



Rank-metric codes and q -polymatroids

Elisa Gorla¹ · Relinde Jurrius² · Hiram H. López³ · Alberto Ravagnani⁴

Received: 30 April 2018 / Accepted: 29 April 2019 / Published online: 18 May 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

This paper contributes to the study of rank-metric codes from an algebraic and combinatorial point of view. We introduce q -polymatroids, the q -analogue of polymatroids, and develop their basic properties. We associate a pair of q -polymatroids with a rank-metric code and show that several invariants and structural properties of the code, such as generalized weights, the property of being MRD or an optimal anticode, and duality, are captured by the associated combinatorial object.

Keywords Rank-metric code · Generalized weights · q -polymatroid · MRD code · Optimal anticode · Duality

1 Introduction and motivation

Rank-metric codes were originally introduced by Delsarte [5] and later rediscovered by Gabidulin [6] and Roth [20]. Due to their application in network coding, the interest in these codes has intensified over the past years and many recent papers have been devoted to their study. While interest in these codes stems from practical applications, rank-metric codes also present interesting algebraic and combinatorial properties. Therefore, their mathematical structure has also been the object of several works. This paper belongs to the latter line of study. Our contributions are twofold: on the one side we study generalized weights of rank-metric codes, and on the other we establish a link with other combinatorial objects. More precisely, we associate with each rank-metric code a q -polymatroid, the q -analogue of a polymatroid, which we define here.

In Sect. 2, we define rank-metric codes and vector rank-metric codes. We recall how to associate a rank-metric code with a vector rank-metric code via the choice of

✉ Elisa Gorla
elisa.gorla@unine.ch

¹ Institut de Matématiques, Université de Neuchâtel, Neuchâtel, Switzerland

² Faculty of Military Science, Netherlands Defence Academy, Den Helder, The Netherlands

³ Department of Mathematics, Cleveland State University, Cleveland, USA

⁴ School of Mathematics and Statistics, University College Dublin, Dublin, Ireland

a basis and establish a number of basic, but fundamental facts. In particular, we recall the notions of equivalence for rank-metric codes and vector rank-metric codes and we discuss in detail why these notions are compatible via the association mentioned above. We also explain that, while the choice of a basis affects the rank-metric code obtained via the association above, the equivalence class of the rank-metric code obtained does not depend on the choice of the basis.

Generalized weights have been defined and studied in different levels of generality by many researchers. Two of the first definitions of generalized weights for vector rank-metric codes are due to Kurihara, Matsumoto, and Uyematsu [12] and to Oggier and Sboui [14]. More definitions are due to Jurrius and Pellikaan [9] and Martínez-Peñas and Matsumoto [13], who also compared the various definitions. Using the theory of anticode, Ravagnani [18] gave a definition of generalized weights for matrix rank-metric codes, which extends the one from [12].

In this paper, we develop further the theory of generalized weights for rank-metric codes, tying together several previously known results on the subject. We adopt the definition from [18] and, in Sect. 3, we show that it is invariant with respect to equivalence of rank-metric codes. We also show that the definition of generalized weights for rank-metric codes from [13], which generalizes definitions from [9, 11, 24], is not invariant with respect to code equivalence.

Given the well-known link between codes in the Hamming metric and matroids, it is a natural question to ask whether there is a q -analogue of this. Rank-metric codes can be viewed as the q -analogue of block-codes endowed with the Hamming metric. So it is natural to ask what is the q -analogue of a matroid. Crapo [3] already studied this combinatorial object from the point of view of geometric lattices. Recently, Jurrius and Pellikaan [10] rediscovered q -matroids and associated a q -matroid with every vector rank-metric code. One goal of the current paper is extending this association with rank-metric codes.

With this in mind, we define the q -analogue of a polymatroid, that we call a q -polymatroid. In Sect. 4, we develop basic properties of q -polymatroids, such as equivalence and duality. In Sect. 5, we associate with every rank-metric code a pair of q -polymatroids. We also show that the q -polymatroids arising from rank-metric codes are in general not q -matroids. We then show that several structural properties of rank-metric codes depend only on the associated q -polymatroid: In Sect. 6, we do this for the minimum distance and the property of being MRD, in Sect. 7 for the generalized weights and for the property of being an optimal anticode, and in Sect. 8 for duality. These results are q -analogues of classical results in coding theory.

While preparing this manuscript, we became aware that a slightly different definition of q -analogue of a polymatroid was given independently by Shiramoto [21]. While our paper applies this theory to equivalence of codes and to generalized weights, [21] focuses on the weight enumerator of rank-metric codes.

2 Rank-metric and vector rank-metric codes

We start by establishing the notation and the definitions used throughout the paper.

Notation 2.1 In the sequel, we fix integers $n, m \geq 2$ and a prime power q . For an integer t , we let $[t] := \{1, \dots, t\}$. We denote by \mathbb{F}_q the finite field with q elements. The space of $n \times m$ matrices with entries in \mathbb{F}_q is denoted by Mat . Up to transposition, we assume without loss of generality that $n \leq m$. We let

$$\begin{aligned}\text{Mat}(J, c) &= \{M \in \text{Mat} \mid \text{colsp}(M) \subseteq J\} \quad \text{and} \\ \text{Mat}(J, r) &= \{M \in \text{Mat} \mid \text{rowsp}(M) \subseteq J\}.\end{aligned}$$

Throughout the paper, we only consider linear codes. All dimensions are computed over \mathbb{F}_q , unless otherwise stated.

Definition 2.2 A **(matrix) rank-metric code** is an \mathbb{F}_q -linear subspace $\mathcal{C} \subseteq \text{Mat}$. The **dual** of \mathcal{C} is

$$\mathcal{C}^\perp = \{M \in \text{Mat} \mid \text{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\},$$

where $\text{Tr}(\cdot)$ denotes the trace. It is easy to check that \mathcal{C}^\perp is a code as well, i.e., that it is \mathbb{F}_q -linear. The **minimum (rank) distance** of a nonzero rank-metric code $\mathcal{C} \subseteq \text{Mat}$ is the integer $d(\mathcal{C}) := \min\{\text{rk}(M) \mid M \in \mathcal{C}, M \neq 0\}$.

The next bound relates the dimension of a code $\mathcal{C} \subseteq \text{Mat}$ to its minimum distance. It is the analogue for the rank metric of the Singleton bound from classical coding theory.

Proposition 2.3 ([5], Theorem 5.4). *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero rank-metric code with minimum distance d . Then $\dim(\mathcal{C}) \leq m(n - d + 1)$.*

Definition 2.4 A code that attains the bound of Proposition 2.3 is called a **maximum rank distance (MRD)** code.

We now introduce some transformations that preserve the dimension and the minimum rank distance of a rank-metric code. These will play a central role throughout the paper.

Notation 2.5 Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code, let $A \in \text{GL}_n(\mathbb{F}_q)$ and $B \in \text{GL}_m(\mathbb{F}_q)$. Define

$$ACB := \{AMB \mid M \in \mathcal{C}\} \subseteq \text{Mat}.$$

When $n = m$, define the **transpose** of a rank-metric code $\mathcal{C} \subseteq \text{Mat}$ as

$$\mathcal{C}^t := \{M^t \mid M \in \mathcal{C}\} \subseteq \text{Mat}.$$

As we are interested in structural properties of rank-metric codes, it is natural to study these objects up to equivalence. Linear isometries of the space of matrices of fixed size induce a natural notion of equivalence among rank-metric codes.

Definition 2.6 Two rank-metric codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \text{Mat}$ are **equivalent** if there exists an \mathbb{F}_q -linear isometry $f : \text{Mat} \rightarrow \text{Mat}$ such that $f(\mathcal{C}_1) = \mathcal{C}_2$. If this is the case, then we write $\mathcal{C}_1 \sim \mathcal{C}_2$.

The next theorem gives a characterization of the linear isometries of Mat . It combines results by Hua and Wan, and it can be found in the form stated below in [23, Theorem 3.4].

