



HAL
open science

Weighted Subspace Designs from q -Polymatroids

Eimear Byrne, Michela Ceria, Sorina Ionica, Relinde Jurrius

► **To cite this version:**

Eimear Byrne, Michela Ceria, Sorina Ionica, Relinde Jurrius. Weighted Subspace Designs from q -Polymatroids. *Journal of Combinatorial Theory, Series A*, 2024, 201. hal-03251251

HAL Id: hal-03251251

<https://hal.science/hal-03251251v1>

Submitted on 6 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

WEIGHTED SUBSPACE DESIGNS FROM q -POLYMATROIDS

EIMEAR BYRNE, MICHELA CERIA, SORINA IONICA, AND RELINDE JURRIUS

ABSTRACT. The Assmus-Mattson theorem gives a way to identify block designs arising from codes. This result was broadened to matroids and weighted designs by Britz et al. in 2009. In this work we present a further two-fold generalisation: first from matroids to polymatroids and also from sets to vector spaces. To achieve this, we study the characteristic polynomial of a q -polymatroid and outline several of its properties. We also derive a MacWilliams duality result and apply this to establish criteria on the weight enumerator of a q -polymatroid for which dependent spaces of the q -polymatroid form the blocks of a weighted subspace design.

1. INTRODUCTION

The characteristic polynomial of a matroid is a well studied object. It was first introduced as a matroid generalisation of the chromatic polynomial of a graph. It arises in critical problems, analyses of the Tutte polynomial, and is the subject of numerous identities [2]. For a thorough treatment of the subject see [20], for example.

In combinatorics, the concept of a q -analogue can be viewed as a generalisation from sets to vector spaces. Recently, the q -analogue of a matroid has been studied [11]. A generalisation of this is a q -polymatroid [9, 10, 17]. Similar to classical matroids, there are many interesting connections between q -(poly)matroids and rank-metric codes. In this paper we develop the theory of the characteristic polynomial of a q -polymatroid. We show the relation between the characteristic polynomial of a polymatroid and its dual, establishing a MacWilliams-like identity for q -polymatroids. In a similar line of research, Shiromoto [17] established a q -analogue of Greene's theorem.

Another motivation to study the characteristic polynomial is to establish a q -analogue of the Assmus-Mattson theorem [1]. This theorem gives a criterion for identifying a t -design as a collection of supports of codewords of fixed weight in a linear code. Since its publication in 1969 it has seen a number of generalisations [6, 13] and has been used widely to obtain new constructions of designs [8, 16]. In one of these results [3], the authors define a weighted t -design as a generalisation of a classical t -design and give criteria for identifying such an object among the dependent sets of a matroid of a fixed cardinality. A weighted t -design is a collection of subsets \mathcal{B} of a fixed cardinality k chosen from an n -set of points \mathcal{P} together with a function f defined on \mathcal{B} such that for any t -set $T \subset \mathcal{P}$ the sum $\sum_{B \in \mathcal{B}: T \subset B} f(B)$ is independent of T . In the case that f is the characteristic polynomial that takes the value 1 if and only if $T \subset B$, the weighted t -design is an ordinary design.

In this paper, we generalise the results of [3] to q -polymatroids, which is a two-fold generalisation: first from matroids to polymatroids and also from sets to vector spaces. Hence the results presented here give a q -analogue of their result. The q -analogue of a weighted t -design is a weighted subspace design; in the definition shown above we replace the collection of subsets \mathcal{B} with a collection of subspaces of a fixed dimension k and T with a t -dimensional subspace.

In Section 2 we study q -polymatroids and their necessary properties for this work. In Section 3 we outline properties of the characteristic polynomial of a q -polymatroid that will be used later and in Section 4 look at the case of q -polymatroids arising from matrix codes. In Section 5 we give a version of the MacWilliams duality result for q -polymatroids. In Section 6 we give criteria for identifying when the dependent spaces of a q -polymatroid are the blocks of

1991 *Mathematics Subject Classification.* 05B35, 05A30, 11T71.

Key words and phrases. q -analogue, q -polymatroid, weighted subspace design, characteristic polynomial.

a weighted t -subspace design.

Notation 1. Throughout, we let n denote a fixed positive integer and we will let q denote a fixed prime power. We let E denote an n -dimensional vector space over the finite field \mathbb{F}_q of order q . We let $\mathcal{L}(E)$ denote the lattice of all subspaces of E , ordered with respect to inclusion, which we denote by \leq . We will write $U < V$ for $U, V \leq E$ if U is strictly contained in V . The join of a pair of subspaces is their vector space sum and the meet of a pair of subspaces is their intersection.

2. q -POLYMATROIDS

q -Polymatroids and their connections to linear codes were introduced in [10] and [17]. Their properties have been further developed in [9]. In our presentation, we will not assume that q -polymatroids are *representable*, that is, we will not assume that the q -polymatroids under consideration here are constructed from rank-metric codes over \mathbb{F}_q . We use the following definition of a q -polymatroid from [17], since it suits our purposes to have an integer valued function in what follows.

Definition 2. A (q, r) -polymatroid is a pair $M = (E, \rho)$ for which $r \in \mathbb{N}_0$ and ρ is a function $\rho : \mathcal{L}(E) \rightarrow \mathbb{N}_0$ satisfying the following axioms.

- (R1) For all $A \leq E$, $0 \leq \rho(A) \leq r \dim A$.
- (R2) For all $A, B \leq E$, if $A \leq B$ then $\rho(A) \leq \rho(B)$.
- (R3) For all $A, B \leq E$, $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

If it is not necessary to specify r , we will simply refer to such an object as a q -polymatroid. If M is a q -polymatroid, we denote its rank function by ρ_M . Note that a $(q, 1)$ -polymatroid is a q -matroid.

Recall that a lattice isomorphism between a pair of lattices $(\mathcal{L}_1, \vee_1, \wedge_1), (\mathcal{L}_2, \vee_2, \wedge_2)$ is a bijective function $\varphi : \mathcal{L}_1 \rightarrow \mathcal{L}_2$ that preserves the meet and join, that is, for all $x, y \in \mathcal{L}_1$ we have that $\varphi(x \wedge_1 y) = \varphi(x) \wedge_2 \varphi(y)$ and $\varphi(x \vee_1 y) = \varphi(x) \vee_2 \varphi(y)$. We hence define a notion of equivalence between q -polymatroids.

Definition 3. Let E_1, E_2 be \mathbb{F}_q -linear spaces. Let $M_1 = (E_1, \rho_1)$ and $M_2 = (E_2, \rho_2)$ be q -polymatroids. We say that M_1 and M_2 are **lattice-equivalent** if there exists a lattice isomorphism $\varphi : \mathcal{L}(E_1) \rightarrow \mathcal{L}(E_2)$ such that $\rho_1(A) = \rho_2(\varphi(A))$ for all $A \leq E_1$. In this case we write $M_1 \cong M_2$.

Remark 4. This definition is not the same as the definition of equivalence of q -polymatroids given in [9] and [10]. The q -polymatroids (E_1, ρ_1) and (E_2, ρ_2) are **equivalent** if there exists an \mathbb{F}_q -linear isomorphism $\tau : E_1 \rightarrow E_2$ such that $\rho_1(A) = \rho_2(\tau(A))$ for all $A \leq E_1$. Since every vector space isomorphism induces a lattice isomorphism, equivalence implies lattice-equivalence for q -polymatroids.

Definition 5. Let F be an \mathbb{F}_q -vector space. We denote by b_F a fixed non-degenerate symmetric bilinear form (which we call an inner product) on F . For any subspace $U \leq F$ we denote the orthogonal complement of U with respect to b_F by $U^{\perp(F)} := \{a \in F : b_F(u, a) = 0 \forall u \in U\}$. We write $U^\perp := U^{\perp(E)}$.

The *dual* q -polymatroid was defined in [10, 17].

Definition 6. Let $M = (E, \rho)$ be a (q, r) -polymatroid. For every subspace $A \leq E$, define $\rho^*(A) := r \dim(A) - \rho(E) + \rho(A^\perp)$. Then $M^* := (E, \rho^*)$ is a (q, r) -polymatroid called the **dual** of M .

As noted in [9], the definition of the dual of M depends on the choice of inner product b_E , but all such choices yield equivalent duals.

It is easy to see that for a map $\rho : \mathcal{L}(E) \rightarrow \mathbb{N}_0$ satisfying the axioms (R1)-(R3), the restriction of that map to $\mathcal{L}(T)$, for each subspace $T \leq E$, also yields a q -polymatroid.

Definition 7. Let $M = (E, \rho)$ be a (q, r) -polymatroid and let $T \leq E$. For every subspace $A \leq T$, define $\rho_{M|_T}(A) := \rho(A)$. Then $M|_T := (T, \rho_{M|_T})$ is a (q, r) -polymatroid called the **restriction** of M to T .

Definition 8. Let $I \leq E$ and let $M = (E, \rho)$ be a (q, r) -polymatroid. We say that I is an **independent space** of M if $\rho(I) = r \dim I$. A subspace that is not independent, is called a **dependent space** of M . We call $C \leq E$ a **circuit** of M if it is a minimal dependent space with respect to inclusion. We call $T \leq E$ a **cocircuit** of M if it is a circuit of M^* .

For q -matroids, the following result is (I2) of the independence axioms (see [5, Definition 7]). We show that this holds for q -polymatroids.

Lemma 9. *Let $M = (E, \rho)$ be a (q, r) -polymatroid and let $I \leq E$ be an independent space of M . Then every subspace of I is independent.*

Proof. Since I is independent, we have $\rho(I) = r \dim(I)$. Let J, J' be subspaces of I such that I is a direct sum of J and J' . By (R1) and applying semimodularity (R3) to J and J' we get

$$\begin{aligned} r \dim(J) + r \dim(J') &\geq \rho(J) + \rho(J') \geq \rho(J + J') + \rho(J \cap J') \\ &= \rho(I) = r \dim(I) = r(\dim(J) + \dim(J')) \end{aligned}$$

Since $\rho(J) \leq r \dim(J)$ and $\rho(J') \leq r \dim(J')$ we must have that $\rho(J) = r \dim(J)$ and $\rho(J') = r \dim(J')$ and the result follows. \square

From the above lemma, it follows that $C \leq E$ is a circuit of a q -polymatroid if it is a dependent space whose proper subspaces are all independent. In the case of a q -matroid, we have $\rho(I) = \dim(I)$ for any independent space of the q -matroid. Furthermore, if I is a maximal independent subspace of $A \leq E$ then $\rho(A) = \rho(I)$.

Proposition 10. *Let $M = (E, \rho)$ be a q -matroid and let $T \leq E$. Define a map*

$$\rho_{M/T} : \mathcal{L}(E/T) \longrightarrow \mathbb{Z} : A \mapsto \rho(A) - \rho(T).$$

Then $M/T := (E/T, \rho_{M/T})$ is a q -matroid.

Proof. It is easy to see that $\rho_{M/T}$ is well-defined, since every subspace of E/T corresponds to a unique subspace of E that contains T . It is straightforward to see that the axioms (R2) and (R3) hold for M/T , given that M is a q -matroid. Let $A \leq E$ such that $T \leq A$. Let $I \leq E$ be a maximal independent space of T and let J be a maximal independent subspace of A that contains I . The space J exists by [5, Lemma 23]. By definition, we have $\rho(A) = \rho(J) = \dim(J)$ and $\rho(T) = \rho(I) = \dim(I) = \dim(T \cap J)$. Therefore,

$$\begin{aligned} \rho_{M/T}(A/T) &= \rho(A) - \rho(T) = \dim(J) - \dim(T \cap J) = \dim(J/(T \cap J)) \\ &= \dim((J + T)/T) = \dim(J + T) - \dim(T) \\ &\leq \dim(A) - \dim(T) = \dim(A/T). \end{aligned}$$

\square

In fact, as shown in [9, Theorem 5.2] the statement holds for q -polymatroids as well, simply applying semimodularity. We thus have the following definition.

Definition 11. Let $M = (E, \rho)$ be a (q, r) -polymatroid and let $T \leq E$. We define the map $\rho_{M/T} : \mathcal{L}(E/T) \longrightarrow \mathbb{Z} : A \mapsto \rho(A) - \rho(T)$. Then $M/T := (E/T, \rho_{M/T})$ is a (q, r) -polymatroid called the **contraction** of M **from** T .

It will sometimes be more convenient for us to use the slightly less commonly used definition of contraction *to* a subspace.

Definition 12. Let $M = (M, \rho)$ be a (q, r) -polymatroid and let $X \leq E$. We denote by $M.X$ the q -polymatroid $M.X := (E/X^\perp, \rho_{E/X^\perp})$. We call $M.X$ the **contraction** of M **to** X .

In the language of classical matroids, the contraction of M to X is the contraction of M from $E - X$, that is $M.X = M/(E - X)$ (see [14, Chapter 3]). In the q -analogue we have $M.X := M/X^\perp$.

The following duality result is a straightforward extension of [11, Theorem 60]. It relates the contraction of a q -polymatroid from a subspace to a restriction of its dual q -polymatroid. We will make good use of this in Section 6, where we give a construction of weighted subspace designs from q -polymatroids.

