector-analogue of the family of j-TBMD codes; see [14, Definition 4.1] for matrix codes and [13, Definition 6.9] for higher-order tensors. The latter are a special class of tensor rank-metric whose *tensor binomial moments* are fully determined by the code parameters.

Definition 75. Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$. We say that C is a (i,j)-**LBMD** code (short for **lattice binomial moment determined**) code if

$$n - \ell_j^{(i)} - \hat{\ell}_1^{(i)\perp} < 0.$$

As an immediate consequence of Proposition 71 and Theorem 73, we have that the lattice binomial moments and the lattice-rank distribution of C associated with the lattice $\mathscr{L}_i(n, m; q)$ are fully determined by its code parameters. The following two results are straighforward consequences of Theorem 66 and Proposition 71.

Proposition 76. *Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$. If C is (i,j)-LBMD then C is $(i-1, j)$-LBMD and $(i, j+1)$-LBMD.*

Proposition 77. *Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$. If C is (i,j)-LBMD, then the (i,j)-th lattice rank distribution and binomial moments are fully determined by n, k, i, and j.*

We now turn to the lattice-analogues of MTR codes, which were introduced in [15].

Definition 78. We say that $C \leqslant \mathbb{F}_{q^m}^n$ is **perfect** if $C = \langle 0 \rangle_{\mathbb{F}_{q^m}}$ or if C has a basis made of rank-1 vectors. Equivalently, C is perfect if $C \in \mathscr{L}_1(n, m; q)$.

In the linear algebra literature, perfect spaces are often called Frobenius-closed.

Remark 79. The concept of perfect space was first introduced in [3], for matrix spaces, and later in [13], for higher order tensors. As observed in [12, Proposition 14.45] and [15, Proposition 3.4], there is a strong connection between perfect spaces and the tensor rank of a tensor code. More precisely, the tensor rank can be defined as the smallest dimension of a perfect space containing a tensor code. As a consequence, the value of $\ell_k^{(1)}$ can be seen as the vectorial analogue of the tensor rank of a tensor code the bound of part (6) of Theorem 66 is the corresponding Kruskal-type bound; see [27].

In Remark 79, we observed that Property (6) of Theorem 66 can be regarded as vector analogue of the tensor-rank bound. Matrix rank-metric codes meeting the Kruskal's bound with equality, namely the *MTR codes*, are of great interested in coding theory for their properties of optimality in terms of storage and encoding; see [15, Table 1]. We introduce the vector analogue of this family of codes.

Definition 80. Let $i \in \{1, \ldots, n\}$. We say that the code C is **i-lattice-optimal** if it attains the bound of part (6) of Theorem 66 for $j = k$, i.e., if

$$\ell_k^{(i)} = \ell_1^{(i)} + k - 1 = \left\lceil \frac{d}{i} \right\rceil + k - 1.$$

In the next result we show that C is i-lattice-optimal if and only if C attains the bound of part (6) of Theorem 66 for i and for all $j \in \{1, \ldots, k\}$. In particular, the lattice-rank weights of such a C indexed by i are fully determined by $\ell_1^{(i)}$.

Proposition 81. *The following statements are equivalent for all $i \in \{1, \ldots, n\}$.*

(1) C is a i-lattice-optimal code.

(2) $\ell_j^{(i)} = \ell_1^{(i)} + j - 1$ for all $j \in \{1, \ldots, k\}$.

Proof. If $\ell_j^{(i)} = \ell_1^{(i)} + j - 1$ for all $j \in \{1, \ldots, k\}$ then, in particular, $\ell_k^{(i)} = \ell_1^{(i)} + k - 1$, which implies that C is i-lattice-optimal. On the other hand, let C be i-lattice-optimal. By parts (2) and (3) of Theorem 66 we have an increasing chain

$$\ell_1^{(i)} < \ell_2^{(i)} < \cdots < \ell_k^{(i)} = \ell_1^{(i)} + k - 1.$$

This implies the statement. $\qquad\square$

As a consequence of Theorem 66 and [32, Corollary 19], we have that property (5) of Theorem 66 can be seen as a generalization of the Singleton-type bound for rank-metric codes (Theorem 24), which can be recovered for $i = 1$ and $j = 1$. This motivates the following definition.