Theorem 2.7 ([8,22]). *Let $f : \text{Mat} \rightarrow \text{Mat}$ be an \mathbb{F}_q -linear isometry with respect to the rank metric.*

- (1) *If $m < n$, then there exist matrices $A \in GL_n(\mathbb{F}_q)$ and $B \in GL_m(\mathbb{F}_q)$ such that $f(M) = AMB$ for all $M \in \text{Mat}$.*
- (2) *If $m = n$, then there exist matrices $A, B \in GL_m(\mathbb{F}_q)$ such that either $f(M) = AMB$ for all $M \in \text{Mat}$, or $f(M) = AM^t B$ for all $M \in \text{Mat}$.*

A class of codes that has recently received a lot of attention is that of vector rank-metric codes, introduced independently by Gabidulin and Roth in [6] and [20], respectively.

Definition 2.8 The **rank weight** $\text{rk}(v)$ of a vector $v \in \mathbb{F}_{q^m}^n$ is the dimension of the \mathbb{F}_q -linear space generated by its entries. A **vector rank-metric code** is an \mathbb{F}_{q^m} -linear subspace $C \subseteq \mathbb{F}_{q^m}^n$. The **dual** of C is the vector rank-metric code

$$C^\perp := \{v \in \mathbb{F}_{q^m}^n \mid \langle v, w \rangle = 0 \text{ for all } w \in C\},$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product of $\mathbb{F}_{q^m}^n$. When $C \neq \{0\}$ is a nonzero vector rank-metric code, the **minimum (rank) distance** of C is $d(C) = \min\{\text{rk}(v) \mid v \in C, v \neq 0\}$.

Notation 2.9 Let $C \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric code and $B \in GL_n(\mathbb{F}_q)$. Define

$$CB := \{vB \mid v \in C\} \subseteq \mathbb{F}_{q^m}^n.$$

Similarly to the case of rank-metric codes, the linear isometries of $\mathbb{F}_{q^m}^n$ induce a notion of equivalence for vector rank-metric codes.

Definition 2.10 Two vector rank-metric codes $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$ are **equivalent** if there exists an \mathbb{F}_{q^m} -linear isometry $f : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_{q^m}^n$ such that $f(C_1) = C_2$. If this is the case, then we write $C_1 \sim C_2$.

The linear isometries of $\mathbb{F}_{q^m}^n$ can be described as follows.

Theorem 2.11 ([1]). *Let $f : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_{q^m}^n$ be an \mathbb{F}_{q^m} -linear isometry with respect to the rank metric. Then there exist $\alpha \in \mathbb{F}_{q^m}^*$ and $B \in GL_n(\mathbb{F}_q)$ such that $f(v) = \alpha vB$ for all $v \in \mathbb{F}_{q^m}^n$.*

There is a natural way to associate a rank-metric code C with a vector rank-metric code C , in such a way that the metric properties are preserved. Given an \mathbb{F}_q -basis $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ of \mathbb{F}_q^m and given a vector $v \in \mathbb{F}_q^m$, let $\Gamma(v)$ denote the unique $n \times m$ matrix with entries in \mathbb{F}_q that satisfies

$$v_i = \sum_{j=1}^m \Gamma_{ij}(v)\gamma_j \quad \text{for all } 1 \leq i \leq n.$$

Proposition 2.12 ([7], Section 1). *The map $v \mapsto \Gamma(v)$ is an \mathbb{F}_q -linear isometry. In particular, if $C \subseteq \mathbb{F}_q^m$ is a vector rank-metric code of dimension k over \mathbb{F}_q^m , then $\Gamma(C)$ is an \mathbb{F}_q -linear rank-metric code of dimension mk over \mathbb{F}_q . Moreover, if $C \neq \{0\}$, then C and $\Gamma(C)$ have the same minimum rank distance.*

As one expects, the rank-metric codes obtained from equivalent vector rank-metric codes using different bases Γ and Γ' are equivalent.

Proposition 2.13 *Let $C_1, C_2 \subseteq \mathbb{F}_q^m$ be vector rank-metric codes. Let Γ and Γ' be bases of \mathbb{F}_q^m over \mathbb{F}_q . If $C_1 \sim C_2$, then $\Gamma(C_1) \sim \Gamma'(C_2)$.*

Proof By [18, Lemma 27.2], $\Gamma(C) \sim \Gamma'(C)$. Hence we may assume without loss of generality that $\Gamma = \Gamma' = \{\gamma_1, \dots, \gamma_m\}$. By definition of Γ

$$\gamma_k \gamma_j = \sum_{\ell=1}^m \Gamma(\gamma_k \gamma_1, \dots, \gamma_k \gamma_m)_{j\ell} \gamma_\ell$$

If $C_1 \sim C_2$, then by Theorem 2.11 there exist $\alpha \in \mathbb{F}_q^{*m}$ and $B = (b_{ij}) \in \text{GL}_n(\mathbb{F}_q)$ such that $C_2 = \alpha C_1 B$. If $v = (v_1, \dots, v_n) \in \mathbb{F}_q^m$, then

$$\begin{aligned} \alpha v_i &= \sum_{h=1}^m \Gamma(v)_{ih} \alpha \gamma_h = \sum_{j=1}^m \sum_{h=1}^m \Gamma(v)_{ih} \Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m)_{hj} \gamma_j \\ &= \sum_{j=1}^m (\Gamma(v) \Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m))_{ij} \gamma_j. \end{aligned}$$

Therefore,

$$\Gamma(\alpha v) = \Gamma(v) \Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m).$$

On the other side

$$\begin{aligned} vB &= \left(\sum_{k=1}^n b_{k1} v_k, \dots, \sum_{k=1}^n b_{kn} v_k \right) \\ &= \left(\sum_{k=1}^n \sum_{j=1}^m b_{k1} \Gamma(v)_{kj} \gamma_j, \dots, \sum_{k=1}^n \sum_{j=1}^m b_{kn} \Gamma(v)_{kj} \gamma_j \right), \end{aligned}$$

hence

$$\Gamma(vB)_{ij} = \sum_{k=1}^n b_{ki} \Gamma(v)_{kj} = (B^t \Gamma(v))_{ij},$$

that is

$$\Gamma(vB) = B^t \Gamma(v).$$

Then for every $v \in C_1$, we obtain $\Gamma(\alpha v B) = B^t \Gamma(v) \Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m)$, i.e.,

$$\Gamma(C_2) = \Gamma(\alpha C_1 B) = B^t \Gamma(C_1) \Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m) \sim \Gamma(C_1)$$

since $B^t \in \text{GL}_n(\mathbb{F}_q)$ and $\text{rk}(\Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m)) = \text{rk}(\alpha \gamma_1, \dots, \alpha \gamma_m) = \text{rk}(\gamma_1, \dots, \gamma_m) = m$, hence $\Gamma(\alpha \gamma_1, \dots, \alpha \gamma_m) \in \text{GL}_m(\mathbb{F}_q)$. \square

Proposition 2.13 suggests a natural definition of \mathbb{F}_{q^m} -linear rank-metric code in the \mathbb{F}_q -linear matrix space Mat .

Definition 2.14 Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code. We say that \mathcal{C} is \mathbb{F}_{q^m} -**linear** if there exists a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ and a basis of Γ of \mathbb{F}_{q^m} over \mathbb{F}_q such that $\mathcal{C} \sim \Gamma(C)$.

3 Optimal anticodes and generalized weights

Optimal linear anticodes were introduced in [18] with the purpose of studying generalized weights in the rank metric.

Definition 3.1 The **maximum rank** of a rank-metric code $\mathcal{C} \subseteq \text{Mat}$ is

$$\text{maxrk}(\mathcal{C}) := \max\{\text{rk}(M) \mid M \in \mathcal{C}\}.$$

A rank-metric code $\mathcal{A} \subseteq \text{Mat}$ is an **optimal anticode** if $\dim(\mathcal{A}) = m \cdot \text{maxrk}(\mathcal{A})$.

The class of optimal anticodes is closed with respect to duality [17, Theorem 54] and code equivalence. The properties of optimal anticodes were exploited in [18] to study a class of algebraic invariants of rank-metric codes, called (Delsarte) generalized weights.