Lemma 13. *Let $M = (E, \rho)$ be a (q, r) -polymatroid and let T be a subspace of E . Then,*

$$M^*/T \cong (M|_{T^\perp})^* \text{ and } (M/T)^* \cong M^*|_{T^\perp}.$$

Proof. Let $\phi : \mathcal{L}(E/T) \rightarrow \mathcal{L}(T^\perp)$ be defined by $\phi(X/T) = (X^\perp)^\perp(T^\perp)$, for each $X \leq E$ such that $T \leq X$ (in which case $X^\perp \leq T^\perp$). That is, $\phi(X/T)$ is the orthogonal complement of X^\perp in T^\perp , with respect to b_{T^\perp} . Clearly $\phi(E/T) = 0^\perp(T^\perp) = T^\perp$, $\phi(T) = (T^\perp)^\perp(T^\perp) = 0$ and if $T \leq X \leq Y$ then $Y^\perp \leq X^\perp$ and so $\phi(X/T) = (X^\perp)^\perp(T^\perp) \leq (Y^\perp)^\perp(T^\perp) = \phi(Y/T)$. Observe that for $T \leq X$ we have

$$\begin{aligned} \dim(\phi(X/T)) &= \dim((X^\perp)^\perp(T^\perp)) = \dim(T^\perp) - \dim(X^\perp) \\ &= \dim(X) - \dim(T) = \dim(X/T). \end{aligned}$$

Let A be subspaces of E satisfying $T \leq A \leq E$. We claim that $\rho_{M^*/T}(A/T) = (\rho_{M|_{T^\perp}})^*(\phi(A/T))$.

$$\begin{aligned} \rho_{M^*/T}(A/T) &= \rho^*(A) - \rho^*(T) \\ &= r \dim(A) - \rho(T^\perp) + \rho(A^\perp) - r \dim(T) \\ &= r \dim(A/T) - \rho_{M|_{T^\perp}}(T^\perp) + \rho_{M|_{T^\perp}}(A^\perp) \\ &= r \dim(\phi(A/T)) - \rho_{M|_{T^\perp}}(T^\perp) + \rho_{M|_{T^\perp}}(\phi(A/T)^\perp(T^\perp)) \\ &= (\rho_{M|_{T^\perp}})^*(\phi(A/T)). \end{aligned}$$

This shows that $M^*/T \cong (M|_{T^\perp})^*$. That $(M/T)^* \cong M^*|_{T^\perp}$ holds can be seen by replacing M with M^* in the previous identity and taking duals. \square

Remark 14. In fact, the above result holds even in terms of equivalence in the stronger sense [9, Definition 2.6 (a)], and not only lattice-equivalence, as was shown in Theorem 5.3 of the same paper. Note that in establishing the equivalence of these q -polymatroids, the vector space isomorphism depends on the choice of the bilinear form arising in the construction of the lattice isomorphism.

Lemma 15. *Let $M = (E, \rho)$ be a (q, r) -polymatroid and let $I \leq E$ be an independent space of M . Let $I \leq A \leq E$. Then A is independent in M if and only if A/I is independent in M/I . Moreover, if A is a circuit in M then A/I is a circuit in M .*

Proof. Let A be independent in M . Then

$$r \dim(A/I) = r \dim(A) - r \dim(I) = \rho(A) - \rho(I) = \rho_{M/I}(A/I),$$

hence A/I is an independent space of M/I . Conversely, if A/I is independent in M/I then

$$r \dim(A) - r \dim(I) = r \dim(A/I) = \rho_{M/I}(A/I) = \rho(A) - \rho(I) = \rho(A) - r \dim(I),$$

so $\rho(A) = r \dim(A)$.

Let A be a circuit in M . Any proper subspace of A/I has the form B/I for some unique $I \leq B < A$. Since A is a circuit, A/I is a dependent space in M/I , and B is an independent space of M . Therefore B/I is independent and so A/I is a circuit of M/I . \square

Example 16 (The Vámos q -Matroid). This q -matroid is constructed over $\mathcal{L}(\mathbb{F}_q^8)$. Choose the canonical basis for \mathbb{F}_q^8 denoted by e_1, \dots, e_8 . Moreover, we consider

$$\mathcal{C} := \{\langle e_1, e_2, e_3, e_4 \rangle, \langle e_1, e_2, e_5, e_6 \rangle, \langle e_3, e_4, e_5, e_6 \rangle, \langle e_3, e_4, e_7, e_8 \rangle, \langle e_5, e_6, e_7, e_8 \rangle\}.$$

For each $A \leq \mathbb{F}_q^8$, we define $\rho(A)$ as follows:

$$\rho(A) := \begin{cases} \dim(A) & \text{if } \dim(A) \leq 3, \\ 3 & \text{if } A \in \mathcal{C}, \\ 4 & \text{if } \dim(A) \geq 4 \text{ and } A \notin \mathcal{C}. \end{cases}$$

We prove that ρ is the rank function of a q -matroid. It is easy to see that (R1) and (R2) hold. Let us consider (R3). If the spaces A, B are both of dimension smaller than 4 or greater than 4, (R3) holds trivially. Indeed, the potential occurrence of a dependent 4-dimensional space can occur only on the left hand side of the inequality, making it stricter but without compromising it. Note also that if we only have the occurrence of independent 4-dimensional spaces then (R3) holds true. Let us consider now the interaction of 4-dimensional dependent spaces with the other spaces. As a first case, let $\dim(A) < 4$ and $\dim(B) = 4$, $\rho(B) = 3$. If $A \leq B$, $\rho(A+B) = \rho(B) = 3$ and $\rho(A \cap B) = \rho(A) = \dim(A)$ and then (R3) holds true. If $A \not\leq B$, there is at least a one-dimensional subspace of A not in B , therefore $\rho(A+B) = 4$, but this also means that $\dim(A \cap B) < \dim(A)$. Therefore $\rho(A+B) + \rho(A \cap B) \leq 4 + \dim(A) - 1 = \rho(A) + \rho(B) = \dim(A) + 3$, so also in this case (R3) is true. Let $\dim(A) = \dim(B) = 4$, $\rho(A) = 4$, $\rho(B) = 3$. Then $\rho(A+B) = 4$ and $\rho(A \cap B) \leq 3$ so (R3) is trivially true. Let $\dim(A) = \dim(B) = 4$, $\rho(A) = \rho(B) = 3$, $A \neq B$ (the equality case is trivial). Then $\rho(A+B) = 4$ and $\rho(A \cap B) \leq 2$ (indeed two 4 dimensional dependent space intersect in a space of dimension at most 2) thus (R3) is trivially true. Now suppose $\dim(A) > 4$, $\dim(B) = 4$, and $\rho(B) = 3$. In this case $\rho(A+B) = 4$ and $\rho(A \cap B) \leq 3$, making (R3) true again. Note that the set \mathcal{C} is the set of circuits of the Vámos q -matroid.

3. CHARACTERISTIC POLYNOMIAL OF A q -POLYMATROID

In this section, we introduce the characteristic polynomial of a q -polymatroid. This polynomial and its properties are well-studied in the case of a classical polymatroid [2, 21], in which case its coefficients are the Möbius coefficients of the lattice of subsets of $\{1, \dots, n\}$. In the q -polymatroid case the underlying lattice is the lattice of subspaces of E . We will use the characteristic polynomial to obtain a version of the MacWilliams identities for q -polymatroids.

3.1. The Möbius Function on a Lattice. Throughout this paper we will use the Möbius function (see, e.g. [19, Chapter 25]), which is fundamental to the definition of a characteristic polynomial. We recall some basic results.

Let (P, \leq) be a partially ordered set. The Möbius function for P is defined via the recursive formula

$$\mu(x, y) := \begin{cases} 1 & \text{if } x = y, \\ -\sum_{x \leq z < y} \mu(x, z) & \text{if } x < y, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 17 (Möbius Inversion Formula). *Let $f, g : P \rightarrow \mathbb{Z}$ be any two functions on a poset P . Then*

- (1) $f(x) = \sum_{x \leq y} g(y)$ if and only if $g(x) = \sum_{x \leq y} \mu(x, y)f(y)$.
- (2) $f(x) = \sum_{x \geq y} g(y)$ if and only if $g(x) = \sum_{x \geq y} \mu(y, x)f(y)$.

For the subspace lattice of E and for two subspaces U and V of dimensions u and v , we have that

$$\mu(U, V) = \begin{cases} (-1)^{v-u} q^{\binom{v-u}{2}} & \text{if } U \leq V \\ 0 & \text{otherwise.} \end{cases}$$

Definition 18. Given a pair of nonnegative integers N and M , the q -**binomial** or **Gaussian coefficient** counts the number of M -dimensional subspaces of an N -dimensional subspace over \mathbb{F}_q and is given by:

$$\begin{bmatrix} N \\ M \end{bmatrix}_q := \prod_{i=0}^{M-1} \frac{q^N - q^i}{q^M - q^i}.$$

We state the following identity, which can be shown using Möbius inversion.

Lemma 19. Let I, J be subspaces of E of dimensions i and j , respectively, satisfying $I \cap J = \{0\}$ and $i + j \leq k$. Then, the number of k -dimensional subspaces of E that contain I and meet trivially with J is

$$\sum_{s=0}^j (-1)^s q^{\binom{s}{2}} \begin{bmatrix} j \\ s \end{bmatrix}_q \begin{bmatrix} n - i - s \\ k - i - s \end{bmatrix}_q = q^{j(k-i)} \begin{bmatrix} n - i - j \\ k - i \end{bmatrix}_q$$

where n is the dimension of E .

3.2. The Characteristic Polynomial. The following definition is mainly for convenience. It originates in weight enumeration in linear codes.

Definition 20. Let $M = (E, \rho)$ be a (q, r) -polymatroid. For each $A \leq E$ we define

$$\ell_M(A) := \rho_M(E) - \rho_M(A).$$

By the definition of the rank function of a q -polymatroid, for each subspace A of E we see that $\ell_M(A)$ is non-negative integer in $\{0, \dots, \rho_M(E)\}$. For the remainder, we let M denote a fixed (q, r) -polymatroid $M = (E, \rho)$ and we write $\ell := \ell_M$ and $\rho := \rho_M$. For the dual q -polymatroid, we write $\ell^* := \ell_{M^*}$ and $\rho^* := \rho_{M^*}$.

Definition 21. The **characteristic polynomial** of M is the polynomial in $\mathbb{Z}[z]$ defined by

$$p(M; z) := \sum_{X: X \leq E} \mu(0, X) z^{\ell(X)}.$$

Clearly $p(M; 1) = 0$ and so unless $p(M; z)$ is identically zero, $z - 1$ is a factor in $\mathbb{Z}[z]$. For the (q, r) -polymatroid M , we have

$$p(M; z) := \sum_{j=0}^n (-1)^j q^{\binom{j}{2}} \sum_{X \leq E, \dim(X)=j} z^{\ell(X)}.$$

Example 22. We calculate the characteristic polynomial of the Vámos q -matroid of Example 16. From the rank function it follows that:

$$\ell(X) := \begin{cases} 4 - \dim(X) & \text{if } \dim(X) \leq 3, \\ 1 & \text{if } X \in \mathcal{C}, \\ 0 & \text{if } \dim(X) \geq 4 \text{ and } X \notin \mathcal{C}. \end{cases}$$

We split our calculations in the coefficients of the powers of z . For the coefficient of z^4 we only have $X \leq E$ with $\dim X = 0$, i.e. the zero space. Then $\mu(0, X) = \mu(0, 0) = 1$ and we get the term z^4 . For z^3 and z^2 we get

$$\sum_{\dim X=1} \mu(0, X) z^{\ell(X)} = - \begin{bmatrix} 8 \\ 1 \end{bmatrix}_q z^3, \quad \sum_{\dim X=2} \mu(0, X) z^{\ell(X)} = q \begin{bmatrix} 8 \\ 2 \end{bmatrix}_q z^2.$$

For the coefficient of z we have to consider the five circuits of dimension 4 and all spaces of dimension 3. This gives

$$\left(5q^6 - q^3 \begin{bmatrix} 8 \\ 3 \end{bmatrix}_q \right) z.$$

Finally, the constant term is determined by all spaces of dimension 4 that are not circuits, plus all spaces of higher dimension:

$$q^6 \binom{[8]}{[4]}_q - 5 - q^{10} \binom{[8]}{[5]}_q + q^{15} \binom{[8]}{[6]}_q - q^{21} \binom{[8]}{[7]}_q + q^{28} = q^6 \left(\binom{[8]}{[4]}_q - 5 - q^4 \binom{[8]}{[3]}_q + q^9 \binom{[8]}{[2]}_q - q^{15} \binom{[8]}{[1]}_q + q^{22} \right)$$

Adding all terms gives the characteristic polynomial of the Vámos q -matroid. For example, for $q = 2$, we have $p(M; z) = z^4 - 255z^3 + 21590z^2 - 776920z + 755584 = (z - 1)(z^3 - 254z^2 + 21336z - 755584)$.

It is easily checked that the characteristic polynomial is an invariant of the lattice-equivalence class of a matroid.

Lemma 23. *Let E_1, E_2 be \mathbb{F}_q -linear spaces. Let $M_1 = (E_1, \rho_1)$ and $M_2 = (E_2, \rho_2)$ be a pair of lattice-equivalent q -polymatroids. Then $p(M_1; z) = p(M_2; z)$.*

Proof. Let $\phi : \mathcal{L}(E_1) \rightarrow \mathcal{L}(E_2)$ be a lattice isomorphism such that $\rho_2(\phi(X)) = \rho_1(X)$ for all $X \in \mathcal{L}(E_1)$. Since $\mathcal{L}(E_1)$ and $\mathcal{L}(E_2)$ are equivalent lattices, we have that $\dim(X) = \dim(\phi(X))$ for all $X \in \mathcal{L}(E_1)$ and in particular $\mu_1(0, X) = \mu_2(0, \phi(X))$, where μ_i denotes the Möbius function on $\mathcal{L}(E_i)$. Moreover, $X \leq Y$ in $\mathcal{L}(E_2)$ if and only if $\phi(X) \leq \phi(Y)$ in $\mathcal{L}(E_1)$. By assumption, $\ell_{M_1}(X) = \ell_{M_2}(\phi(X))$ for each $X \in \mathcal{L}(E_1)$ and so the result now follows. \square

We have the following results on the characteristic polynomial of the contraction of M to a subspace T . These will be important later when we define the q -polymatroid version of the rank weight enumerator.