Definition 82. Let $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$. We say that C is (i,j)-**LMRD** (short for **lattice maximum rank distance**) if C meets the bound of property (5) of Theorem 66 with equality, i.e., if

$$\ell_j^{(i)} = n - k + j.$$

The following result can be seen as the vector-analogue of [14, Theorem 4.15].

Proposition 83. *C is MRD if and only if C is $(1,1)$-LBMD.*

Proof. Recall that by Remark 64 we have that if $\{X^\perp : X \in \mathscr{L}_1(n, m; q)\} = \mathscr{L}_1(n, m; q)$. If C is MRD then $C^\perp$ is MRD as well [20] and we have

$$n - d - d^\perp = n - (n - k + 1) - (k + 1) = -2 < 0,$$

which implies that C is $(1,1)$-LBMD. On the other hand, if C is $(1,1)$-LBMD then we have $n < d + d^\perp$. Therefore, we must have $d + d^\perp = n + 2$ and C is MRD, for example, by [19, Corollary 18]. $\qquad\square$

We conclude this work with an example that illustrates some notion of optimality defined in this section.

Example 84. Let $q = 2$ and $n = m = 4$. Consider $C := \langle (1, 0, \alpha^2, \alpha^7), (0, 1, \alpha^6, \alpha^2) \rangle$, where the span is over $\mathbb{F}_{2^4}$ and α is a primitive element of $\mathbb{F}_{2^4}$ with $\alpha^4 + \alpha + 1 = 0$. We have $C^\perp = \langle (1, 0, \alpha^6, \alpha^{10}), (0, 1, \alpha^{11}, \alpha^6) \rangle$. Recall that by Remark 64 we have that $\{X^\perp : X \in \mathscr{L}_1(n, m; q)\} = \mathscr{L}_1(n, m; q)$. The following hold.

(1) $\ell_1^{(1)}(C) = \ell_1^{(1)}(C^\perp) = 3$, which implies that $d(C) = d(C^\perp) = 3$ by Theorem 66. This value is attained, for example, by the element $\langle (1, 0, 1, 0), (0, 1, 0, 0), (0, 0, 0, 1) \rangle$ of $\mathscr{L}_1(4, 4; 2)$, whose intersections with C and $C^\perp$ are the span of $(1, \alpha^2, 1, \alpha^3)$ and $(1, \alpha^2, 1, \alpha)$, respectively.

(2) $\ell_2^{(1)}(C) = 4$. This means that the only element of $\mathscr{L}_1(4, 4; 2)$ containing C is the full space $\mathbb{F}_{2^4}^4$.

Therefore, we have

$$4 - \ell_1^{(1)}(C) - \ell_1^{(1)}(C^\perp) = -2 < 0, \qquad 4 - \ell_2^{(1)}(C) - \ell_1^{(1)}(C^\perp) = -3 < 0.$$

It follows that C is $(1, 1)$-LBMD and $(1, 2)$-LBMD. Moreover, one can easily check that C is also MRD. Note that this is in line with Proposition 83.

References

[1] G. E. Andrews. *The Theory of Partitions*. Cambridge University Press, 1998.

[2] J. Antrobus and H. Gluesing-Luerssen. Maximal Ferrers diagram codes: Constructions and genericity considerations. *IEEE Transactions on Information Theory*, 65(10):6204–6223, 2019.

[3] M. D. Atkinson and S. Lloyd. The ranks of $m \times n \times (mn - 2)$ tensors. *SIAM Journal on Computing*, 12(4):611–615, 1983.

[4] D. Bartoli, M. Giulietti, G. Marino, and O. Polverino. Maximum scattered linear sets and complete caps in galois spaces. *Combinatorica*, 38(2):255–278, 2018.

[5] D. Bartoli, G. Marino, and A. Neri. New MRD codes from linear cutting blocking sets. `arXiv:2106.12465`, 2022.

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

[7] A. Blass and B. E. Sagan. Möbius functions of lattices. *Advances in Mathematics*, 127(1):94–123, 1997.

[8] J. E. Bonin. Automorphism groups of higher-weight dowling geometries. *Journal of Combinatorial Theory, Series B*, 58(2):161–173, 1993.