Definition 3.2 Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero code. For $i \geq 1$, the i -th **generalized weight** of \mathcal{C} is

$$a_i(\mathcal{C}) := \frac{1}{m} \min\{\dim(\mathcal{A}) \mid \mathcal{A} \subseteq \text{Mat} \text{ is an optimal anticode, } \dim(\mathcal{C} \cap \mathcal{A}) \geq i\}.$$

Remark 3.3 $a_1(\mathcal{C})$ is the minimum rank distance of \mathcal{C} . See [18, Theorem 30] for details.

As one may expect, equivalent codes have the same generalized weights.

Proposition 3.4 *Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \text{Mat}$ be nonzero codes and assume $\mathcal{C}_1 \sim \mathcal{C}_2$. Then*

$$a_i(\mathcal{C}_1) = a_i(\mathcal{C}_2) \text{ for every integer } i \geq 1.$$

Proof Since $\mathcal{C}_1 \sim \mathcal{C}_2$, there exist $A \in \text{GL}_n(\mathbb{F}_q)$ and $B \in \text{GL}_m(\mathbb{F}_q)$ such that either $\mathcal{C}_2 = AC_1B$, or $\mathcal{C}_2 = AC_1^tB$ and $n = m$. We prove the proposition in the second case, as the proof in the first is similar.

Let $\text{Ant}(\text{Mat})$ denote the set of optimal anticodes in Mat , and fix a positive integer i . The chain of equalities

$$A(\mathcal{A} \cap \mathcal{C}_1)^t B = (AA^t \mathcal{B}) \cap (AC_1^t B) = (AA^t \mathcal{B}) \cap \mathcal{C}_2$$

implies that the isometry $f : \text{Ant}(\text{Mat}) \rightarrow \text{Ant}(\text{Mat})$ defined by $f(\mathcal{A}) := AA^t \mathcal{B}$ gives a bijection between the anticodes $\mathcal{A} \subseteq \text{Mat}$ such that $\dim(\mathcal{A} \cap \mathcal{C}_1) \geq i$ and the anticodes $\mathcal{B} \subseteq \text{Mat}$ such that $\dim(\mathcal{B} \cap \mathcal{C}_2) \geq i$. Then \mathcal{C}_1 and \mathcal{C}_2 have the same generalized weights by definition. \square

The definition of generalized weights in terms of anticodes suggests the following natural questions. Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code, and let \mathcal{A} be an optimal anticode such that $\dim(\mathcal{C} \cap \mathcal{A}) \geq i$ and $a_i(\mathcal{C}) = \dim(\mathcal{A})/m$.

- (1) Can one find an optimal anticode \mathcal{A}' such that $\mathcal{A} \subseteq \mathcal{A}'$, $\dim(\mathcal{C} \cap \mathcal{A}') \geq i + 1$, and $a_{i+1}(\mathcal{C}) = \dim(\mathcal{A}')/m$?
- (2) Can one find an optimal anticode \mathcal{A}'' such that $\mathcal{A}'' \subseteq \mathcal{A}$, $\dim(\mathcal{C} \cap \mathcal{A}'') \geq i - 1$, and $a_{i-1}(\mathcal{C}) = \dim(\mathcal{A}'')/m$?

The following example shows that the answer to both questions is negative.

Example 3.5 Let $q = 2$ and $n = m = 3$. Let \mathcal{C} be the rank-metric code generated by the three independent matrices

$$M_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M_2 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

It is easy to check that $a_1(\mathcal{C}) = 1$ and $a_2(\mathcal{C}) = 2$. By [4, Theorems 4 and 6], the optimal anticodes in $\text{Mat}_{3 \times 3}(\mathbb{F}_2)$ are of the form $\text{Mat}(J, c)$ or $\text{Mat}(J, r)$ for some $J \subseteq \mathbb{F}_2^3$. Let \mathcal{A}_1 be an optimal anticode of dimension 3 with $\dim(\mathcal{C} \cap \mathcal{A}_1) \geq 1$. Then we have $\mathcal{A}_1 = \text{Mat}(((1, 0, 0)), c)$ or $\mathcal{A}_1 = \text{Mat}(((1, 0, 0)), r)$. Let \mathcal{A}_2 be an optimal anticode of dimension 6 with $\dim(\mathcal{C} \cap \mathcal{A}_2) \geq 2$. Then we have $\mathcal{A}_2 = \text{Mat}(((0, 1, 0), (0, 0, 1)), c)$ or $\mathcal{A}_2 = \text{Mat}(((0, 1, 0), (0, 0, 1)), r)$.

Notice that one could also define generalized weights for rank-metric codes following a support-based analogy with codes endowed with the Hamming metric. This naturally leads to generalizing the invariants proposed in [11], [24] and [9] as in the following Definition 3.6. This approach has been followed, e.g., in [13]. Notice that in [13] supports are defined as column spaces also in the case when $n > m$.

Definition 3.6 Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero code. The **support** of a subcode $\mathcal{D} \subseteq \mathcal{C}$ is

$$\text{supp}(\mathcal{D}) := \sum_{M \in \mathcal{D}} \text{colsp}(M) \subseteq \mathbb{F}_q^n,$$

where the sum is the sum of vector spaces. The i -th **support weight** of \mathcal{C} is

$$cs_i(\mathcal{C}) := \min\{\dim(\text{supp}(\mathcal{D})) \mid \mathcal{D} \subseteq \mathcal{C}, \dim(\mathcal{D}) = i\}.$$

Remark 3.7 Although Definition 3.6 produces an interesting and well-behaved algebraic invariant, we observe that the analogue of Proposition 3.4 does not hold for support weights. In other words, while equivalent codes always have the same generalized weights, they might not have the same support weights. We illustrate this in the following example.

Example 3.8 Let \mathcal{C} be the binary code defined by

$$\mathcal{C} := \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \mid a, b \in \mathbb{F}_2 \right\}.$$

Then \mathcal{C} is an optimal anticode of dimension 2. Therefore, $a_2(\mathcal{C}) = 1$. On the other hand, $\text{supp}(\mathcal{C}) = \mathbb{F}_2^2$, hence $cs_2(\mathcal{C}) = 2 \neq a_2(\mathcal{C})$. Now observe that $\mathcal{C} \sim \mathcal{C}^t$. In particular, $a_2(\mathcal{C}) = a_2(\mathcal{C}^t) = 1$. However, $cs_2(\mathcal{C}) = 2$, while $cs_2(\mathcal{C}^t) = 1$.

Generalized weights and support weights relate to each other as follows.

Proposition 3.9 ([13], Theorem 9). *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero code, and let $i \geq 1$ be an integer. If $m > n$, then $a_i(\mathcal{C}) = cs_i(\mathcal{C})$. If $m = n$, then $a_i(\mathcal{C}) \leq cs_i(\mathcal{C})$.*

We stress that there exist codes $\mathcal{C} \subseteq \text{Mat}$ with $m = n$ and $a_i(\mathcal{C}) < cs_i(\mathcal{C})$, e.g., the code \mathcal{C} of Example 3.8.

4 The q -analogue of a polymatroid

This section introduces q -polymatroids, that are a q -analogue of polymatroids. For more on (poly)matroids, see the standard references [15,25].

Definition 4.1 A q -**polymatroid** is a pair $P = (\mathbb{F}_q^n, \rho)$ where $n \geq 1$ and ρ is a function from the set of all subspaces of \mathbb{F}_q^n to \mathbb{R} such that, for all $A, B \subseteq \mathbb{F}_q^n$:

- (P1) $0 \leq \rho(A) \leq \dim(A)$,
- (P2) if $A \subseteq B$, then $\rho(A) \leq \rho(B)$,
- (P3) $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

Notice that a q -polymatroid such that ρ is integer-valued is a q -**matroid** according to [10, Definition 2.1].