Lemma 24. *Let $T \leq E$. The following hold.*

- (1) $\ell_{M.T}(X/T^\perp) = \ell_{M/T^\perp}(X/T^\perp) = \ell(X)$.
- (2) $p(M.T; z) = \sum_{T^\perp \leq X \leq E} \mu(T^\perp, X) z^{\ell(X)}$.

Proof. The first part follows from a direct computation.

$$\begin{aligned} \ell_{M.T}(X/T^\perp) &= \ell_{M/T^\perp}(X/T^\perp) = \rho_{M/T^\perp}(E/T^\perp) - \rho_{M/T^\perp}(X/T^\perp) \\ &= \rho(E) - \rho(T^\perp) - \rho(X) + \rho(T^\perp) \\ &= \rho(E) - \rho(X) = \ell(X). \end{aligned}$$

Let $\bar{\mu}$ denote the Möbius function on the lattice of subspaces of E/T . Then, applying (1) we have:

$$p(M.T; z) = p(M/T^\perp; z) = \sum_{T^\perp \leq X \leq E} \bar{\mu}(0, X/T^\perp) z^{\ell_{M/T^\perp}(X/T^\perp)} = \sum_{T^\perp \leq X \leq E} \mu(T^\perp, X) z^{\ell(X)},$$

which proves (2). \square

Clearly, if T has dimension t , $p(M.T; z) = \sum_{j=0}^t (-1)^j q^{\binom{j}{2}} \sum_{T^\perp \leq Y, \dim(Y)=n-t+j} z^{\ell(Y)}$.

Example 25. Let T be a subspace of E . We calculate $p(M.T; z)$ where M is the Vámos q -matroid (Example 16). If T has dimension 5, then $\dim T^\perp = 3$. We need only consider two cases, depending on whether or not T^\perp is contained in a circuit (a member of \mathcal{C}). Note that the circuits intersect pairwise in dimension 2 or 0, so T^\perp cannot be in more than one circuit. Suppose T^\perp is in none of the circuits. Then for all X such that $T^\perp < X \leq E$ we have that $\ell(X) = 0$. For $X = T^\perp$, we have $\ell(X) = 1$. So the q -matroid $M.T$ is lattice-equivalent to the uniform q -matroid $U_{1,5}$. Its characteristic polynomial is

$$p(M.T; z) = \mu(T^\perp, T^\perp) z^1 + \sum_{T^\perp < X \leq E} \mu(T^\perp, X) z^0 = z - 1.$$

Suppose now that T^\perp is contained in a circuit $C \in \mathcal{C}$. Among all X such that $T^\perp \leq X \leq E$ we have that $\ell(X) = 1$ for $X = T^\perp$ and $X = C$. Otherwise, $\ell(X) = 0$. The q -matroid $M.T$ has rank 1 and all 1-dimensional spaces are independent, except for the circuit C/T^\perp . For the characteristic polynomial we get the following:

$$\begin{aligned} p(M.T; z) &= \mu(T^\perp, T^\perp)z + \mu(T^\perp, C)z + \sum_{X: T^\perp < X \leq E, X \neq C} \mu(T^\perp, X) \\ &= z - z - \left(\begin{bmatrix} 8-3 \\ 4-3 \end{bmatrix}_q - 1 \right) + q \begin{bmatrix} 8-3 \\ 5-3 \end{bmatrix}_q - q^3 \begin{bmatrix} 8-3 \\ 6-3 \end{bmatrix}_q + q^6 \begin{bmatrix} 8-3 \\ 7-3 \end{bmatrix}_q - q^{10}, \\ &= - \left(\begin{bmatrix} 5 \\ 1 \end{bmatrix}_q - 1 \right) + q \begin{bmatrix} 5 \\ 2 \end{bmatrix}_q - q^3 \begin{bmatrix} 5 \\ 3 \end{bmatrix}_q + q^6 \begin{bmatrix} 5 \\ 4 \end{bmatrix}_q - q^{10} = 0. \end{aligned}$$

In fact, since $\sum_{X: T^\perp < X \leq E, X \neq C} \mu(T^\perp, X) + 1 + \mu(T^\perp, C) = 0$, we see that the constant term is zero without the need for any calculation.

We continue to develop technical properties of the characteristic polynomial of the contraction $M.T$. In Section 6, we will use the fact that the characteristic polynomial of $M.T$ is identically zero when T is an independent space of the dual q -polymatroid.

Lemma 26. *If $T \leq E$ is an independent space of M^* then $\ell(T^\perp) = 0$.*

Proof. Let $V = T^\perp$. We will show that if V^\perp is an independent space of M then $\ell^*(V) = 0$. Then the statement of the lemma will follow by replacing M with M^* and V with T^\perp . By definition, $\ell^*(T) = \rho^*(E) - \rho^*(T)$. It also holds that $\rho^*(Y) = \dim(Y) - \rho(E) + \rho(Y^\perp)$ for any subspace $Y \leq E$. Therefore,

$$\begin{aligned} \ell^*(V) &= r \dim(E) - \rho(E) - (r \dim(V) - \rho(E) + \rho(V^\perp)) \\ &= r \dim(E) - r \dim(V) - \rho(V^\perp) \\ &= r \dim(V^\perp) - \rho(V^\perp), \end{aligned}$$

which evaluates to zero if V^\perp is an independent space of M . \square

Lemma 27. *If $T \leq E$ is an independent space of M^* then $p(M.T; z) = 0$.*

Proof. By Lemma 26, $\ell(T^\perp) = 0$. Since all subspaces of an independent space are independent, we have that $\ell(X) = 0$ for all $T^\perp \leq X$. Applying this to the characteristic polynomial, we get

$$p(M.T; z) = \sum_{T^\perp \leq X \leq E} \mu(T^\perp, X) z^{\ell(X)} = \sum_{T^\perp \leq X \leq E} \mu(T^\perp, X) = 0.$$

\square

Lemma 28. *Let $T \leq E$ be a circuit of $M^* = (E, \rho^*)$. Then $p(M.T; z) = z^{\ell(T^\perp)} - 1$.*

Proof. Let $X \leq E$. If T^\perp is strictly contained in X , then X^\perp is strictly contained in T , and so X^\perp is independent in M^* by Lemma 9. Therefore, $\rho^*(X^\perp) = r \dim(X^\perp)$ and so

$$\ell(X) = \rho(E) - \rho(X) = \rho(E) - (\rho^*(X^\perp) - r \dim(X^\perp) + \rho(E)) = r \dim(X^\perp) - \rho^*(X^\perp) = 0.$$

Therefore,

$$\begin{aligned} p(M.T; z) &= \sum_{T^\perp \leq X \leq E} \mu(T^\perp, X) z^{\ell(X)} = z^{\ell(T^\perp)} + \sum_{T^\perp < X \leq E} \mu(T^\perp, X) \\ &= z^{\ell(T^\perp)} - \mu(T^\perp, T^\perp) = z^{\ell(T^\perp)} - 1. \end{aligned}$$

\square

Remark 29. Note that if M is a q -matroid, a cocircuit T of M has $\ell(T^\perp) = \dim(T) - \rho^*(T) = \dim(T) - (\dim(T) - 1) = 1$ hence $p(M.T; z) = z - 1$.

Lemma 30. *Let $T \leq E$ be an independent space of M^* . The following hold.*

- (1) $\rho(E) = \rho(T^\perp)$.
- (2) For any subspace $U \leq T^\perp$, we have $\ell_{M|_{T^\perp}}(U) = \ell(U)$.

Proof. By definition of the dual q -polymatroid, we have $\rho(T^\perp) = \rho^*(T) - \dim(T) + \rho(E)$. Since T is independent in M^* , $\rho^*(T) = \dim(T)$ and so we get $\rho(T^\perp) = \rho(E)$, which establishes (1). Therefore, $\ell_{M|_{T^\perp}}(U) = \rho_{M|_{T^\perp}}(T^\perp) - \rho_{M|_{T^\perp}}(U) = \rho(T^\perp) - \rho(U) = \rho(E) - \rho(U) = \ell(U)$, which proves (2). \square

Corollary 31. *Let $T \leq U$ be subspaces of E such that T is independent in M^* . If U/T is a circuit in M^*/T then*

$$p((M^*/T))^*(U/T; z) = p(M|_{T^\perp} \cdot (U^\perp)^{\perp(T^\perp)}; z) = z^{\ell(U^\perp)} - 1.$$

Proof. Recall that $(M^*/T)^* \cong M|_{T^\perp}$ under the map $\phi : A/T \mapsto (A^\perp)^{\perp(T^\perp)}$ for any $A \leq E$ with $T \leq A$. In particular, if U/T is a circuit in M^*/T then $\phi(U/T)$ is a circuit in $(M|_{T^\perp})^*$. Moreover $\phi(U/T)^{\perp(T^\perp)} = U^\perp$. From Lemmas 30 and 28 we have

$$p((M^*/T))^*(U/T; z) = p(M|_{T^\perp} \cdot \phi(U/T); z) = z^{\ell_{M|_{T^\perp}}(U^\perp)} - 1 = z^{\ell(U^\perp)} - 1. \quad \square$$

The following result will be used in the proof of Corollary 69.

Lemma 32. *Let $W \leq E$ and let $T \leq W$ be an independent space of M^* . Then*

$$p(M|_{T^\perp}/W^\perp; z) = \sum_{A:A+T=W} p(M.A; z).$$

Proof. By Lemmas 24 and 30, we have $\ell_{M|_{T^\perp}/W^\perp}(U/W^\perp) = \ell(U)$ for any subspace U satisfying $T \leq U \leq W$. Since $p(M/U; z) = \sum_{A:U \leq A \leq E} \mu(U, A) z^{\ell(A)}$, by applying the Möbius inversion formula we have $z^{\ell(U)} = \sum_{A:U \leq A \leq E} p(M/A; z)$. Therefore, we have

$$\begin{aligned} p(M|_{T^\perp}/W^\perp; z) &= \sum_{U:W^\perp \leq U \leq T^\perp} \mu(W^\perp, U) z^{\ell(U)} \\ &= \sum_{U:W^\perp \leq U \leq T^\perp} \mu(W^\perp, U) \sum_{A:U \leq A \leq E} p(M/A; z) \\ &= \sum_{U:W^\perp \leq U \leq T^\perp} \mu(W^\perp, U) \sum_{A:U \leq A \leq E} p(M.A^\perp; z) \\ &= \sum_{U^\perp:W^\perp \leq U^\perp \leq T^\perp} \mu(W^\perp, U^\perp) \sum_{A:U^\perp \leq A \leq E} p(M.A^\perp; z) \\ &= \sum_{U:T \leq U \leq W} \mu(W^\perp, U^\perp) \sum_{A:0 \leq A \leq U} p(M.A; z) \\ &= \sum_{A:0 \leq A \leq W} p(M.A; z) \sum_{U:A+T \leq U \leq W} \mu(W^\perp, U^\perp) \\ &= \sum_{A:A+T=W} p(M.A; z), \end{aligned}$$

where the last equality follows from the fact that

$$\sum_{U:A+T \leq U \leq W} \mu(W^\perp, U^\perp) = \sum_{U:W^\perp \leq U^\perp \leq A^\perp \cap T^\perp} \mu(W^\perp, U^\perp) = \begin{cases} 1 & \text{if } A^\perp \cap T^\perp = W^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

\square

Remark 33. Let $W, T, X \leq E$ such that $\phi(W/T) = X$. Then $(W^\perp)^\perp(T^\perp) = X$ and so $X^\perp(T^\perp) = W^\perp$. Therefore, $M|_{T^\perp}.X = M|_{T^\perp}/W^\perp$.

We now present some further results on the characteristic polynomial.

Definition 34. A **loop** of the (q, r) -polymatroid M is a circuit of dimension 1.

Clearly, if e is a loop of M , then $0 \leq \rho(e) < r$. If M is a q -matroid then the loops of M all have rank zero.

Lemma 35. Let e be a one-dimensional subspace of E . The following are equivalent:

- (1) $p(M.e; z) = 0$,
- (2) $\rho(e^\perp) = \rho(E)$,
- (3) e is not a loop in M^* .

Proof. We have $p(M.e; z) = z^{\ell(e^\perp)} - z^{\ell(E)} = z^{\ell(e^\perp)} - 1$, which is zero if and only if $\ell(e^\perp) = \rho(E) - \rho(e^\perp) = 0$. This shows that (i) and (ii) are equivalent. The one-dimensional space e is independent in M^* if and only if $\rho^*(e) = r$. Since $\rho^*(e) = r \dim(e) - \rho(E) + \rho(e^\perp) = r - \rho(E) + \rho(e^\perp)$, this occurs if and only if $\rho(e^\perp) = \rho(E)$, which shows that (ii) and (iii) are equivalent. \square

Remark 36. We remark that for a classical matroid M , if e is a loop of M then it is easy to see that $p(M.e; z) = 0$. This is because if e is a loop, by semimodularity, the fact that $e \notin E - e$ forces $\rho(E - e) = \rho(E)$. Then by the classical version of the lemma above, this gives that $p(M.e; z) = 0$. For a q -matroid, however, it may occur that $e \leq e^\perp$, in which case if e is a loop, the same argument using semimodularity does not imply that $\rho(e^\perp) = \rho(E)$.