[9] J. E. Bonin. Modular elements of higher-weight dowling lattices. *Discrete Mathematics*, 119:3–11, 1993.

[10] A. Brini. Some remarks on the critical problem. In A. Barlotti, editor, *Matroid Theory and its Applications*, 113–124. 1982.

[11] T. Britz. Extensions of the critical theorem. *Discrete Mathematics*, 305(1-3):55–73, 2005.

[12] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*, volume 315. Springer Science & Business Media, 1996.

[13] E. Byrne and G. Cotardo. Tensor codes and their invariants. arXiv:2112.08100, 2021.

[14] E. Byrne, G. Cotardo, and A. Ravagnani. Rank-metric codes, generalized binomial moments and their zeta functions. *Linear Algebra and its Applications*, 604:92–128, 2020.

[15] E. Byrne, A. Neri, A. Ravagnani, and J. Sheekey. Tensor representation of rank-metric codes. *SIAM Journal on Applied Algebra and Geometry*, 3(4):614–643, 2019.

[16] E. Byrne and A. Ravagnani. Partition-balanced families of codes and asymptotic enumeration in coding theory. *Journal of Combinatorial Theory, Series A*, 171, 2020.

[17] H. Crapo and G.-C. Rota. *On the Foundations of Combinatorial Theory: Combinatorial Geometries*. MIT Press, 1970.

[18] B. Csajbók, G. Marino, O. Polverino, and F. Zullo. Maximum scattered linear sets and MRD-codes. *Journal of Algebraic Combinatorics*, 46(3):517–531, 2017.

[19] J. de la Cruz, E. Gorla, H. H. López, and A. Ravagnani. Weight distribution of rank-metric codes. *Designs, Codes and Cryptography*, 86(1):1–16, 2018.

[20] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[21] T. A. Dowling. Codes, packings and the critical problem. *Atti del Convegno di Geometria Combinatoria e sue Applicazioni*, 209–224, 1971.

[22] T. A. Dowling. A q-analog of the partition lattice. In *A Survey of Combinatorial Theory*, 101–115. 1973.

[23] I. M. Duursma. Combinatorics of the two-variable zeta function. *International Conference on Finite Fields and Applications*, 109–136, 2003.

[24] R. A. Games. The packing problem for projective geometries over $GF(3)$ with dimension greater than five. *Journal of Combinatorial Theory, Series A*, 35(2):126–144, 1983.

[25] A. Gruica and A. Ravagnani. Common complements of linear subspaces and the sparseness of MRD codes. *SIAM Journal on Applied Algebra and Geometry*, 6, 2022.

[26] J. Hallam and B. Sagan. Factoring the characteristic polynomial of a lattice. *Journal of Combinatorial Theory, Series A*, 136:39–63, 2015.

[27] J. B. Kruskal. Three-way arrays: rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics. *Linear Algebra and its Applications*, 18(2):95–138, 1977.

[28] J. P. S. Kung. Critical problems. *Contemporary Mathematics*, 197:1–128, 1996.

[29] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Transactions On information theory*, 61(7):3912–3936, 2015.

[30] G. Marino, A. Neri, and R. Trombetti. Evasive subspaces, generalized rank weights and near MRD codes. `arXiv:2204.11791`, 2022.

[31] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[32] A. Ravagnani. Generalized weights: An anticode approach. *Journal of Pure and Applied Algebra*, 220(5):1946–1962, 2016.

[33] A. Ravagnani. Whitney numbers of combinatorial geometries and higher-weight Dowling lattices. *SIAM Journal on Applied Algebra and Geometry*, 6(2):156–189, 2022.

[34] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Annali di Matematica Pura ed Applicata*, 39(1):357–379, 1955.

[35] R. P. Stanley. Modular elements of geometric lattices. *Algebra Universalis*, 1(1):214–217, 1971.

[36] R. P. Stanley. Supersolvable lattices. *Algebra Universalis*, 2(1):197–217, 1972.

[37] R. P. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 2nd edition, 2011.

[38] T. Zaslavsky. The möbius function and the characteristic polynomial. *Combinatorial geometries*, 29:114–38, 1987.