Remark 4.2 Our definition of q -polymatroid is slightly different from that of (q, r) -polymatroid given by Shiromoto in [21, Definition 2]. However, a (q, r) -polymatroid (E, ρ) as defined by Shiromoto corresponds to the q -polymatroid $(E, \rho/r)$ according to our definition. Moreover, a q -polymatroid whose rank function takes values in \mathbb{Q} corresponds to a (q, r) -polymatroid as defined by Shiromoto up to multiplying the rank function for an r which clears denominators.

Remark 4.3 One could also define a q -polymatroid P as a pair (\mathbb{F}_q^n, ρ) that satisfies $\rho(A) \geq 0$ for all $A \subseteq \mathbb{F}_q^n$, (P2), and (P3). Up to multiplying the rank function by a suitable constant, one may additionally assume that $\rho(x) \leq 1$ for all 1-dimensional subspaces $x \subseteq \mathbb{F}_q^n$. It is easy to show that this is equivalent to Definition 4.1.

The definition of q -polymatroid that we propose is a direct q -analogue of the definition of an ordinary polymatroid, with the extra property that $\rho(A) \leq \dim(A)$ for all A . As in the ordinary case, a q -matroid is a q -polymatroid. At the end of Sect. 6 we give an example of a q -polymatroid that is not a q -matroid. One has the following natural notion of equivalence for q -polymatroids.

Definition 4.4 Let (\mathbb{F}_q^n, ρ_1) and (\mathbb{F}_q^n, ρ_2) be q -polymatroids. We say that (\mathbb{F}_q^n, ρ_1) and (\mathbb{F}_q^n, ρ_2) are **equivalent** if there exists an \mathbb{F}_q -linear isomorphism $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ such that $\rho_1(A) = \rho_2(\varphi(A))$ for all $A \subseteq \mathbb{F}_q^n$. In this case, we write $(\mathbb{F}_q^n, \rho_1) \sim (\mathbb{F}_q^n, \rho_2)$.

We start by introducing a notion of duality for q -polymatroids.

Definition 4.5 Let $P = (\mathbb{F}_q^n, \rho)$ be a q -polymatroid. For all subspaces $A \subseteq \mathbb{F}_q^n$ define

$$\rho^*(A) = \dim(A) - \rho(\mathbb{F}_q^n) + \rho(A^\perp),$$

where A^\perp is the orthogonal complement of A with respect to the standard inner product on \mathbb{F}_q^n . We call $P^* = (\mathbb{F}_q^n, \rho^*)$ the **dual** of the q -polymatroid P .

The proof of the next theorem is essentially the same as the proof of [10, Theorem 42].

Theorem 4.6 *The dual P^* is a q -polymatroid.*

We will need the following property of dual q -polymatroids.

Proposition 4.7 *Let $P_1 = (\mathbb{F}_q^n, \rho_1)$ and $P_2 = (\mathbb{F}_q^n, \rho_2)$ be q -polymatroids. If $P_1 \sim P_2$, then $P_1^* \sim P_2^*$. Moreover, for every q -polymatroid P we have $P^{**} = P$.*

Proof By definition, there exists an \mathbb{F}_q -isomorphism $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ with the property that $\rho_1(A) = \rho_2(\varphi(A))$ for all $A \subseteq \mathbb{F}_q^n$. In particular, $\varphi(\mathbb{F}_q^n) = \mathbb{F}_q^n$. Therefore, by definition of ρ_1^* , for all $A \subseteq \mathbb{F}_q^n$ we have

$$\rho_1^*(A) = \dim(A) - \rho_2(\mathbb{F}_q^n) + \rho_2(\varphi(A^\perp)).$$

Now let $\psi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ be the adjoint of φ with respect to the standard inner product of \mathbb{F}_q^n . Then ψ is an \mathbb{F}_q -isomorphism, and $\varphi(A)^\perp = \psi(A)^\perp$ for all $A \subseteq \mathbb{F}_q^n$. Therefore,

$$\rho_1^*(A) = \dim(A) - \rho_2(\mathbb{F}_q^n) + \rho_2(\psi(A)^\perp) = \rho_2^*(\psi(A)).$$

If $P = (\mathbb{F}_q^n, \rho)$ is a q -polymatroid, then it is straightforward to check that $\rho^{**}(A) = \rho(A)$. This implies $P^{**} = P$. \square

5 Rank-metric codes and q -polymatroids

Starting from a rank-metric code $\mathcal{C} \subseteq \text{Mat}$, in this section we construct two q -polymatroids: one associated with the column spaces, and the other to the row spaces. They will be denoted by $P(\mathcal{C}, c)$ and $P(\mathcal{C}, r)$, respectively. As the reader will see in the next sections, several structural properties of \mathcal{C} can be read off the associated q -polymatroids.

We start by studying subcodes of a given code, whose matrices are *supported* on a subspace $J \subseteq \mathbb{F}_q^n$ or $K \subseteq \mathbb{F}_q^m$. See [19] for a lattice-theoretic definition of support.

Notation 5.1 Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code, and let $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$ be subspaces. We define

$$\mathcal{C}(J, c) := \{M \in \mathcal{C} \mid \text{colsp}(M) \subseteq J\} \quad \text{and} \quad \mathcal{C}(K, r) := \{M \in \mathcal{C} \mid \text{rowsp}(M) \subseteq K\},$$

where $\text{colsp}(M) \subseteq \mathbb{F}_q^n$ and $\text{rowsp}(M) \subseteq \mathbb{F}_q^m$ are the spaces generated over \mathbb{F}_q by the columns, respectively the rows, of M .

Notice that $\mathcal{C}(J, c)$ and $\mathcal{C}(K, r)$ are subcodes of \mathcal{C} for all $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$. In the sequel, we denote by J^\perp the orthogonal of a space $J \subseteq \mathbb{F}_q^n$ with respect to the standard inner product of \mathbb{F}_q^n . We use the same notation for subspaces $K \subseteq \mathbb{F}_q^m$. No confusion will arise with the trace-dual of a code $\mathcal{C} \subseteq \text{Mat}$.

Notation 5.2 Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code. For subspaces $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$ define the rational numbers

$$\begin{aligned} \rho_c(\mathcal{C}, J) &:= (\dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c)))/m, \\ \rho_r(\mathcal{C}, K) &:= (\dim(\mathcal{C}) - \dim(\mathcal{C}(K^\perp, r)))/n. \end{aligned}$$

For simplicity of notation, in the sequel we sometimes drop the index \mathcal{C} and denote the rank functions simply by ρ_c and ρ_r . The following result shows that a rank-metric code $\mathcal{C} \subseteq \text{Mat}$ gives rise to a pair of q -polymatroids via ρ_c and ρ_r .

Theorem 5.3 *Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code. The pairs (\mathbb{F}_q^n, ρ_c) and (\mathbb{F}_q^m, ρ_r) are q -polymatroids.*

To prove the theorem we need a preliminary result, whose proof is left to the reader.

Lemma 5.4 *Let $I, J \subseteq \mathbb{F}_q^n$ be subspaces. We have:*

$$\text{Mat}(I \cap J, c) = \text{Mat}(I, c) \cap \text{Mat}(J, c) \quad \text{and} \quad \text{Mat}(I + J, c) = \text{Mat}(I, c) + \text{Mat}(J, c).$$

Proof of Theorem 5.3 We prove that (\mathbb{F}_q^n, ρ_c) is a q -polymatroid. The proof that (\mathbb{F}_q^m, ρ_r) is a q -polymatroid is completely analogous, hence we omit it.