Definition 37. For each $A \in \mathcal{L}(E)$, define $c(A) := \{X \leq E : A \leq X, \rho(A) = \rho(X)\}$. The **closure** of A in the (q, r) -polymatroid M is denote by $\text{cl}(A)$ and is defined to be the vector space sum of the members of $c(A)$ that is, $\text{cl}(A) := \sum_{X \in c(A)} X$.

Lemma 38. Let $L = \text{cl}(\{0\})$. Let X be a subspace of E such that $X^\perp \leq L$. Then

$$p(M.X; z) = \begin{cases} z^{\rho(E)} + \sum_{A: X^\perp \subsetneq A \leq E} \mu(X^\perp, A) z^{\ell(A)} & \text{if } X = L^\perp, \\ \sum_{A: X^\perp \leq A \leq E, A \not\subseteq L} \mu(X^\perp, A) z^{\ell(A)} & \text{otherwise.} \end{cases}$$

If $X^\perp = L$ then $p(M.X; z)$ is a monic polynomial of degree $\rho(E)$ in z . In particular, if M is a q -matroid and has no loops then $p(M; z)$ is monic polynomial of degree $\rho(E)$.

Proof. From Lemma 24 we have, $p(M.X; z) =$

$$\sum_{A: X^\perp \leq A \leq E} \mu(X^\perp, A) z^{\ell(A)} = z^{\rho(E)} \sum_{A: X^\perp \leq A \leq L} \mu(X^\perp, A) + \sum_{A: X^\perp \leq A \leq E, A \not\subseteq L} \mu(X^\perp, A) z^{\ell(A)}$$

By the definition of the Möbius function, $\sum_{A: X^\perp \leq A \leq L} \mu(X^\perp, A) = 0$ unless $X^\perp = L$. If $A \not\subseteq L$ then $\ell(A) = \rho(E) - \rho(A) < \rho(E)$, so if $L = X^\perp$ then $p(M.X; z)$ is a monic polynomial with leading term $z^{\rho(E)}$. Setting $X = E$, we obtain that if furthermore M is a q -matroid with no loops, its characteristic polynomial is monic of degree $\rho(E)$. \square

Remark 39. If M is a q -matroid, $\text{cl}(\{0\})$ is the space containing all the loops. By contrast if M is a q -polymatroid, this is not necessarily the case, since loops need not have rank 0.

In the q -matroid case, cryptomorphisms between matroidal axiom systems such as those relating to independent spaces, the closure function, flats, hyperplanes etc were established in [5]. A subspace F is called a **flat** of a q -matroid if $\text{cl}(F) = F$. Moreover, if M is a q -matroid, its collection of flats forms a semi-modular lattice [4, Theorem 2]. The following result will be used in Corollary 74.

Theorem 40. *Let M be a q -matroid. Let $X \leq E$ such that X contains a unique cocircuit C . Then*

$$p(M.X; z) = \begin{cases} z - 1 & \text{if } X = C, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Denote the independent and dependent spaces of M^* by \mathcal{I}^* and \mathcal{D}^* , respectively. Clearly X is a dependent space of M^* and by the uniqueness of C , any subspace of X in \mathcal{D}^* contains C . Therefore, $\ell(A^\perp) = 0$ for every $A \leq X$ such that $C \not\leq A$.

Let $U \leq X$ such that $X = C + U$, $U \cap C = \{0\}$. If U is the zero space then $X = C$ and it follows that $p(M.X; z) = z - 1$ by Lemma 28. Assume that $U \neq \{0\}$. For any proper subspace I of C we have $U + I \in \mathcal{I}^*$, so that $\ell(A^\perp) = 0$ where $A = U + I$. Moreover, $U \in \mathcal{I}^*$ is non-trivial, so that X is not a sum of cocircuits of M and in particular is not an open set. By [5, Corollary 78], X^\perp is not a flat in M .

Since C is a cocircuit, by [5, Corollary 71] C^\perp is a hyperplane in M and in particular, $\text{cl}(C^\perp) = C^\perp$. Let \mathcal{F} denote the set of flats of the q -matroid M . Then $F = \text{cl}(F)$ for each $F \in \mathcal{F}$ and for each $B \leq E$, there is a unique flat F such that $\text{cl}(B) = F$, in which case $\rho(B) = \rho(F)$.

$$\begin{aligned} p(M.X; z) &= \sum_{A: X^\perp \leq A \leq E} \mu(X^\perp, A) z^{\ell(A)} = \sum_{A: A \leq X} \mu(A, X) z^{\ell(A^\perp)}, \\ &= \sum_{A: C \leq A \leq X} \mu(A, X) z^{\ell(A^\perp)} + \sum_{A: A \leq X, C \not\leq A} \mu(A, X), \\ &= \sum_{\substack{F \in \mathcal{F} \\ X^\perp \leq F \leq C^\perp}} \sum_{\substack{A: X^\perp \leq A^\perp \leq C^\perp \\ \text{cl}(A^\perp) = F}} \mu(X^\perp, A^\perp) z^{\ell(F)} + \sum_{I: I < C} \sum_{Y: Y \leq U} \mu(I + Y, C + U), \\ &= \sum_{\substack{F \in \mathcal{F} \\ X^\perp \leq F \leq C^\perp}} z^{\ell(F)} \sum_{\substack{A: X^\perp \leq A^\perp \leq C^\perp \\ \text{cl}(A^\perp) = F}} \mu(X^\perp, A^\perp) + \sum_{I: I < C} \mu(I, C) \sum_{Y: Y \leq U} \mu(Y, U), \\ &= \sum_{\substack{F \in \mathcal{F} \\ X^\perp \leq F \leq C^\perp}} z^{\ell(F)} \sum_{\substack{A: X^\perp \leq A^\perp \leq C^\perp \\ \text{cl}(A^\perp) = F}} \mu(X^\perp, A^\perp) - \sum_{Y: Y \leq U} \mu(Y, U). \end{aligned}$$

Since $U \neq \{0\}$ by assumption, we have $\sum_{Y: Y \leq U} \mu(Y, U) = 0$. Equivalently, X^\perp is not a flat in M . By [4, Theorem 2] \mathcal{F} forms a semimodular lattice and so by [21, Proposition 3.3], we have

$$\sum_{A: X^\perp \leq A^\perp \leq C^\perp, \text{cl}(A^\perp) = F} \mu(X^\perp, A^\perp) = 0.$$

□

Remark 41. In fact, by a similar argument (also essentially the same as for classical matroids), it holds that for a q -matroid M , $p(M.X; z) = 0$ unless X^\perp is a flat in M . Equivalently, we have that $p(M.X; z) = 0$ unless X is a sum of co-circuits of M .

3.3. The Weight Enumerator of a q -Polymatroid. We define next the *weight enumerator* of a q -polymatroid. In Section 5, we will show that these coefficients satisfy a duality property and in Section 6, we will apply this duality result to establish a criterion for identifying a weighted subspace design determined by a q -polymatroid.

Definition 42. We define the **weight enumerator** of the (q, r) -polymatroid M to be the list $[A_M(i; z) : 0 \leq i \leq n]$, where for each i we define

$$A_M(i; z) := \sum_{X \leq E, \dim(X) = i} p(M.X; z) = \sum_{X \leq E, \dim(X) = i} p(M/X^\perp; z).$$

Lemma 43. *Let $T \leq E$. The following hold.*

(1) *If $Z \leq E$ and $T \leq Z$ then $p((M/T)/(Z/T); z) = p(M.Z^\perp; z)$.*

(2) $A_{M/T}(j; z) = \sum_{X \leq T^\perp: \dim(X)=j} p(M.X; z)$.

Proof. Let $T \leq Z \leq Y \leq E$. Then $(Y/T)/(Z/T)$ and Y/Z are isomorphic. Let $V = (E/T)/(Z/T)$ and write $M_V = (M/T)/(Z/T)$. We have a lattice isomorphism between $\mathcal{L}(E/Z)$ and $\mathcal{L}(V)$. Moreover, it is easy to check that $\rho_{M_V}((Y/T)/(Z/T)) = \rho_{M/Z}(Y/Z)$. Therefore, M_V and M/Z are lattice-equivalent and $Z^\perp \leq T^\perp$. We thus have

$$p(M_V; z) = p(M/Z; z) = p(M.Z^\perp; z).$$

Let $X \leq T^\perp$. It is straightforward to check that $\dim((X^\perp/T)^\perp(E/T)) = \dim(X)$. Therefore,

$$A_{M/T}(j; z) = \sum_{X^\perp/T \leq E/T: \dim((X^\perp/T)^\perp(E/T))=j} p(M/T/(X^\perp/T); z) = \sum_{X \leq T^\perp: \dim(X)=j} p(M.X; z)$$

□

4. MATRIX CODES AND q -POLYMATROIDS

We consider properties of a q -polymatroid arising from an \mathbb{F}_q -linear rank-metric code. There are several papers outlining properties of rank-metric codes. The q -polymatroids associated with these structures have been studied in [10, 9, 17].

Notation 44. Throughout this section, we let m be a positive integer. As stated in Definition 5, we write U^\perp to denote the orthogonal complement of $U \leq E$ with respect to b_E . By abuse of notation, we also write U^\perp to denote the orthogonal complement of

- $U \leq \mathbb{F}_q^{n \times m}$ with respect to the inner product $b_{\mathbb{F}_q^{n \times m}}$ defined by $b_{\mathbb{F}_q^{n \times m}}(X, Y) = \text{Tr}(XY^T)$ for all $X, Y \in \mathbb{F}_q^{n \times m}$ and
- $U \leq \mathbb{F}_q^n$ with respect to the dot product defined by $x \cdot y = \sum_{i=1}^n x_i y_i$ for all $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$.

Definition 45. We say that $C \subseteq \mathbb{F}_q^{n \times m}$ is a **linear rank metric code**, or a **matrix code** if C is a subspace of $\mathbb{F}_q^{n \times m}$. The **minimum distance** of C is the minimum rank of any member of C . We say that C is an \mathbb{F}_q - $[n \times m, k, d]$ rank metric code if it has \mathbb{F}_q -dimension k and minimum distance d . The **dual code** of C is $C^\perp := \{Y \in \mathbb{F}_q^{n \times m} : \text{Tr}(XY^T) = 0 \forall X \in C\}$.

Definition 46. Let $X \in \mathbb{F}_q^{n \times m}$ and let $U \leq E$. We say that U is the **support** of X if $\text{colsp}(X) = U$. Let C be an \mathbb{F}_q - $[n \times m, k, d]$ rank metric code. We say that U is a **support** of C if there exists some $X \in C$ with support U .

Definition 47. Let m be a positive integer and let C be an \mathbb{F}_q - $[n \times m, k, d]$ rank-metric code. For each subspace $U \leq E$, we define

$$C_U := \{A \in C : \text{colsp}(A) \leq U^\perp\} \text{ and } C_{=U} := \{A \in C : \text{colsp}(A) = U^\perp\}.$$

Let $\rho : \mathcal{L}(E) \rightarrow \mathbb{N}_{\geq 0}$ be defined by $\rho(U) := k - \dim(C_U)$. We denote by M_C the (q, m) -polymatroid (E, ρ) .

Clearly, we have $\ell(U) = \dim(C_U)$ for every $U \leq E$.

Lemma 48. *Let C be an \mathbb{F}_q - $[n \times m, k, d]$ rank-metric code. The following hold.*

- (1) $M_{C^\perp} = (M_C)^*$,
- (2) $p(M/U; q) = |C_{=U}|$.
- (3) $W_i(C) = A_{M_C}(i, q)$ for each $i \in \{1, \dots, n\}$,
- (4) $A_{M_C}(i, q) = 0$ if and only if $p(M/U; q) = 0$ for every i -dimensional subspace $U \leq E$,
- (5) If $A_{M_C}(i, q) = 0$ then $A_{M_C/T}(i, q) = 0$ for every t -dimensional subspace $T \leq E$.

Proof. (1) has been established in [10, Theorem 7.1]. Since $|C_U| = \sum_{U \subset V} |C_{=V}|$, by Möbius inversion we have

$$|C_{=U}| = \sum_{U \leq V} \mu(U, V) |C_V| = \sum_{U \leq V} \mu(U, V) q^{\ell(V)} = p(M.U^\perp; q) = p(M/U; q).$$

Therefore (2) holds. The number of codewords of C that have rank i over \mathbb{F}_q is

$$W_i(C) = \sum_{U: \dim(U)=n-i} |C_{=U}| = \sum_{U: \dim(U)=n-i} p(M.U^\perp; q) = \sum_{U: \dim(U)=i} p(M.U; q) = A_{M_C}(i; q),$$

which gives (3). Clearly, $A_{M_C}(i; q) = 0$ if and only if $p(M.U; q) = 0$ for each $U \leq E$ of dimension i , which gives (4). Let T be a t -dimensional subspace of E . By Lemma 43 we have

$$A_{M_C/T}(i, q) = \sum_{X \leq T^\perp: \dim(X)=i} p(M.X; q).$$

If $A_{M_C}(i; q) = 0$, then from (4) we have $p(M.X; q) = 0$ for each i -dimensional subspace X , and so we get $A_{M_C/T}(i, q) = 0$, which proves (5). \square

Remark 49. Note that Part (2) of Lemma 48 is an instance of the critical theorem for q -polymatroids and matrix codes.

