q-Matroids, their Cyclic Flats and Relations to Codes

Gianira N. Alfarano[1,2] and Eimear Byrne[3]

[1]Institute of Mathematics, University of Zurich, Switzerland,
gianiranicoletta.alfarano@math.uzh.ch
[2]Department of Mathematics and Computer Science, Eindhoven University of Technology, the Netherlands, g.n.alfarano@tue.nl
[3]School of Mathematics and Statistics, University College Dublin, Belfield, Ireland,
ebyrne@ucd.ie

Abstract

In this paper we develop the theory of cyclic flats of q-matroids. We show that the cyclic flats, together with their ranks, uniquely determines a q-matroid and hence derive a new q-cryptomorphism. We introduce the notion of $\mathbb{F}_{q^m}$-independence of an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ and we show that q-matroids generalize this concept, in the same way that matroids generalize the notion of linear independence of vectors over a given field.

Introduction

The concept of q-matroid may be traced back to Crapo's PhD thesis [6]. More recently, the relation between rank-metric codes and q-matroids has led to these combinatorial objects getting a lot of attention from researchers.

There are many equivalent ways to describe a q-matroid axiomatically, which are called *q-cryptomorphisms* [5]. Any (q)-matroid is uniquely determined both by its *lattice of flats* and by its lattice of *cycles*. This led many researchers to investigate the intersection between these lattices, namely the collection of *cyclic flats* of the matroid. Cyclic flats have also played several important roles such as in the work of Brylawski, who showed in [3] that the cyclic flats of a matroid, together with their ranks uniquely determine the matroid. Moreover, Eberhardt showed that they provide the Tutte polynomial in [7], and Bonin and de Mier showed in [2] that every lattice is isomorphic to the lattice of cyclic flats of a matroid. Finally, applications to coding theory have been recently investigated. In fact, it has been proved that many central invariants in coding theory can be naturally described in terms of the lattice of cyclic flats of the associated matroid; see [8, 16].

We define the cyclic flats of a q-matroid along with a *cyclic operator*. We use the two operators in showing that the collection of cyclic flats is a lattice that is not induced by the lattice of flats nor cyclic spaces, nor the lattice of subspaces of the ground space. We show that the lattice of cyclic flats, together with their ranks, fully determines the q-matroid. We exploit the theory of cyclic flats to establish a new q-cryptomorphism and we provide a necessary and sufficient condition for a lattice $\mathcal{Z}$ of subspaces endowed with a function to be the lattice of cyclic flats of a q-matroid. We introduce the notion of $\mathbb{F}_{q^m}$-*independence* of an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$ and we show that q-matroids generalize this concept, in the same way that matroids generalize the notion of linear independence of vectors over a given field.

Notation Throughout this paper, n denotes a fixed positive integer, q is a prime power, and $\mathbb{F}_q$ denotes the finite field of order q. We denote by E a fixed n-dimensional vector space over $\mathbb{F}_q$

and by $\mathcal{L}(E)$ the lattice of subspaces of E, ordered with respect to inclusion. We write $A \leq B$ to indicate that A is a subspace of B. If a subspace is to be understood as being 1-dimensional, we represent it by a lowercase letter, so for instance, $x \leq A$ means that x is a one-dimensional subspace of A. For every $A \in \mathcal{L}(E)$, we denote by $\mathrm{Hyp}(A)$ the set of hyperplanes of A, i.e. the set of codimension-1 subspaces of A. The standard basis of the space $\mathbb{F}_q^n$ is denoted by $\{e_1, \ldots, e_n\}$. Finally, for a space $A \leq E$, we denote by $A^\perp$ the orthogonal complement of A in E, with respect to a fixed non-degenerate bilinear form.

1 Background

In this section, we recall some preliminary notions on q-matroids and rank-metric codes. The following definition of q-matroid is given in terms of a rank function; see [11]. Notice that this definition does not require E to be a vector space over a finite field, however, we will assume that a q-matroid is an object defined with respect to an $\mathbb{F}_q$-vector space.

Definition 1.1. A q-matroid M is a pair (E, r) where r is an integer-valued function defined on $\mathcal{L}(E)$ with the following properties:

(R1) Boundedness: $0 \leq r(A) \leq \dim A$, for all $A \in \mathcal{L}(E)$.

(R2) Monotonicity: $A \leq B \Rightarrow r(A) \leq r(B)$, for all $A, B \in \mathcal{L}(E)$.