We start by proving (P1). It is clear from the definition that $\rho_c(J) \geq 0$. The other inequality follows from [17, Lemma 28]:

$$\rho_c(J) = (\dim(\mathcal{C}) - (\dim(\mathcal{C}) - m(n - \dim J^\perp) + \dim(\mathcal{C}^\perp(J))))/m \leq \dim(J).$$

Now let $I, J \subseteq \mathbb{F}_q^n$ such that $I \subseteq J$. Then $\mathcal{C}(J^\perp, c) \subseteq \mathcal{C}(I^\perp, c)$, thus $\rho_c(I) \leq \rho_c(J)$. This establishes (P2). For (P3), we have

$$\begin{aligned} & \dim \mathcal{C}((I + J)^\perp, c) + \dim \mathcal{C}((I \cap J)^\perp, c) \\ &= \dim(\mathcal{C} \cap \text{Mat}(I^\perp \cap J^\perp, c)) + \dim(\mathcal{C} \cap \text{Mat}(I^\perp + J^\perp, c)) \\ &\geq \dim(\mathcal{C} \cap \text{Mat}(I^\perp, c) \cap \text{Mat}(J^\perp, c)) + \dim((\mathcal{C} \cap (\text{Mat}(I^\perp, c) \\ &\quad + (\mathcal{C} \cap \text{Mat}(J^\perp, c)))) \\ &= \dim(\mathcal{C} \cap \text{Mat}(I^\perp, c)) + \dim(\mathcal{C} \cap \text{Mat}(J^\perp, c)), \end{aligned}$$

where the first equality follows from [17, Lemma 27]. The inequality follows from combining Lemma 5.4 with $\mathcal{C} \cap (\text{Mat}(I^\perp, c) + \text{Mat}(J^\perp, c)) \supseteq (\mathcal{C} \cap \text{Mat}(I^\perp, c)) + (\mathcal{C} \cap \text{Mat}(J^\perp, c))$. □

Notation 5.5 The q -polymatroids associated with a rank-metric code $\mathcal{C} \subseteq \text{Mat}$ are denoted by $P(\mathcal{C}, c)$ and $P(\mathcal{C}, r)$, respectively.

6 Structural properties of codes via q -polymatroids

In this section, we investigate some connections between rank-metric codes and the associated q -polymatroids. We show that the q -polymatroids associated with a code \mathcal{C} determine the dimension of the code and its minimum distance, and characterize the property of being MRD.

Proposition 6.1 *Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code. Then*

$$\dim(\mathcal{C}) = m \cdot \rho_c(\mathcal{C}, \mathbb{F}_q^n) = n \cdot \rho_r(\mathcal{C}, \mathbb{F}_q^m).$$

The above result follows directly from the definitions. We now relate the minimum distance of a code to the rank functions of the associated q -polymatroids.

Proposition 6.2 *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero rank-metric code. The following are equivalent:*

- (1) $d(\mathcal{C}) \geq d$,
- (2) $\rho_c(J) = \dim(\mathcal{C})/m$ for all $J \subseteq \mathbb{F}_q^n$ with $\dim(J) \geq n - d + 1$,
- (3) $\rho_r(K) = \dim(\mathcal{C})/n$ for all $K \subseteq \mathbb{F}_q^m$ with $\dim(K) \geq m - d + 1$.

Proof It is easy to see that the following are equivalent:

- 1' $d(\mathcal{C}) \geq d$,
 2' $\mathcal{C}(J, c) = \{0\}$ for all $J \subseteq \mathbb{F}_q^n$ with $\dim(J) \leq d - 1$,
 3' $\mathcal{C}(K, r) = \{0\}$ for all $K \subseteq \mathbb{F}_q^m$ with $\dim(K) \leq d - 1$.

By definition, for all $J \subseteq \mathbb{F}_q^n$ and $K \subseteq \mathbb{F}_q^m$ we have $m\rho_c(J) = \dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c))$ and $n\rho_r(K) = \dim(\mathcal{C}) - \dim(\mathcal{C}(K^\perp, r))$. Hence (2) \Leftrightarrow (2') and (3) \Leftrightarrow (3'). \square

Therefore, the minimum distance of a rank-metric code can be expressed in terms of the rank function of one of the associated q -polymatroids as follows.

Corollary 6.3 *Let $0 \neq \mathcal{C} \subseteq \text{Mat}$. The minimum distance of \mathcal{C} is*

$$\begin{aligned} d(\mathcal{C}) &= n + 1 - \min \left\{ d \mid \rho_c(J) = \frac{\dim(\mathcal{C})}{m} \text{ for all } J \subseteq \mathbb{F}_q^n \text{ with } \dim(J) = d \right\} \\ &= m + 1 - \min \left\{ d \mid \rho_r(K) = \frac{\dim(\mathcal{C})}{n} \text{ for all } K \subseteq \mathbb{F}_q^m \text{ with } \dim(K) = d \right\}. \end{aligned}$$

This allows us to characterize the property of being MRD in terms of the rank function of one of the associated q -polymatroids.

Theorem 6.4 *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero code of minimum distance d . The following are equivalent:*

- (1) \mathcal{C} is MRD,
- (2) $\rho_c(J) = \dim(J)$ for all $J \subseteq \mathbb{F}_q^n$ with $\dim(J) \leq n - d + 1$,
- (3) $\rho_c(J) = \dim(J)$ for some $J \subseteq \mathbb{F}_q^n$ with $\dim(J) = n - d + 1$.

Proof Assume that \mathcal{C} is MRD. We claim that

$$\dim(\mathcal{C}(J, c)) = \dim(\mathcal{C}) - m(n - \dim(J)) \text{ for all } J \subseteq \mathbb{F}_q^n \text{ with } \dim(J) \geq d - 1.$$

This is straightforward if $\dim(J) = d - 1$. When $\dim(J) \geq d$, it follows from [19, Lemma 48]. Let $J \subseteq \mathbb{F}_q^n$ be a subspace with $\dim(J) \leq n - d + 1$. Since $\dim(J^\perp) \leq d - 1$ and $\dim(\mathcal{C}(J, c)) = \dim(\mathcal{C}) - m(n - \dim(J))$, we obtain

$$m\rho_c(J) = \dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c)) = \dim(\mathcal{C}) - \dim(\mathcal{C}) + m \dim(J) = m \dim(J).$$

This establishes (1) \Rightarrow (2).

It is clear that (2) implies (3). So we assume that (3) holds and prove (1). Since $\dim(J) = n - d + 1$, then $\dim(J^\perp) = d - 1$, therefore $\dim(\mathcal{C}(J^\perp, c)) = 0$. It follows that

$$m \dim(J) = m\rho_c(J) = \dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c)) = \dim(\mathcal{C}),$$

from which we obtain $\dim(\mathcal{C}) = m \dim(J) = m(n - d + 1)$. Hence \mathcal{C} is MRD. \square

Remark 6.5 If $m = n$ and $0 \neq \mathcal{C} \subseteq \text{Mat}$, then the same proof as in Theorem 6.4 shows that the following are equivalent:

- \mathcal{C} is MRD,
- $\rho_{\mathcal{C}}(K) = \dim(K)$ for all $K \subseteq \mathbb{F}_q^m$ with $\dim(K) = m - d + 1$
- $\rho_{\mathcal{C}}(K) = \dim(K)$ for some $K \subseteq \mathbb{F}_q^m$ with $\dim(K) = m - d + 1$.

Combining Proposition 6.2 and Theorem 6.4, we obtain an explicit formula for the rank function of the (column) q -polymatroid associated with an MRD code.

Corollary 6.6 *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero MRD code of minimum distance d . Then for all $J \subseteq \mathbb{F}_q^n$ we have*

$$\rho_{\mathcal{C}}(J) = \begin{cases} n - d + 1 & \text{if } \dim(J) \geq n - d + 1, \\ \dim(J) & \text{if } \dim(J) \leq n - d + 1. \end{cases} \tag{1}$$

In particular, the q -polymatroid associated with an MRD code has an integer-valued rank function, i.e., it is a q -matroid. It is in fact the uniform q -matroid, as explained in [10, Example 4.16]

It is natural to expect that equivalent rank-metric codes give rise to equivalent q -polymatroids. This is true in the following precise sense.

Proposition 6.7 *Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \text{Mat}$ be rank-metric codes. Assume $\mathcal{C}_1 \sim \mathcal{C}_2$. If $m > n$, then $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c)$ and $P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, r)$. If $n = m$, then one of the following holds:*

- $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c)$ and $P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, r)$,
- $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, r)$ and $P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, c)$.