Remark 50. In [10], the authors define a pair of q -polymatroids associated with matrix code. The one given above is the q -polymatroid whose rank function is determined by the column-spaces of the codewords. A second q -polymatroid is one whose rank function is determined by the row-spaces of the codewords.

One way to construct an \mathbb{F}_q - $[n \times m, k, d]$ rank metric code is by taking a subspace of $\mathbb{F}_{q^m}^n$, and expanding its elements with respect to a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . This class of rank metric codes are referred to as vector rank-metric codes.

Definition 51. Let Γ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . For each $x \in \mathbb{F}_{q^m}^n$, we write $\Gamma(x)$ to denote the $n \times m$ matrix over \mathbb{F}_q whose i th row is the coordinate vector of the i th coefficient of x with respect to the basis Γ . The **rank** of x is the rank of the matrix $\Gamma(x)$. Note that the rank of x is well-defined, being independent of the choice of basis Γ .

For the remainder, we fix Γ to be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q .

Definition 52. A (linear rank-metric) **vector code** C is an \mathbb{F}_{q^m} -subspace of $\mathbb{F}_{q^m}^n$. The **minimum distance** of C is the minimum rank of any non-zero element of C . We say that C is an \mathbb{F}_{q^m} - $[n, k, d]$ code if it has \mathbb{F}_q -dimension k and $\Gamma(C)$ has minimum rank distance d . The code C^\perp denotes the **dual code** of C with respect to the standard dot product on $\mathbb{F}_{q^m}^n$.

Each vector rank metric code determines a q -matroid, as follows.

Definition 53. Let $m \geq n$ and let C be an \mathbb{F}_{q^m} - $[n, k, d]$ rank-metric code. Let $U \leq E$ and let $x \in C$. We say that U is a **support** of x if U is the column space of $\Gamma(x)$ and we write $\sigma(x) = U$. For each subspace $U \leq E$, we define

$$C_U := \{x \in C : \sigma(x) \leq U^\perp\} \text{ and } C_{=U} := \{x \in C : \sigma(x) = U^\perp\}.$$

Let $\rho : \mathcal{L}(E) \rightarrow \mathbb{N}_{\geq 0}$ be defined by $\rho(U) := k - \dim_{\mathbb{F}_{q^m}}(C_U)$. We denote by M_C the q -matroid (E, ρ) .

Remark 54. Note that in the definition given above, the rank function for the q -matroid of C is the rank function of the associated (q, m) -polymatroid as defined in Definition 47, divided by m . Since C is \mathbb{F}_{q^m} -linear, C_U is an \mathbb{F}_{q^m} -vector space for each subspace U and so has \mathbb{F}_q -dimension a multiple of m . Therefore the results of Lemma 48 hold with q^m in place of q . For example, with respect to the characteristic polynomial of the q -matroid, we have $p(M/U; q^m) = |C_{=U}|$ for an \mathbb{F}_{q^m} - $[n, k, d]$ code C and subspace U .

Example 55. Let α be a primitive element of \mathbb{F}_{2^6} and let C be the \mathbb{F}_{2^6} - $[6, 3, 3]$ vector rank metric code generated by the matrix:

$$G = \begin{bmatrix} 1 & 0 & 0 & \alpha^{13} & \alpha^{47} & \alpha^{35} \\ 0 & 1 & 0 & \alpha^{44} & \alpha^{62} & \alpha^{32} \\ 0 & 0 & 1 & \alpha^{34} & \alpha^{22} & \alpha^{19} \end{bmatrix}.$$

With respect to the basis $\Gamma = \{1, \dots, \alpha^5\}$, the rows of G are expanded to the following binary matrices:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

A basis of $\Gamma(C)$ over \mathbb{F}_2 , which has 18 elements, is found by multiplying each row of G by successive powers of α and expanding with respect to Γ . $\Gamma(C)$ is an \mathbb{F}_2 - $[6 \times 6, 18, 3]$ rank metric code with rank-metric weight distribution $[1, 0, 0, 567, 37044, 142884, 81648]$. Moreover, C is formally self-dual, that is, its dual code has the same weight distribution. Now consider the q -matroid arising from C , with rank function satisfying $\rho(U) = 3 - \dim_{\mathbb{F}_{2^6}}(C_U)$ for each $U \leq \mathbb{F}_2^6$. There are 9 different 3-dimensional spaces that are supports of C and for each such subspace U we have $p(M.U; 2^6) = |C_{=U^\perp}| = 2^6$. Also $|C_{U^\perp}| = |C_{=U^\perp}| + 1$, so that $\rho(U^\perp) = 3 - 1 = 2$, and $\ell(U^\perp) = 1$. These subspaces U are the cocircuits of the q -matroid M_C of minimum dimension, which we list below.

$$\begin{aligned} &\langle (010011), (001010), (000100) \rangle, \langle (101100), (010000), (000001) \rangle, \langle (100001), (011000), (000010) \rangle, \\ &\langle (100111), (010010), (001101) \rangle, \langle (100110), (010101), (001001) \rangle, \langle (100010), (001011), (000111) \rangle, \\ &\langle (110001), (000101), (000011) \rangle, \langle (100100), (010100), (001111) \rangle, \langle (100000), (010110), (001000) \rangle. \end{aligned}$$

There are 588 4-dimensional supports of C . Similarly, for each such subspace U we have $p(M.U; 2^6) = |C_{=U^\perp}| = 2^6$, $\rho(U^\perp) = 2$, and $\ell(U^\perp) = 1$. It can be checked that none of these spaces contains a cocircuit of dimension 3, so these are also cocircuits of M_C . There are 63 5-dimensional supports of C and of course the only 6-dimensional support is the entire space \mathbb{F}_2^6 . Each 5-dimensional support U is the support of exactly 2268 different codewords, so $p(M.U; 2^6) = |C_{=U^\perp}| = 2268$. We have $|C_{U^\perp}| = 4096$ for each such U , so that $\rho(U^\perp) = 3 - 2 = 1$, and $\ell(U^\perp) = 2$.

$\ell(U) \backslash \dim(U)$	0	1	2	3	4	5	6
0		0	0	$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_2 - 9 = 1386$	$\begin{bmatrix} 6 \\ 4 \end{bmatrix}_2 = 651$	$\begin{bmatrix} 6 \\ 5 \end{bmatrix}_2 = 63$	1
1	0	0	588	9	0	0	0
2	0	$\begin{bmatrix} 6 \\ 1 \end{bmatrix}_2 = 63$	$\begin{bmatrix} 6 \\ 2 \end{bmatrix}_2 - 588 = 63$	0	0	0	0
3	1	0	0	0	0	0	

We now write down the characteristic polynomial of M_C .

$$\begin{aligned} p(M_C; z) &= \sum_{U: 0 \leq U \leq E} \mu(0, U) z^{\ell(U)} \\ &= z^3 + \sum_{U: 0 < U \leq E, \ell(U)=2} \mu(0, U) z^2 + \sum_{U: 0 < U \leq E, \ell(U)=1} \mu(0, U) z + \sum_{U: 0 < U \leq E, \ell(U)=0} \mu(0, U) \\ &= z^3 + 63z^2 + 1104z - 1168 = (z - 1)(z^2 + 64z + 1168). \end{aligned}$$

5. MACWILLIAMS IDENTITIES FOR q -POLYMATROIDS

We establish a version of the MacWilliams identities for the (q, r) -polymatroids that we shall use in establishing criteria for the existence of a weighted t -design over \mathbb{F}_q . Duality via the rank polynomial of a q -polymatroid was considered in [17]. We start with a result that relates the characteristic polynomial of a q -polymatroid with that of its dual.

Lemma 56. *Let $U \leq E$. Then*

$$\sum_{A:A \leq U} p(M^*.A; z) = z^{r \dim(U) - \rho(E)} \sum_{A:A \leq U^\perp} p(M.A; z).$$

Proof. Since $p(M/U; z) = \sum_{A:U \leq A \leq E} \mu(U, A) z^{\ell(A)}$, by Möbius inversion we have

$$z^{\ell(U)} = \sum_{A:U \leq A \leq E} p(M/A; z).$$

Therefore,

$$z^{\ell^*(U)} = \sum_{A:U \leq A \leq E} p(M^*/A; z) = z^{\ell(U^\perp) - \rho(E) + r \dim(U^\perp)},$$

and so

$$\sum_{A:U \leq A \leq E} p(M^*/A; z) = z^{\ell(U^\perp) - \rho(E) + r \dim(U^\perp)} = z^{r \dim(U^\perp) - \rho(E)} \sum_{A:U^\perp \leq A \leq E} p(M/A; z).$$

It follows that $\sum_{A:U \leq A^\perp \leq E} p(M^*.A; z) = z^{r \dim(U^\perp) - \rho(E)} \sum_{A:U^\perp \leq A^\perp \leq E} p(M.A; z)$, and so

$$\sum_{A:A \leq U} p(M^*.A; z) = z^{r \dim(U) - \rho(E)} \sum_{A:A \leq U^\perp} p(M.A; z).$$

□

We now show that for any subspace $U \leq E$, the characteristic polynomial of $M^*.U$ is completely determined by the set $\{p(M.V; z) : V \leq E\}$.

Corollary 57. *Let $U \leq E$. We have the identity:*

$$z^{\rho(E)} p(M^*.U; z) = \sum_{V \leq E} p(M.V; z) \sum_{j=0}^{\dim(V^\perp \cap U)} \left[\begin{matrix} \dim(V^\perp \cap U) \\ j \end{matrix} \right]_q (-1)^{\dim(U) - j} q^{\binom{\dim(U) - j}{2}} z^{jr}.$$

Proof. From Lemma 56, we have:

$$\sum_{A:A \leq U} p(M^*.A; z) = z^{r \dim(U) - \rho(E)} \sum_{A:A \leq U^\perp} p(M.A; z). \quad (1)$$

Apply the Möbius inversion formula to (1) to get the identity

$$p(M^*.U; z) = \sum_{A:A \leq U} \mu(A, U) z^{r \dim(A) - \rho(E)} \sum_{V:V \leq A^\perp} p(M.V; z).$$

Then

$$\begin{aligned} z^{\rho(E)} p(M^*.U; z) &= \sum_{A:A \leq U} \mu(A, U) z^{r \dim(A)} \sum_{V \leq A^\perp} p(M.V; z) \\ &= \sum_{(A,V): A \leq U, A \leq V^\perp} p(M.V; z) \mu(A, U) z^{r \dim(A)} \\ &= \sum_{V \leq E} p(M.V; z) \sum_{A:A \leq U \cap V^\perp} \mu(A, U) z^{r \dim(A)}. \end{aligned}$$

Finally, this yields

$$z^{\rho(E)} p(M^*.U; z) = \sum_{V \leq E} p(M.V; z) \sum_{j=0}^{\dim(V^\perp \cap U)} \left[\begin{matrix} \dim(V^\perp \cap U) \\ j \end{matrix} \right]_q (-1)^{\dim(U)-j} q^{\binom{\dim(U)-j}{2}} z^{jr}. \quad (2)$$

□

We now have the following MacWilliams identity, relating the weight enumerators of M and M^* . This version of the identity, or rather its corollary will be used in the main theorem of Section 6.

Theorem 58. *Let $s \in \{0, \dots, n\}$. Then*

$$\sum_{i=0}^{n-s} \left[\begin{matrix} n-i \\ s \end{matrix} \right]_q A_M(i; z) = z^{\rho(E)-rs} \sum_{i=0}^s \left[\begin{matrix} s \\ i \end{matrix} \right]_q A_{M^*}(i; z).$$

Proof. We start with the left-hand-side of the equation and rewrite it, noting that $\left[\begin{matrix} n-i \\ s \end{matrix} \right]_q = \left[\begin{matrix} n-i \\ n-s-i \end{matrix} \right]_q$ counts the number of $(n-s)$ -dimensional subspaces that contain a fixed space of dimension i . This yields:

$$\begin{aligned} \sum_{i=0}^{n-s} \left[\begin{matrix} n-i \\ s \end{matrix} \right]_q A_M(i; z) &= \sum_{i=0}^{n-s} \left[\begin{matrix} n-i \\ n-s-i \end{matrix} \right]_q \sum_{\dim(X)=i} p(M.X; z) \\ &= \sum_{\{(U,X): X \leq E, X \leq U, \dim(U)=n-s\}} p(M.X; z) \\ &= \sum_{U: \dim(U)=n-s} \sum_{X \leq U} p(M.X; z) \end{aligned}$$

From Lemma 56, this gives:

$$\begin{aligned} \sum_{i=0}^{n-s} \left[\begin{matrix} n-i \\ s \end{matrix} \right]_q A_M(i; z) &= \sum_{U: \dim(U)=n-s} z^{\rho(E)-r \dim(U^\perp)} \sum_{X \leq U^\perp} p(M^*.X; z) \\ &= \sum_{V: \dim(V)=s} z^{\rho(E)-rs} \sum_{X \leq V} p(M^*.X; z) \\ &= z^{\rho(E)-rs} \sum_{\{(V,X): \dim(V)=s, X \leq V\}} p(M^*.X; z) \\ &= z^{\rho(E)-rs} \sum_{i=0}^s \left[\begin{matrix} s \\ i \end{matrix} \right]_q \sum_{X \leq E: \dim(X)=i} p(M^*.X; z) \\ &= z^{\rho(E)-rs} \sum_{i=0}^s \left[\begin{matrix} s \\ i \end{matrix} \right]_q A_{M^*}(i; z) \end{aligned}$$