Proof Since $\mathcal{C}_1 \sim \mathcal{C}_2$, then either $\mathcal{C}_2 = AC_1B$ for some invertible A, B , or $\mathcal{C}_2 = AC_1^tB$ for some invertible A, B and $m = n$. Since the proofs are similar, we only treat the case when there exist invertible matrices A, B such that $\mathcal{C}_2 = AC_1B$. Let $\psi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ be the \mathbb{F}_q -linear isomorphism associated with the matrix A with respect to the standard basis. Fix a subspace $J \subseteq \mathbb{F}_q^n$. Multiplication by A on the left and B on the right induces a bijection

$$\mathcal{C}_1(J^\perp, c) \rightarrow \mathcal{C}_2(\psi(J^\perp), c). \tag{2}$$

Let $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ denote the \mathbb{F}_q -linear isomorphism associated with the matrix $(A^{-1})^t$ with respect to the standard basis. Then we have $\psi(J^\perp) = \varphi(J)^\perp$, hence bijection (2) can be thought of as a bijection

$$\mathcal{C}_1(J^\perp, c) \rightarrow \mathcal{C}_2(\varphi(J)^\perp, c). \tag{3}$$

Therefore, for all subspaces $J \subseteq \mathbb{F}_q^n$ we have $\rho_{\mathcal{C}_1}(J) = \rho_{\mathcal{C}_2}(\varphi(J))$. This establishes the q -polymatroid equivalence $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c)$. The equivalence $P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, r)$ can be shown similarly. \square

Proposition 6.7 says that equivalent codes have equivalent associated q -polymatroids. The next example shows that the converse is false in general, i.e., that inequivalent codes may have equivalent (in fact, even identical) associated q -polymatroids.

Example 6.8 Let $q = 2$ and $m = n = 4$. Let \mathcal{C}_1 be the code of [2, Example 7.2], i.e., the code generated by the four linearly independent binary matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

The code \mathcal{C}_1 is MRD and has minimum distance $d(\mathcal{C}_1) = 4$. Let \mathcal{C}_2 be a rank-metric code obtained from a Gabidulin code $C \subseteq \mathbb{F}_{2^4}^4$ of minimum distance 4 via Proposition 2.12. By [2, Example 7.2], the code \mathcal{C}_1 has covering radius $\text{cov}(\mathcal{C}_1) = 2$, while it is well known that $\text{cov}(\mathcal{C}_2) = d(C) - 1 = 3$. Since the covering radius of a code is preserved under isometries, we conclude that the codes \mathcal{C}_1 and \mathcal{C}_2 are not equivalent.

On the other hand, the four codes \mathcal{C}_1 , \mathcal{C}_2 , \mathcal{C}_1^t and \mathcal{C}_2^t are all MRD with the same parameters. Therefore, by Corollary 6.6 the rank function of their q -polymatroids is determined and given by the formula in (1). This shows that $P(\mathcal{C}_1, c) = P(\mathcal{C}_1, r) = P(\mathcal{C}_2, c) = P(\mathcal{C}_2, r)$, although $\mathcal{C}_1 \not\approx \mathcal{C}_2$.

It is known from [10] that a vector rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ gives rise to a q -matroid $M(C)$ on \mathbb{F}_q^n . In our notation, $M(C) = P(\Gamma(C), c)$, where Γ is any \mathbb{F}_q -basis of \mathbb{F}_{q^m} .

Proposition 6.9 Let $C \subseteq \mathbb{F}_{q^m}^n$ be a vector rank-metric code, and let Γ, Γ' be \mathbb{F}_q -bases of \mathbb{F}_{q^m} . We have $P(\Gamma(C), c) = P(\Gamma'(C), c)$ and $P(\Gamma(C), r) \sim P(\Gamma'(C), r)$.

Proof The statement that $P(\Gamma(C), c) = P(\Gamma'(C), c)$ follows from [10, Corollary 4.7]. The statement that $P(\Gamma(C), r) \sim P(\Gamma'(C), r)$ follows by Propositions 2.13 and 6.7. \square

We continue by showing that there exist rank-metric codes whose associated q -polymatroids are not q -matroids. Even more, in the next example we show that there are q -polymatroids such that no nonzero multiple of their rank function defines a q -matroid.

Example 6.10 Let $q = 3$ and $n = m = 2$. Let \mathcal{C} be a rank-metric code generated by the matrices

$$M_1 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_2 := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad M_3 := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Consider the subspaces $J := \langle (1, 0) \rangle$ and $I := \langle (0, 1) \rangle$. Since $\mathcal{C}(J^\perp, c) = \langle M_3 \rangle$, we have $\rho_c(\mathcal{C}, J) = 1$. As $\mathcal{C}(I^\perp, c) = \langle M_1, M_2 \rangle$, then $\rho_c(\mathcal{C}, I) = 1/2$. Hence $P(\mathcal{C}, c)$ is a q -polymatroid which is not a q -matroid.

Let $\alpha \in \mathbb{R}$ with $\alpha \neq 0$, and consider the function $\rho := \alpha \rho_c$. Since $\rho(J) = \alpha$, in order for ρ to be the rank function of a q -polymatroid it must be $0 < \alpha \leq 1$. Then $\rho(I) = \alpha/2$ is not an integer, so ρ cannot be the rank function of a q -matroid.

7 Generalized weights as q -polymatroid invariants

In this section, we provide further evidence that the q -polymatroids associated with a rank-metric code adequately capture the structure of the code. More precisely, in the next theorem we show that the generalized rank-weights of the code are an invariant of the associated q -polymatroids. Later in the section, we show that the property of being an optimal anticode can be characterized in terms of the rank function of the associated q -polymatroids.

Theorem 7.1 *Let $\mathcal{C} \subseteq \text{Mat}$ be a nonzero rank-metric code and let $1 \leq i \leq \dim(\mathcal{C})$ be an integer. If $n > m$, we have*

$$a_i(\mathcal{C}) = \min\{n - \dim(J) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C}) - m\rho_{\mathcal{C}}(\mathcal{C}, J) \geq i\}.$$

If $n = m$, we have

$$a_i(\mathcal{C}) = \min\{a_i(\mathcal{C}, c), a_i(\mathcal{C}, r)\},$$

where

$$\begin{aligned} a_i(\mathcal{C}, c) &:= \min\{n - \dim(J) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C}) - m\rho_{\mathcal{C}}(\mathcal{C}, J) \geq i\}, \\ a_i(\mathcal{C}, r) &:= \min\{m - \dim(K) \mid K \subseteq \mathbb{F}_q^m, \dim(\mathcal{C}) - n\rho_r(\mathcal{C}, K) \geq i\}. \end{aligned}$$

Proof Let $J \subseteq \mathbb{F}_q^n$, then by [17, Lemma 26]

$$\dim(\text{Mat}(J^\perp, c)) = m \dim(J^\perp) = m(n - \dim(J)). \tag{4}$$

Assume that $m > n$. By [4, Theorem 6], the optimal anticodes in Mat are the spaces of the form $\text{Mat}(J^\perp, c)$, where J ranges over the subspaces of \mathbb{F}_q^n . Therefore,

$$\begin{aligned} m \cdot a_i(\mathcal{C}) &= \min\{\dim(\text{Mat}(J^\perp, c)) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C} \cap \text{Mat}(J^\perp, c)) \geq i\} \\ &= m \cdot \min\{n - \dim(J) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C}) - m\rho_{\mathcal{C}}(\mathcal{C}, J) \geq i\}, \end{aligned}$$

where the last equality follows from (4) and the definition of $\rho_{\mathcal{C}}(\mathcal{C}, J)$.

Now assume that $n = m$. By [4, Theorem 4], the anticodes in Mat are the spaces of the form $\text{Mat}(J^\perp, c)$ or $\text{Mat}(J^\perp, r)$, as J ranges over the subspaces of \mathbb{F}_q^n . Then

$$\begin{aligned} a_i(\mathcal{C}) &= \frac{1}{n} \min \left\{ \dim(\text{Mat}(J^\perp, c)) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C} \cap \text{Mat}(J^\perp, c)) \geq i \right\} \\ &\quad \cup \left\{ \dim(\text{Mat}(J^\perp, r)) \mid J \subseteq \mathbb{F}_q^n, \dim(\mathcal{C} \cap \text{Mat}(J^\perp, r)) \geq i \right\} \\ &= \min\{a_i(\mathcal{C}, c), a_i(\mathcal{C}, r)\}, \end{aligned}$$

where the last equality follows from (4) and the definition of $\rho_{\mathcal{C}}(\mathcal{C}, J), \rho_r(\mathcal{C}, J)$. \square

In the next theorem, we prove that the property of being an optimal anticode is captured by the rank function of the associated q -polymatroids.

Theorem 7.2 *Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code and let $t = \maxrk(\mathcal{C})$. The following are equivalent:*

1. \mathcal{C} is an optimal anticode,
2. $\left\{ \rho_c(\mathcal{C}, J) \mid J \subseteq \mathbb{F}_q^n \right\} = \{0, 1, \dots, t\}$, or $\left\{ \rho_r(\mathcal{C}, J) \mid J \subseteq \mathbb{F}_q^n \right\} = \{0, 1, \dots, t\}$ and $m = n$,
3. $\rho_c(\mathcal{C}, \mathbb{F}_q^n) = t$, or $\rho_r(\mathcal{C}, \mathbb{F}_q^n) = t$ and $m = n$.

In particular, the q -polymatroid associated with an optimal anticode is a q -matroid.

Proof (1) \Rightarrow (2) By [4, Theorems 4 and 6], either $\mathcal{C} = \text{Mat}(K, c)$ for a t -dimensional subspace $K \subseteq \mathbb{F}_q^n$, or $\mathcal{C} = \text{Mat}(K, r)$ for a t -dimensional subspace $K \subseteq \mathbb{F}_q^m$, where the latter is only possible if $m = n$. We assume that $\mathcal{C} = \text{Mat}(K, c)$, as the proof in the other situation is analogous. One has, for all $J \subseteq \mathbb{F}_q^n$,

$$\rho_c(\mathcal{C}, J) = (mt - \dim(\text{Mat}(K, c) \cap \text{Mat}(J^\perp, c)))/m = t - \dim(K \cap J^\perp),$$

where the second equality follows from Lemma 5.4 and [17, Lemma 26]. Hence we obtain

$$\begin{aligned} \left\{ \rho_c(\mathcal{C}, J) \mid J \subseteq \mathbb{F}_q^n \right\} &= \{0, 1, \dots, t\} \text{ if } \mathcal{C} = \text{Mat}(K, c), \\ \left\{ \rho_r(\mathcal{C}, J) \mid J \subseteq \mathbb{F}_q^n \right\} &= \{0, 1, \dots, t\} \text{ if } \mathcal{C} = \text{Mat}(K, r). \end{aligned}$$

(3) \Rightarrow (1) We have

$$\rho_c(\mathcal{C}, \mathbb{F}_q^n) = \dim(\mathcal{C})/m \text{ and } \max\{\rho_r(\mathcal{C}, K) \mid K \subseteq \mathbb{F}_q^m\} = \rho_r(\mathcal{C}, \mathbb{F}_q^m) = \dim(\mathcal{C})/n.$$

Then either $\dim(\mathcal{C})/m$, or $\dim(\mathcal{C})/n = t$ and $m = n$. Either way one has $\dim(\mathcal{C}) = mt$, hence \mathcal{C} is an optimal anticode. \square

Corollary 7.3 *Let $\mathcal{C} \subseteq \text{Mat}$ be an optimal anticode and let $t = \maxrk(\mathcal{C})$. If $m > n$, then $P(\mathcal{C}, c) \sim (\mathbb{F}_q^n, \rho)$ where*

$$\rho(J) = \dim(J + \langle e_1, \dots, e_{n-t} \rangle) - (n - t) \tag{5}$$

and e_i denotes the i -th vector of the standard basis of \mathbb{F}_q^n . If $m = n$, then either $P(\mathcal{C}, c) \sim (\mathbb{F}_q^n, \rho)$ or $P(\mathcal{C}, r) \sim (\mathbb{F}_q^n, \rho)$.

Proof If $m > n$, then $\mathcal{C} = \text{Mat}(K, c)$ for some $K \subseteq \mathbb{F}_q^n$ of $\dim(K) = t$. If $m = n$, then either $\mathcal{C} = \text{Mat}(K, c)$ or $\mathcal{C}^t = \text{Mat}(K, c)$, for some $K \subseteq \mathbb{F}_q^n$ of $\dim(K) = t$. Since $P(\mathcal{C}^t, c) = P(\mathcal{C}, r)$, it suffices to consider the case when $\mathcal{C} = \text{Mat}(K, c)$. Up to code equivalence, we may also assume without loss of generality that $K = \langle e_{n-t+1}, \dots, e_n \rangle$.

It follows from the proof of Theorem 7.2 that $\rho_c(\mathcal{C}, J) = t - \dim(K \cap J^\perp)$. Therefore, $\rho_c(\mathcal{C}, J) = t - (n - \dim(\langle e_{n-t+1}, \dots, e_n \rangle \cap J^\perp)) = \dim(J + \langle e_1, \dots, e_{n-t} \rangle) - (n - t)$. \square

Remark 7.4 One consequence of our results is that, in certain cases, the generalized weights of a code determine the associated q -polymatroid $P(\mathcal{C}, c)$ up to equivalence. This is the case, e.g., in the following situations:

- if \mathcal{C} has the generalized weights of an MRD code, then \mathcal{C} is MRD and $P(\mathcal{C}, c)$ is the uniform q -matroid (see Corollary 6.6),
- if \mathcal{C} has the generalized weights of an optimal anticode, then \mathcal{C} is an optimal anticode and $P(\mathcal{C}, c)$ is the q -matroid described in Corollary 7.3,
- if $\dim(\mathcal{C}) = 1$, then $\mathcal{C} = \langle M \rangle$ and $a_1(\mathcal{C}) = d_{\min}(\mathcal{C}) = \text{rk}(M)$. Moreover, $P(\mathcal{C}, c)$ is given by

$$\rho_c(\mathcal{C}, J) = \begin{cases} 0 & \text{if } \text{colsp}(M) \subseteq J^\perp, \\ \frac{1}{m} & \text{else.} \end{cases}$$

Notice that if $\mathcal{C}_1 = \langle M_1 \rangle$ and $\mathcal{C}_2 = \langle M_2 \rangle$ have the same minimum distance, then $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c)$. In fact, $\rho_c(\mathcal{C}_1, J) = \rho_c(\mathcal{C}_2, \varphi(J))$, where $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is an \mathbb{F}_q -linear isomorphism such that $\varphi(\text{colsp}(M_1)) = \text{colsp}(M_2)$.

One should, however, not expect this to be the case in general. In other words, the generalized weights of a rank-metric code \mathcal{C} are invariants of the associated q -polymatroid $P(\mathcal{C}, c)$, but they do not determine it, as the next example shows. Similar examples may be found for rectangular matrices.

Example 7.5 Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \text{Mat}_{2 \times 2}(\mathbb{F}_2)$,

$$\mathcal{C}_1 = \left\langle \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) \right\rangle, \quad \mathcal{C}_2 = \left\langle \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) \right\rangle.$$

The codes \mathcal{C}, \mathcal{D} have generalized weights $a_1(\mathcal{C}_1) = a_1(\mathcal{C}_2) = 1$ and $a_2(\mathcal{C}_1) = a_2(\mathcal{C}_2) = 2$. In fact, any rank-metric code of dimension 2 and minimum distance 1 which is not an optimal anticode has the same generalized weights as \mathcal{C}_1 and \mathcal{C}_2 .