□

Corollary 59. *Let $S \leq \{1, \dots, n\}$. The pair of lists*

$$[A_{M^*}(i; z) : i \in \{|S| + 1, \dots, n\}] \text{ and } [A_M(j; z) : j \in S],$$

is determined uniquely by the pair of lists

$$[A_{M^*}(i; z) : i \in \{1, \dots, |S|\}] \text{ and } [A_M(j; z) : j \in \{1, \dots, n\} - S].$$

Proof. From Theorem 58, we have the matrix equation

$$\left(\left[\begin{matrix} n-i \\ s \end{matrix} \right]_q \right)_s^i (A_M(i; z))_i = \text{diag}(z^{\rho(E)-rs})_s \left(\left[\begin{matrix} s \\ i \end{matrix} \right]_q \right)_s^i (A_{M^*}(i; z))_i.$$

Let $t = |S|$. It is well-known that every $t \times t$ minor of the matrix $\left(\begin{bmatrix} n-i \\ s \\ i \end{bmatrix}_q \right)_{0 \leq i \leq n, 0 \leq s \leq t}$ is non-zero and every $t \times t$ minor of the matrix $\left(\begin{bmatrix} s \\ i \end{bmatrix}_q \right)_{0 \leq i \leq n, n+1-t \leq s \leq n}$ is non-zero. If the coefficients $\{A_M(j; z) : j \in S\}$ are known, then since the corresponding $t \times t$ submatrix of $\left(\begin{bmatrix} s \\ i \end{bmatrix}_q \right)_{0 \leq i \leq n, n+1-t \leq s \leq n}$ is invertible, the coefficients $\{A_{M^*}(i; z) : i \leq |S|\}$ can be retrieved. Similarly, we can retrieve the coefficients $\{A_M(j; z) : j \in \{1, \dots, n\} - S\}$. \square

6. WEIGHTED SUBSPACE DESIGNS FROM q -POLYMATROIDS

6.1. Weighted Subspace Designs. In [3], the authors give a definition of a *weighted subspace design*, which generalizes a t -design. An t - (n, k, λ) design is a collection of k -subsets of an n -set (called blocks) with the property that every t -subset of the n -set is contained in exactly λ blocks. A q -analogue of this notion is that of a t -design over \mathbb{F}_q , which is a collection of k -dimensional subspaces of E called blocks, with the property that every t -dimensional subspace of E is contained in the same number of blocks. Similarly, there is a q -analogue of a weighted t -design.

Definition 60. Let \mathbb{G} be a group. A weighted t - $(n, k, \lambda; q)$ design \mathcal{D} is a triple (E, \mathcal{B}, f) for which \mathcal{B} is a collection of k -subspaces of E (called blocks), and $f : \mathcal{B} \mapsto \mathbb{G}$ is a weight function such that the equality $\sum_{B:T \leq B} f(B) = \lambda$ holds for some $\theta \in \mathbb{G}$ and for all t -spaces T of V . We say that \mathcal{D} is a **weighted subspace design** or is a **weighted design over \mathbb{F}_q** .

A subspace design (a design over \mathbb{F}_q) can be interpreted as a weighted subspace design with the weight function $f(B) := 1$ for all $B \in \mathcal{B}$. For an excellent survey on subspace designs, see [12]. In general, obtaining new subspace designs is a difficult problem, often highly dependent on computer search, which is exacerbated by the number of subspaces involved, which is exponential in comparison to classical designs for the same parameters. For example, it is not yet known if a 3 - $(8, 4, 1; 2)$ subspace design exists; such a design would have 6477 blocks, chosen from an ambient space having 200,787 4-dimensional subspaces. Its classical analogue, the extended Fano plane, has 14 blocks, chosen from a collection of 70 4-sets. In [4], a construction of a q -analogue of a perfect matroid design (q -PMD) was given, which is a q -matroid for which all flats of the same dimension have the same rank. This q -PMD yields a construction of a subspace design from a q -Steiner system. In the following sections we will show another way that subspace designs and weighted subspace designs can arise from q -polymatroids satisfying certain rigidity properties.

The *intersection numbers* of a weighted subspace design are important invariants and can be used to establish non-existence results.

Theorem 61. *Let (E, \mathcal{B}, f) be a t - $(n, k, \lambda; q)$ weighted subspace design and let I, J be two subspaces of E of dimension i and j , respectively such that $I \cap J = \{0\}$. If $i + j \leq t$, then*

$$\sum_{B \in \mathcal{B}: I \leq B, B \cap J = \{0\}} f(B) = q^{(k-i)j} \begin{bmatrix} n-i-j \\ k-i \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1} \lambda.$$

In particular, this number is independent of the choice of I of dimension i and J of dimension j . We denote it by $\lambda_{i,j}$.

Proof. If X be a subspace of E of dimension $x \leq t$, then since (E, \mathcal{B}, f) is a weighted subspace design, we have

$$\begin{aligned} \begin{bmatrix} k-x \\ t-x \end{bmatrix}_q \sum_{B \in \mathcal{B}: X \leq B} f(B) &= \sum_{B \in \mathcal{B}: X \leq B} \sum_{T: X \leq T \leq E, \dim(T)=t} f(B), \\ &= \sum_{T: X \leq T \leq E, \dim(T)=t} \sum_{B \in \mathcal{B}: T \leq B} f(B) = \begin{bmatrix} n-x \\ t-x \end{bmatrix}_q \lambda. \end{aligned} \quad (3)$$

Now suppose that $X = I + K$ for some $K \leq J$ of dimension s . Then $I \cap K = \{0\}$ and $\dim(I + K) = i + s$ and so (3) becomes:

$$g(K) := \sum_{B \in \mathcal{B}: I+K \leq B} f(B) = \begin{bmatrix} n-(i+s) \\ t-(i+s) \end{bmatrix}_q \begin{bmatrix} k-(i+s) \\ t-(i+s) \end{bmatrix}_q^{-1} \lambda.$$

Define $h(K) = \sum_{B \in \mathcal{B}: I \subseteq B, B \cap J = K} f(B)$. We wish to compute $h(\{0\})$. Since $g(\{0\}) = \sum_{K \leq J} h(K)$, applying Möbius inversion on the lattice $\mathcal{L}(J)$, we get:

$$\begin{aligned} h(\{0\}) &= \sum_{K \leq J} \mu(0, K) g(K) = \sum_{s=0}^j \begin{bmatrix} j \\ s \end{bmatrix}_q (-1)^s q^{\binom{s}{2}} \begin{bmatrix} n-i-s \\ t-i-s \end{bmatrix}_q \begin{bmatrix} k-i-s \\ t-i-s \end{bmatrix}_q^{-1} \lambda \\ &= \lambda \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1} \sum_{s=0}^j (-1)^s q^{\binom{s}{2}} \begin{bmatrix} j \\ s \end{bmatrix}_q \begin{bmatrix} n-i-s \\ k-i-s \end{bmatrix}_q \\ &= \lambda \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1} q^{j(k-i)} \begin{bmatrix} n-i-j \\ k-i \end{bmatrix}_q, \end{aligned}$$

where the last equality follows from Lemma 19. \square

Remark 62. The proof outlined above is a direct q -analogue of [3, Theorem 2.6]. The intersection numbers for subspace designs were given in [7, 18], for which the authors proposed an inductive argument.

We have the following constructions of new weighted subspace designs from a given one.

Corollary 63. *Let $\mathcal{D} := (E, \mathcal{B}, f)$ be a weighted t - $(n, k, \lambda; q)$ design. Let $I, J \leq E$ have dimension i and j , respectively, for $0 \leq i, j \leq t$.*

- (1) \mathcal{D} is an $i - (n, k, \lambda_i; q)$ weighted subspace design with $\lambda_i = \begin{bmatrix} n-i \\ k-i \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1} \lambda$
- (2) Define $\mathcal{B}^\perp := \{B^\perp : B \in \mathcal{B}\}$. Then $\mathcal{D}^\perp = (E, \mathcal{B}^\perp)$ is a $t - (n, n-k, \lambda^\perp; q)$ weighted subspace design with $\lambda^\perp := \begin{bmatrix} n-k \\ t \end{bmatrix}_q \begin{bmatrix} k \\ t \end{bmatrix}_q^{-1} \lambda$.

Proof. To see that (1) holds, apply Theorem 61 with $\lambda_i := \lambda_{i,0}$. Let I be an i -dimensional subspace of E . We have $\lambda_{i,0} = \sum_{B \in \mathcal{B}: I \leq B} f(B) = \begin{bmatrix} n-i \\ k-i \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1}$.

To see that (2) holds, apply Theorem 61 with $\lambda^\perp := \lambda_{0,t}$. Clearly the members of \mathcal{B} all have dimension $n-k$. A t -dimensional subspace T is contained in $B^\perp \in \mathcal{B}^\perp$ if and only if $B \leq T^\perp$, in which case B has trivial intersection with a t -dimensional space. \square

6.2. Subspace Designs from q -Polymatroids. We now present criteria for the existence of a weighted subspace design arising from the dependent spaces of a q -matroid. The approach is in essence a generalization of the original argument given by Assmus and Mattson [1]. To do this, we obtain a q -analogue of [3, Theorem 3.3]. Throughout this section we let \mathbb{F} denote an arbitrary field. Since $p(M; z) \in \mathbb{Z}[z]$, it gives a well-defined function on any field, viewed as a \mathbb{Z} -module. We define the following sets (c.f. [3]).

Definition 64. Let $\theta \in \mathbb{F}$. We define the following.

- $D_M(i; \theta) := \{X \leq E : \dim(X) = i, p(M.X; \theta) \neq 0\}$,
- $R_M(t; \theta) := \{j \in \{1, \dots, n-t\} : A_{M^*}(j; \theta) \neq 0\}$,
- $d_M := \min\{\dim(X) : X \leq E, X \text{ is a cocircuit of } M\}$.

Proposition 65. Let $\theta \in \mathbb{F}$ such that $\theta^s \neq 1$ for any $s \in \{1, \dots, r\}$. For each $i \in \{1, \dots, n\}$, the following holds. The members of $D_M(i; \theta)$ are all dependent spaces of M^* . Moreover $D_M(d_M; \theta)$ is precisely the set of all circuits of M^* of dimension d_M .

Proof. If $X \in D_M(i; \theta)$ then $p(M.X; \theta) \neq 0$, which by Lemma 27, means that X is a dependent space of M^* . By Lemma 28, for any circuit X of M^* we have $p(M.X; z) = z^{\ell(X^\perp)} - 1$. By (R2), $\rho^*(X)$ is lower-bounded by the rank of any of its subspaces, which are all independent in M^* . Therefore, $\rho^*(X) \geq r(\dim(X) - 1)$ and so

$$r = r \dim(X) - r(\dim(X) - 1) \geq r \dim(X) - \rho^*(X) = \ell(X^\perp) > 0.$$

By hypothesis, $p(M.X; \theta) = \theta^{\ell(X^\perp)} - 1 \neq 0$ and so $X \in D_M(\dim(X); \theta)$. In particular, $D_M(d_M; \theta)$ is precisely the set of all circuits of M^* of dimension d_M . \square

We will now present the main results of this section: Theorem 66 and its two corollaries.

Theorem 66. Let $\theta \in \mathbb{F}$ such that $\theta^s \neq 1$ for any $s \in \{1, \dots, r\}$. Let $t < d_M$ be a positive integer. Suppose that $\sigma^* := |R_M(t; \theta)| \leq d_M - t$ and suppose further that for each t -dimensional subspace T and $j \leq n - t$ it holds that

$$A_{M^*}(j; \theta) = 0 \implies A_{M^*/T}(j; \theta) = 0.$$

Then $(E, D_M(d_M; \theta), f)$ is a weighted t -design over \mathbb{F}_q with $f(X) := p(M.X; \theta)$.

Proof. Let T be a t -dimensional subspace of E . Since $t < d_M$, T is independent in M^* . By Lemma 15, any dependent space A of M^*/T has the form $A = B/T$ for a dependent space B of M^* . Therefore,

$$\sigma^* \leq d_M - t \leq \dim(B) - t = \dim(A). \quad (4)$$

In other words, no dependent space of M^*/T has dimension less than σ^* . By Lemma 27, if X is independent in M^*/T then $p((M^*/T)^*.X; \theta) = 0$. Therefore,

$$A_{(M^*/T)^*}(i; \theta) = \sum_{X \leq E/T: \dim(X)=i} p((M^*/T)^*.X; \theta) = 0, \text{ for all } 0 \leq i \leq \sigma^* - 1.$$

By hypothesis, $A_{M^*/T}(j; \theta) = 0$ for all $j \notin R_M(t; \theta)$. So the coefficients,

$$[A_{M^*/T}(j; \theta) : j \notin R_M(t; \theta)] \text{ and } [A_{(M^*/T)^*}(i; \theta) : 0 \leq i \leq \sigma^* - 1],$$

are known. Now apply Corollary 59, (setting $S = R_M(t; \theta)$) to see that the coefficients

$$[A_{M^*/T}(j; \theta) : j \in R_M(t; \theta)] \text{ and } [A_{(M^*/T)^*}(i; \theta) : \sigma^* \leq i \leq n - t],$$

are uniquely determined and independent of our choice of T of dimension t . It follows that the $A_{(M^*/T)^*}(i; \theta)$ are uniquely determined for $0 \leq i \leq n - t$. We will now show that

$$\sum_{X \in D_M(d_M; \theta): T \leq X} p(M.X; \theta) = A_{(M^*/T)^*}(d_M - t; \theta)$$

which will establish that $(E, D_M(d_M; \theta), f)$ is a weighted t -design over \mathbb{F}_q with $f(X) := p(M.X; \theta)$.