Let $P(\mathcal{C}_1, c) = (\mathbb{F}_2^2, \rho_1)$ and $P(\mathcal{C}_2, c) = (\mathbb{F}_2^2, \rho_2)$. Let $J \subseteq \mathbb{F}_2^2$ be a 1-dimensional linear subspace. Then

$$\rho_1(J) = \begin{cases} \frac{1}{2} & \text{if } J = \langle (0, 1) \rangle \\ 1 & \text{if } J = \langle (1, 0) \rangle \text{ or } J = \langle (1, 1) \rangle \end{cases}$$

while

$$\rho_2(J) = \begin{cases} \frac{1}{2} & \text{if } J = \langle (0, 1) \rangle \text{ or } J = \langle (1, 0) \rangle, \\ 1 & \text{if } J = \langle (1, 1) \rangle \end{cases}$$

Therefore, $P(\mathcal{C}_1, c) \approx P(\mathcal{C}_2, c)$. Notice moreover that $P(\mathcal{C}_1, c) \sim P(\mathcal{C}_1, r)$ and $P(\mathcal{C}_2, c) \sim P(\mathcal{C}_2, r)$.

8 Duality

In this last section of the paper, we establish a connection between the notions of code duality and q -polymatroid duality. We start by showing that the q -polymatroids associated with the dual code \mathcal{C}^\perp are the duals of the q -polymatroids associated with the original code \mathcal{C} .

Theorem 8.1 *Let $\mathcal{C} \subseteq \text{Mat}$ be a rank-metric code. We have $P(\mathcal{C}, c)^* = P(\mathcal{C}^\perp, c)$ and $P(\mathcal{C}, r)^* = P(\mathcal{C}^\perp, r)$.*

Proof We only show the result for $P(\mathcal{C}, c)$. The proof for $P(\mathcal{C}, r)$ is analogous. Let $J \subseteq \mathbb{F}_q^n$ be a subspace. Since $\rho_c(\mathcal{C}, J) = (\dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c)))/m$, then

$$\begin{aligned}\rho_c^*(\mathcal{C}, J) &= \dim(J) - \dim(\mathcal{C})/m + (\dim(\mathcal{C}) - \dim(\mathcal{C}(J, c)))/m \\ &= \dim(J) - \dim(\mathcal{C}(J, c))/m.\end{aligned}$$

Therefore, by [17, Lemma 28] one has

$$m\rho_c^*(\mathcal{C}, J) - m\rho_c(\mathcal{C}^\perp, J) = m\dim(J) - \dim(\mathcal{C}^\perp) - \dim(\mathcal{C}) + mn - m\dim(J) = 0.$$

□

Finally, it is natural to ask how the q -polymatroids associated with the dual of a vector rank-metric code relate to the q -polymatroids associated with the original vector rank-metric code. It turns out that they are dual to each other, as the following result shows.

Corollary 8.2 *Let $C \subseteq \mathbb{F}_q^n$ be a vector rank-metric code, and let Γ be a basis of \mathbb{F}_q^m over \mathbb{F}_q . We have*

$$\begin{aligned}P(\Gamma(C^\perp), c) &= P(\Gamma^*(C), c)^* = P(\Gamma(C), c)^* \text{ and } P(\Gamma(C^\perp), r) \\ &= P(\Gamma^*(C), r)^* \sim P(\Gamma(C), r)^*\end{aligned}$$

where Γ^* is the dual of the basis Γ .

Proof Applying [17, Theorem 21] to C , we obtain $\Gamma(C^\perp) = \Gamma^*(C)^\perp$, hence $P(\Gamma(C^\perp), c) = P(\Gamma^*(C)^\perp, c)$ and $P(\Gamma(C^\perp), r) = P(\Gamma^*(C)^\perp, r)$. On the other hand, Theorem 8.1 gives $P(\Gamma^*(C)^\perp, c) = P(\Gamma^*(C), c)^*$ and $P(\Gamma^*(C)^\perp, r) = P(\Gamma^*(C), r)^*$. By Proposition 6.9 we have $P(\Gamma^*(C), c) = P(\Gamma(C), c)$ and $P(\Gamma^*(C), r) \sim P(\Gamma(C), r)$. Therefore, by Proposition 4.7 it follows that $P(\Gamma^*(C), c)^* = P(\Gamma(C), c)^*$ and $P(\Gamma^*(C), r)^* \sim P(\Gamma(C), r)^*$. □

Acknowledgements Elisa Gorla was partially supported by the Swiss National Science Foundation through Grant No. 200021_150207. Hiram H. López was partially supported by SNI, Mexico. Alberto Ravagnani was partially supported by the Swiss National Science Foundation through Grant No. P2NEP2_168527.

References

1. Berger, T.P.: Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Trans. Inform. Theory* **49**(11), 3016–3019 (2002)
2. Byrne, E., Ravagnani, A.: Covering radius of matrix codes endowed with the rank metric. *SIAM J. Discrete Math.* **31**(2), 927–944 (2017)
3. Crapo, H.: On the theory of combinatorial independence, Ph.D. Thesis, Massachusetts Institute of Technology, Dept. of Mathematics (1964)
4. de Seguins Pazzis, C.: The classification of large spaces of matrices with bounded rank. *Israel J. Math.* **208**(1), 219–259 (2015)
5. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A* **25**(3), 226–241 (1978)
6. Gabidulin, E.: Theory of codes with maximum rank distance. *Probl. Inf. Transm.* **1**(2), 1–12 (1985)
7. Gorla, E., Ravagnani, A.: Codes endowed with the rank metric. In: Greferath, M., Pavcevic, M., Vazquez-Castro, A., Silberstein, N. (eds.) *Random Network Coding and Designs Over $GF(q)$* . Signals and Communication Technology. Springer, Berlin (2018)
8. Hua, L.-K.: A theorem on matrices over a sfield and its applications. *Acta Math. Sin.* **1**, 109–163 (1951)
9. Jurrius, R., Pellikaan, R.: On defining generalized rank weights. *Adv. Math. Commun.* **11**(1), 225–235 (2017)
10. Jurrius, R., Pellikaan, R.: Defining the q -analogue of a matroid. *Electron. J. Combin.* **25**(3), 1–32 (2018)
11. Kløve, T.: The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$. *Discrete Math.* **23**, 159–168 (1978)
12. Kurihara, J., Matsumoto, R., Uyematsu, T.: Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans. Inform. Theory* **61**(7), 3912–3936 (2015)
13. Martínez-Peñas, U., Matsumoto, R.: Relative generalized matrix weights of matrix codes for universal security on wire-tap networks. *IEEE Trans. Inform. Theory* **64**(4), 2529–2549 (2018)
14. Oggier, F., Sboui, A.: On the existence of generalized rank weights. In: *IEEE ISIT-2012, International Symposium on Information Theory*, pp. 406–410 (2012)
15. Oxley, J.: *Matroid Theory*. Oxford Graduate Texts in Mathematics, 2nd edn. Oxford University Press, Oxford (2011)
16. Oxley, J., Whittle, G.: A characterization of Tutte invariants of 2-polymatroids. *J. Combin. Theory Ser. B* **59**(2), 210–244 (1993)
17. Ravagnani, A.: Rank-metric codes and their duality theory. *Des. Codes Cryptogr.* **80**(1), 197–216 (2016)
18. Ravagnani, A.: Generalized weights: an anticode approach. *J. Pure Appl. Algebra* **220**(5), 1946–1962 (2016)
19. Ravagnani, A.: Duality of codes supported on regular lattices, with an application to enumerative combinatorics. *Des. Codes Cryptogr.* **86**(9), 2035–2063 (2018)
20. Roth, R.M.: Maximum-rank array codes and their application to criss-cross error correction. *IEEE Trans. Inform. Theory* **37**(2), 328–336 (1991)
21. Shiromoto, K.: Codes with the rank metric and matroids. *Des. Codes Cryptogr.* (2018). <https://doi.org/10.1007/s10623-018-0576-0>
22. Wan, Z.-X.: A proof of the automorphisms of linear groups over a field of characteristic 2. *Scientia Sinica* **11**, 1183–1194 (1962)
23. Wan, Z.-X.: *Geometry of Matrices*. World Scientific, Singapore (1996)
24. Wei, V.: Generalized hamming weights for linear codes. *IEEE Trans. Inform. Theory* **37**(5), 1412–1418 (1991)
25. Welsh, D.: *Matroid Theory*. Dover Publications, INC., Mineola (1976)