Let B be a circuit of M^* that contains T such that $\dim(B) = d_M$. From Lemma 15, B/T is a circuit of M^*/T and $\dim(B/T) = \dim(B) - t = d_M - t$. Conversely, if A is a circuit of M^*/T satisfying $\dim(A) = d_M - t$, then $A = B/T$ for a dependent space B of M^* of dimension $\dim(B) = d_M$, which is therefore a circuit of M^* , as it has minimal dimension.

By Proposition 65, $D_M(d_M; \theta)$ is precisely the set of all cocircuits of M of dimension d_M and hence there is a one-to-one correspondence between the members of $D_M(d_M; \theta)$ that contain T and the circuits of M^*/T of dimension $d_M - t$. By (4), no dependent space of M^*/T has

dimension less than $d_M - t$, so any dependent space of M^*/T of dimension $d_M - t$ is a circuit of M^*/T and all such circuits are members of $D_{(M^*/T)^*}(d_M - t; \theta)$. Therefore, there is a one-to-one correspondence between the members of $D_M(d_M; \theta)$ that contain T and the members of $D_{(M^*/T)^*}(d_M - t; \theta)$.

From Corollary 31, for any circuit X/T of M^*/T we have

$$p((M^*/T)^*.(X/T); \theta) = \theta^{\ell(X^\perp)} - 1.$$

Therefore,

$$\begin{aligned} \sum_{X \in D_M(d_M; \theta), T \leq X} p(M.X; \theta) &= \sum_{X \in D_M(d_M; \theta), T \leq X} (\theta^{\ell(X^\perp)} - 1), \\ &= \sum_{X/T \in D_{(M^*/T)^*}(d_M - t; \theta)} (\theta^{\ell(X^\perp)} - 1), \\ &= \sum_{X/T \leq E/T: \dim(X/T) = d_M - t} p((M^*/T)^*.(X/T); \theta), \\ &= A_{(M^*/T)^*}(d_M - t; \theta), \end{aligned}$$

which is independent of our choice of T of dimension t . It follows that $(E, D_M(d_M; \theta), f)$ is a weighted t -design over \mathbb{F}_q with $f(X) := p(M.X; \theta)$. \square

Remark 67. Recall that in Remark 33 we observed that if $W, T, X \leq E$ satisfy $T \leq W$ and $\phi(W/T) = X$ then $M|_{T^\perp}.X = M|_{T^\perp}/W^\perp$. Clearly, $\dim(W) = \dim(X) + \dim(T)$ and so if T is a t -dimensional space then:

$$A_{M|_{T^\perp}}(j; z) = \sum_{X \leq T^\perp: \dim(X) = j} p(M|_{T^\perp}.X; z) = \sum_{W \leq E: \dim(W) = j+t} p(M|_{T^\perp}/W^\perp; z).$$

Remark 68. In the proof of Theorem 66, we saw that with the hypothesis of the theorem, that the $A_{(M^*/T)^*}(i; \theta)$ (and therefore the $A_{M^*/T}(i; \theta)$) are uniquely determined for $0 \leq i \leq n - t$. By Lemma 13, it then follows that the $A_{M|_{T^\perp}}(i; \theta)$ are uniquely determined for $0 \leq i \leq n - t$.

Corollary 69. Let $\theta \in \mathbb{F}$ such that $\theta^s \neq 1$ for any $s \in \{1, \dots, r\}$. Let $t < d_M$ be a positive integer. Suppose that $\sigma^* := |R_M(t; \theta)| \leq d_M - t$ and suppose further that for each t -dimensional subspace T and $j \leq n - t$ it holds that

$$A_{M^*}(j; \theta) = 0 \implies A_{M^*/T}(j; \theta) = 0.$$

Then for each $j \in \{d_M, \dots, n - t\}$, $(E, D_M(j; \theta), f)$ is a weighted t -design over \mathbb{F}_q with $f(X) := p(M.X; \theta)$.

Proof. We will prove by induction on $w \in \{d_M, \dots, n - t\}$ that $(E, D_M(w, \theta), f)$ is a weighted t -design. The first step was proved in Theorem 66. Suppose now that $(E, D_M(j, \theta), f)$ is a weighted t -design for each $j \in \{d_M, \dots, w - 1\}$. We will show that $(E, D_M(w, \theta), f)$ is also a weighted t -design.

Let $T \leq E$ have dimension t and let $W \leq E$ contain T and have dimension w . Let $A \leq W$ such that $A + T = W$. Then $A \cap T = I$ for a unique subspace I of dimension i , so that $\dim(A) = w - t + i$. Therefore,

$$\{A \leq W : A + T = W\} = \bigcup_{I \leq T} \{A \leq W : A \cap T = I, \dim(A) = w - t + \dim(I)\}.$$

Using this observation and Lemma 32 we have

$$p(M|_{T^\perp}/W^\perp) = \sum_{A: A+T=W} p(M.A; \theta) = \sum_{I \leq T} \sum_{A: A \leq W, A \cap T = I, \dim(A) = w - t + \dim(I)} p(M.A; \theta).$$

By hypothesis, for each $1 \leq j \leq w-1$, $(E, D_M(j, \theta), p(M \bullet))$ is a weighted t -design, and so by Theorem 61, for any subspaces $I \leq T$ of dimension $0 \leq i < t$ (so that $d_M - t \leq w - t \leq w - t + i \leq w - 1$) we have

$$\sum_{A: A \leq W, A \cap T = I, \dim(A) = w - t + i} p(M.A; \theta) = \Lambda_{i, t-i}^w(M; \theta),$$

for $\Lambda_{i, t-i}^w(M; \theta)$ that depend only on t, w, i . It follows that

$$p(M|_{T^\perp}/W^\perp) = p(M.W; \theta) + \sum_{I < T} \Lambda_{\dim(I), t - \dim(I)}^w(M; \theta) = p(M.W; \theta) + \sum_{i=0}^{t-1} \binom{t}{i} \Lambda_{i, t-i}^w(M; \theta).$$

Therefore, by Remark 67 we have

$$\begin{aligned} A_{M|_{T^\perp}}(w-t; \theta) &= \sum_{W: T \leq W, \dim(W) = w} p(M|_{T^\perp}/W^\perp) \\ &= \sum_{W: T \leq W, \dim(W) = w} \left(p(M.W; \theta) + \sum_{i=0}^{t-1} \binom{t}{i} \Lambda_{i, t-i}^w(M; \theta) \right) \\ &= \sum_{W: T \leq W, \dim(W) = w} p(M.W; \theta) + \binom{n-t}{w-t} \sum_{i=0}^{t-1} \binom{t}{i} \Lambda_{i, t-i}^w(M; \theta). \end{aligned}$$

By Remark 68, $A_{M|_{T^\perp}}(w-t; \theta)$ is independent of our choice of T of dimension t . It follows that

$$\sum_{W: T \leq W, \dim(W) = w} p(M.W; \theta) \text{ depends only on the integers } w, t. \quad \square$$

Corollary 70. *Let $\theta \in \mathbb{F}$ such that $\theta \neq 1$. Let $t < d_M$ be a positive integer. Suppose that $\sigma^* := |R_M(t; \theta)| \leq d_M - t$ and suppose further that for each t -dimensional subspace T and $j \leq n - t$ it holds that*

$$A_{M^*}(j; \theta) = 0 \implies A_{M^*/T}(j; \theta) = 0.$$

Then for each $j \in \{d_{M^}, \dots, n - t\}$, $(E, D_{M^*}(j; \theta), f^*)$ is a weighted t -design over \mathbb{F}_q with $f^*(X) := p(M^*.X; \theta)$ for all subspaces $X \leq E$.*

Proof. For each $d_{M^*} \leq j \leq n - t$, define the set $\mathcal{D}_j := \{X^\perp : X \in D_{M^*}(j; \theta)\}$. Let T be a t -dimensional subspace of E . Then for each j we have:

$$\sum_{X \in D_{M^*}(j, \theta), T \leq X^\perp} p(M^*.X; \theta) = \sum_{X: X \leq T^\perp, \dim(X) = j} p(M^*.X; \theta) = \sum_{X: X \leq T^\perp, \dim(X) = j} p(M^*/X^\perp; \theta).$$

Now for each $X \leq T^\perp$ we have $(E/T)/(X^\perp/T) \cong E/X^\perp$ and it is easy to see that the corresponding q -polymatroids are lattice-equivalent. Then, applying Lemma 13 and using the fact that $\phi(X^\perp/T)^{\perp(T^\perp)} = X$, we get

$$M^*.X \cong (M^*/T)/(X^\perp/T) \cong (M|_{T^\perp})^*/\phi(X^\perp/T) = (M|_{T^\perp})^*.\phi(X^\perp/T)^{\perp(T^\perp)} \cong (M|_{T^\perp})^*.X.$$

Therefore,

$$\sum_{X \in \mathcal{D}_j, T \leq X} p(M^*.X; \theta) = \sum_{X: T \leq X, \dim(X) = n-j} p((M|_{T^\perp})^*.X; \theta) = A_{(M|_{T^\perp})^*}(n-j; \theta).$$

From Remark 68, $A_{(M|_{T^\perp})^*}(n-j; \theta)$ is independent of the choice of T of dimension t . It follows that (E, \mathcal{D}_j, f^*) is a weighted subspace design with f^* defined by $f^*(X) = p(M^*.X; \theta)$ for each $X \leq E$. The result now follows by Corollary 63: the required subspace design is the dual of (E, \mathcal{D}_j, f^*) . \square

Remark 71. The quantities in Definition 64 and the results of Proposition 65, Theorem 66 and Corollaries 69 and 70 all hold with an indeterminate z in place of a specific choice of θ in \mathbb{F} . In particular, $p(M.X; z)$ is a non-zero polynomial on \mathbb{F} for any cocircuit X of M .

In general, a (q, r) -polymatroid M may satisfy the hypothesis of Corollary 69 for one choice of θ , but fail for another choice. However, if the hypothesis holds for indeterminate z , then a weighted t -design over \mathbb{F}_q can be constructed for any choice of θ that doesn't vanish on $p(M.X; z)$ for a cocircuit X of M . This is the case with the uniform q -matroid.

Example 72. Let k be a positive integer, $k \leq n$ and let $M = (E, \rho)$ be the uniform q -matroid, with rank function defined as follows:

$$\rho(U) := \begin{cases} \dim(U) & \text{if } \dim(U) \leq k, \\ k & \text{if } \dim(U) > k. \end{cases}$$

We denote this q -matroid by $U_{k,n}$. Then $M^* = (E, \rho^*)$ is the uniform q -matroid $U_{n-k,n}$, whose independent spaces are exactly those of dimension $n - k$ or less, and for which all other spaces are dependent and have rank $n - k$. Therefore, $d_M = n - k + 1$ is the size of any cocircuit of M . Now $p(M^*.X; z) = 0$ for all subspaces X such that $1 \leq \dim(X) \leq k$, as these are the independent spaces of M , and so $A_{M^*}(i; z) = 0$ for all $i \in \{1, \dots, k\}$. Therefore for any $t \leq d_M - 1 = n - k$, we have $R_M(t; z) \leq \{k + 1, \dots, n - t\}$ and so $|R_M(t; z)| \leq n - k - t \leq d_M - t$.

We claim that $A_{M^*/T}(j, z) = 0$ whenever $A_{M^*}(j, z) = 0$ for $j \in \{1, \dots, n - t\}$ and $t \in \{1, \dots, n - k\}$. Let T be a t -dimensional subspace of E . By Lemma 24, the q -matroid M^*/T satisfies

$$A_{M^*/T}(j, z) = \sum_{X \leq T^\perp: \dim(X)=j} p(M^*.X; z) = 0 \quad \forall j \in \{1, \dots, k\}.$$

Therefore, $A_{M^*}(j; z) = A_{M^*/T}(j, z) = 0$ for $j \in \{1, \dots, k\}$.

Let $X \leq E$ be a subspace of dimension at least $k + 1$ and let subspace $U \leq E$ be a subspace containing X^\perp . Since $\dim(U/X^\perp) \geq \dim(U) - n + k + 1$, if $\dim(U/X^\perp) \geq 1$ then $\dim(U) \geq n - k$ and so $\rho^*(U) = n - k$. Then $\rho(X^\perp) = \dim(X^\perp) \leq n - k - 1$ and

$$\rho_{M^*/X^\perp}(U/X^\perp) = \rho^*(U) - \rho^*(X^\perp) = \rho^*(U) - \dim(X^\perp) \geq \rho^*(U) - n + k + 1 = 1.$$

In particular, $M^*.X$ has no loops and so by Lemma 38, $p(M^*.X; z)$ is a monic polynomial of degree $n - k - \dim(X^\perp)$. Therefore, if $A_{M^*}(j; z) = 0$, then $p(M^*.X; z) = 0$ for each j -dimensional space X , $k + 1 \leq j \leq n - 1$. It follows again by Lemma 24 that $A_{M^*}(j; z) = 0$. Therefore, $M = U_{k,n}$ satisfies the hypothesis of Corollary 69, so that $(E, D_{U_{k,n}}(i, z), p(U_{k,n}; z))$ is a weighted t -design for $1 \leq t < n - k$.

6.3. Further Implications. We now obtain a weaker form of the Assmus-Mattson theorem for matrix codes as a direct consequence of Theorem 66. Note that the result for subspace designs (those weighted designs with $f(B) = 1$) obtained from rank-metric codes was shown in [6] with the further assumption that the number of codewords with a given support was dependent only on the dimension i of that space for some range of i .

Corollary 73. *Let C be an \mathbb{F}_q - $[n \times m, k, d]$ rank metric code. Let $t < d$ be a positive integer and let C^\perp have no more than $d - t$ distinct rank weights in the set $\{1, \dots, n - t\}$. For each $i \in \{d, \dots, n - t\}$, let*

$$B(i) = \{U \leq E : \dim(U) = i, |C_{=U}| \neq 0\}.$$

Then for each $i \in \{d, \dots, n - t\}$, $(E, B(i), f)$ is a weighted t -design over \mathbb{F}_q with $f(X) := |C_{=X}|$.

Proof. By Lemma 48, we have that $(M_C)^* = M_{C^\perp}$ and for any $i \in \{1, \dots, n\}$, $W_i(C^\perp) = A_{(M_C)^*}(i; q)$. Also, $p(M_C.X; q) = |C_{=X}|$ for any subspace $X \leq E$. Now $d_M = \min\{\dim X : X \text{ is a cocircuit of } M\}$, which by Proposition 65, is the minimum dimension of any subspace X such that $p(M.X; q) \neq 0$.

Since C has minimum distance d , there exists a d -dimensional subspace $X \leq E$ such that $|C_{=X}| = p(M.X; q) \neq 0$, while $p(M.U; q) = 0$ for every subspace $U \leq E$ with $\dim(U) < d$. Therefore, $d = d_M$. By hypothesis, at most $d - t = d_M - t$ of the integers $W_i(C^\perp)$ are non-zero for $i \in \{1, \dots, n - t\}$. By Lemma 48,

$$A_{(M_C)^*}(i; q) = 0 \implies A_{(M_C)^*/T}(i; q) = 0,$$

for any t -dimensional subspace $T \leq E$. Therefore M_C satisfies the hypothesis of Corollary 69 and so the result follows. \square

In the case of a q -matroid M satisfying the hypothesis of Theorem 66, with an extra assumption on the cocircuits of M , our results imply the existence of a subspace design.

Corollary 74. *Let M be a q -matroid, $\theta \in \mathbb{F}, \theta \neq 1$ and let p be the greatest integer such that any subspace $X \leq E$ of dimension at most p contains at most one cocircuit of M . Then, for each $i \in \{d_M, \dots, p\}$, it holds that $D_M(i; \theta) = \{C \leq E : C \text{ is a cocircuit of } M, \dim(C) = i\}$.*

Proof. If C is a cocircuit of M then $p(M.C; \theta) = \theta - 1 \neq 0$ and so $C \in D_M(\dim(C); \theta)$. Now let $X \in D_M(i; \theta)$ for some $i \leq p$. Then $p(M.X; \theta) \neq 0$ and X is a dependent space of M^* of dimension at most p , so that X contains a unique circuit. By Theorem 40, we have $X = C$ and the result follows. \square

Corollary 75. *Let M be a q -matroid that has at least one circuit and one cocircuit. Let $t < d_M$ be a positive integer such that the hypothesis of Theorem 66 holds for some $\theta \in \mathbb{F}, \theta \neq 1$. Let p be the greatest integer such that any subspace $X \leq E$ of dimension at most p contains at most one cocircuit (respectively, at most one circuit) of M . Then for each $i \in \{d_M, \dots, p\}$ (respectively, $\{d_{M^*}, \dots, p\}$) the set of cocircuits (respectively, the set of circuits) of M of dimension $\min\{i, n - t\}$ form the blocks of a t -subspace design. Consequently, for each $i \in \{d_M, \dots, p\}$ (respectively, $\{d_{M^*}, \dots, p\}$), the set of hyperplanes of M (respectively, of M^*) of dimension $n - i$ form the blocks of a t -subspace design.*

Proof. From Corollary 74, for each $i \in \{d_M, \dots, p\}$ we have that $C_i := D_M(i; \theta)$ is the set of cocircuits of M of dimension i . Then by Corollary 69, for each $i \in \{d_M, \dots, p\}$, C_i is the set of blocks of a weighted t -subspace design with $f(X) = p(M.X; \theta) = \theta - 1$. Define a function $\hat{f} : D_M(i; \theta) \rightarrow \mathbb{F}$ by $\hat{f}(X) = (\theta - 1)^{-1}f(X)$. This yields a t -subspace design \mathcal{D}_i whose blocks are C_i . By [5, Corollary 71], for each i -dimensional cocircuit X of M , X^\perp is a hyperplane of M and has dimension $n - i$. By Corollary 63, the set of hyperplanes of M of dimension $n - i$ form the blocks of a t -subspace design, i.e. the complementary design of \mathcal{D}_i . With the same arguments as above, by Corollary 70 the analogous statements hold for the circuits of M and the hyperplanes of M^* . \square

An element c of an \mathbb{F}_{q^m} - $[n, k, d]$ vector rank metric code C is called *minimal* if for any $c' \in C$, $\sigma(c') \leq \sigma(c) \implies c' \in \langle c \rangle_{\mathbb{F}_{q^m}} := \{\nu c : \nu \in \mathbb{F}_{q^m}\}$. In this case, for $U = \sigma(c)$, we have $p(M.X; q^m) = |C_{=U}| = q^m - 1$. If every codeword of rank i in C is minimal, then $A(M_C^\perp)(i; q^m) = W_i(C^\perp) = (q^m - 1)|D_M(i; q^m)|$. If we apply this with Corollary 75, we retrieve the Assmus-Mattson theorem for \mathbb{F}_{q^m} - $[n, k, d]$ codes (c.f. [6]).

Corollary 76. *Let C be an \mathbb{F}_{q^m} - $[n, k, d]$ code. Let $t < d$ be a positive integer and let C^\perp be an \mathbb{F}_{q^m} - $[n, n - k, d^\perp]$ code having no more than $d - t$ distinct rank weights in the set $\{1, \dots, n - t\}$. Let p be the greatest integer such that every codeword of C of rank at most p is minimal.*

- (1) *The supports of the words of rank weight d in C (respectively d^\perp in C^\perp) form the blocks of a t -design over \mathbb{F}_q .*
- (2) *For each $i \in \{d, \dots, p\}$ (respectively, $\{d^\perp, \dots, p\}$) the supports of the minimal codewords of C (respectively C^\perp) of dimension $\min\{i, n - t\}$ form the blocks of a t -design over \mathbb{F}_q .*

Example 77. In [15, Theorem 12], the author shows that any non-degenerate \mathbb{F}_{q^m} - $[N, k > 1]$ rank metric code with constant weight d satisfies $N = km$, $d = m$ and is generated by a matrix $G \in \mathbb{F}_{q^m}^{k \times N}$ whose N columns form a basis of $\mathbb{F}_{q^m}^k$ as an \mathbb{F}_q vector space. Moreover, the dual code has minimum distance 2. Let C^\perp be an \mathbb{F}_{q^m} - $[km, k, m]$ constant weight code constructed as above. Let $M = M_C$, so that $M^* = M_{C^\perp}$. For any $X \leq \mathbb{F}_q^{km}$, we have $p(M.X; q^m) = 0$ unless X is the support of a codeword of C^\perp , in which case $\dim(X) = m$. Therefore, $A_{M^*}(m, q^m) = q^{km} - 1$, $A_{M^*}(0, q^m) = 1$ and $A_{M^*}(i, q^m) = 0$ for $i \neq 0, m$. Then $d_M = d = 2$ and $R_M(2; \theta) = \{m\}$. Therefore, by Corollary 76 the cocircuits of M of dimension

2, which are the supports of codewords of rank 2, form a 1-design over \mathbb{F}_q . Similarly, the supports of the words of rank m in C^\perp form the blocks of a 1-design over \mathbb{F}_q , in fact a $1-(km, m, 1; q)$ design, which is a q -Steiner system, whose blocks form a spread in \mathbb{F}_q^{km} .

Example 78. Let C be the \mathbb{F}_2^6 - $[6, 3, 3]$ vector rank metric code of Example 55. Then both C and its dual have weight distribution $[1, 0, 0, 567, 37044, 142884, 81648]$. From Corollary 76, the supports of the words of weight 3 and the supports of the words of weight 4 form the blocks of a pair of 1-designs. Explicitly, the supports of the words of rank 3 in C form a $1-(6, 3, 1; 2)$ design, which is a q -Steiner system having 9 blocks. This collection of blocks is a spread in \mathbb{F}_2^6 . The supports of the words of rank 4 form a $1-(6, 4, 140; 2)$ design having 588 blocks.

7. ACKNOWLEDGEMENTS

The authors would like to say thanks to Elif Saçıkara for many useful discussions in the preparation of this work. The authors are grateful to Heide Gluesing-Luerssen and Benjamin Jany for their helpful remarks on q -polymatroid equivalence and lattice-equivalence. This paper stems from a collaboration that was initiated at the Women in Numbers Europe (WIN-E3) conference, held in Rennes, August 26-30, 2019. The authors are very grateful to the organisers: Sorina Ionica, Holly Krieger, and Elisa Lorenzo García, for facilitating their participation at this workshop, which was supported by the Henri Lebesgue Center, the Association for Women in Mathematics (AWM) and the Clay Mathematics Institute (CMI).

REFERENCES

- [1] E. F. Assmus and M. H. F. New 5-designs. *J. Combin. Theory*, 6:122–151, 1969.
- [2] J. Bonin, J. Oxley, and B. Sevatius. *Matroid Theory*. Contemporary Mathematics, 1996.
- [3] T. Britz, G. Royle, and K. Shiromoto. Designs from matroids. *SIAM Journal on Discrete Mathematics*, 23(2):1082–1099, 2009.
- [4] E. Byrne, M. Ceria, S. Ionica, R. Jurrius, and E. Saçıkara. Constructions of new matroids and designs over \mathbb{F}_q . *Women in Numbers Europe III: Research Directions in Number Theory*, 2021.
- [5] E. Byrne, M. Ceria, and R. Jurrius. Constructions of new q -cryptomorphisms. *arXiv:2104.01486v2*, 2021.
- [6] E. Byrne and A. Ravagnani. An Assmus–Mattson theorem for rank metric codes. *SIAM Journal on Discrete Mathematics*, 33(3):1242–1260, 2019.
- [7] P. J. Cameron. Generalisation of Fisher’s inequality to fields with more than one element. *Combinatorics, London Math. Soc. Lecture Note Ser.*, 13:9–13, 1973.
- [8] C. Ding and C. Li. Infinite families of 2-designs and 3-designs from linear codes. *Discrete Mathematics*, 340:2415–2431, 2017.
- [9] H. Gluesing-Luerssen and B. Jany. q -Polymatroids and their relation to rank-metric codes. *arXiv:2104.06570v1*, 2021.
- [10] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani. Rank-metric codes and q -polymatroids. *Journal of Algebraic Combinatorics*, pages 1–19, 2019.
- [11] R. Jurrius and R. Pellikaan. Defining the q -analogue of a matroid. *Electronic Journal of Combinatorics*, 25(3):P3.2, 2018.
- [12] M. K. M. Braun and A. Wassermann. q -Analogues of designs: Subspace designs. In M. Greferath, M. O. Pavčević, N. Silberstein, and M. Á. Vázquez-Castro, editors, *Network Coding and Subspace Designs*, pages 171–211. Springer, 2018.
- [13] J. V. S. Morales and H. Tanaka. An Assmus–Mattson theorem for codes over commutative association schemes. *Designs, Codes, Cryptography*, 86:1039–1062, 2018.
- [14] J. Oxley. *Matroid Theory*. Oxford University Press, second edition, 2011.
- [15] T. H. Randrianarisoa. A geometric approach to rank metric codes and a classification of constant weight codes. *Designs, Codes and Cryptography*, 88:1331–1348, 2020.
- [16] D. J. Shin, P. V. Kumar, and T. Helleseth. An Assmus–Mattson-type approach for identifying 3-designs from linear codes over F_4 . *Designs, Codes, Cryptography*, 31:75–92, 2004.
- [17] K. Shiromoto. Codes with the rank metric and matroids. *Designs, Codes and Cryptography*, 87(8):1765–1776, 2019.
- [18] H. Suzuki. On the inequalities of t -designs over a finite field. *European Journal of Combinatorics*, 11(6):601–607, 1990.
- [19] J. van Lint and R. Wilson. *A Course in Combinatorics*. Cambridge University Press, 1992.
- [20] D. Welsh. *Matroid Theory*. L.M.S Monographs, 1976.
- [21] G. Whittle. Characteristic polynomials of weighted lattices. *Advances in Mathematics*, pages 125–151, 1993.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY COLLEGE DUBLIN, BELFIELD, IRELAND
Email address: `ebyrne@ucd.ie`

DEPT. OF MECHANICS, MATHEMATICS & MANAGEMENT, POLITECNICO DI BARI, ITALY
Current address: Via Orabona 4 - 70125 Bari - Italy
Email address: `michela.ceria@gmail.com`

UNIVERSITY OF PICARDIE JULES VERNE
Current address: 33 rue Saint Leu Amiens, 80039, France
Email address: `sorina.ionica@u-picardie.fr`

FACULTY OF MILITARY SCIENCES, NETHERLANDS DEFENCE ACADEMY, THE NETHERLANDS
Email address: `rpmj.jurrius@mindef.nl`