(R3) Submodularity: $r(A + B) + r(A \cap B) \leq r(A) + r(B)$, for all $A, B \in \mathcal{L}(E)$.

The function r is called the **rank function** of the q-matroid.

Given a q-matroid (E, r), we define the **nullity** function n to be

$$\nu : \mathcal{L}(E) \to \mathbb{Z}, \ A \mapsto \dim(A) - r(A).$$

Definition 1.2. Let (E, r) be a q-matroid. A subspace A of E is called an **independent** space of (E, r) if $r(A) = \dim A$. We write $\mathcal{I}_r$ to denote the set of independent spaces of the q-matroid (E, r):

$$\mathcal{I}_r := \{I \in \mathcal{L}(E) \mid \dim(I) = r(I)\}.$$

If $x \leq E$ and $r(x) = 0$, then x is called **loop** of M. A subspace that is not an independent space of (E, r) is called a **dependent space** of (E, r). We call $C \in \mathcal{L}(E)$ a **circuit** if it is itself a dependent space and every proper subspace of C is independent. We write $\mathcal{D}_r$ and $\mathcal{C}_r$ to denote the sets of dependent spaces and the circuits of the q-matroid (E, r), respectively. A subspace is called an **open space** of (E, r) if it is a (vector space) sum of circuits. We write $\mathcal{O}_r$ to denote the set of open spaces of (E, r).

We define a closure operator as follows (c.f. [4, Definition 5]).

Definition 1.3. Let (E, r) be a q-matroid. For each $A \in \mathcal{L}(E)$, define

$$\mathrm{Cl}_r(A) := \{x \in \mathcal{L}(E) \mid r(A + x) = r(A)\}.$$

The **closure function** of a q-matroid (E, r) is the function defined by

$$\mathrm{cl}_r : \mathcal{L}(E) \to \mathcal{L}(E) : A \mapsto \mathrm{cl}_r(A) = \sum_{x \in \mathrm{Cl}_r(A)} x.$$

Definition 1.4. A subspace A of a q-matroid (E, r) is called a **flat** or **closed space** if for all $x \in \mathcal{L}(E)$ such that $x \not\leq A$, we have

$$r(A + x) > r(A).$$

We write $\mathcal{F}_r$ to denote the set of flats of the q-matroid (E, r), that is

$$\mathcal{F}_r := \{A \in \mathcal{L}(E) \mid r(A + x) > r(A) \ \forall x \in \mathcal{L}(E),\ x \not\leq A\}.$$

If it is clear from the context, we will simply write $\mathcal{I}, \mathcal{D}, \mathcal{C}, \mathcal{O}, \mathrm{cl}$ in place of $\mathcal{I}_r, \mathcal{D}_r, \mathcal{C}_r, \mathcal{O}_r, \mathrm{cl}_r$. Recall that for any $A \in \mathcal{L}(E)$, we have that $r(A) = r(\mathrm{cl}(A))$; see for instance [9].
Finally, we define the restriction and the contraction operations for q-matroids; see [4, 9].

Definition 1.5. Let $M := (E, r)$ be a q-matroid and $A \leq E$ be any subspace of E. For every space $T \leq A$, we define $r_{M|_A}(T) := r(T)$. The q-matroid $M|_A := (A, r_{M|_A})$ is called the **restriction of** M **to** A. Define a map

$$r_{M/A} : \mathcal{L}(E/A) \to \mathbb{Z} : T \mapsto r(\pi^{-1}(T)) - r(A),$$

where $\pi : E \to E/A$ is the canonical projection. Then the q-matroid $M/A := (E/A, r_{M/A})$ is called the **contraction of** M **from** A.

We conclude with the notion of *dual matroid* ([11]), which we will use in Sections 2 and 4.

Definition 1.6. Let $M = (E, r)$ be a q-matroid and consider the function

$$\begin{aligned} r^* : \mathcal{L}(E) &\to \mathbb{Z}, \\ A &\mapsto \dim(A) - r(E) + r(A^\perp). \end{aligned}$$

Then r^* is a rank function and $M^* = (E, r^*)$ is a q-matroid, called the **dual q-matroid** of M.

2 Cyclic Spaces and Cyclic Flats

This section is devoted to the introduction of the q-analogue of cyclic flats and to present some of the properties of these objects. This will be the starting point for establishing a description of q-matroids in terms of cyclic flats. For the remainder, $M = (E, r)$ will denote an arbitrary but fixed q-matroid with ground space E and rank function r.

2.1 Cyclic Spaces

We first define what it means for a space to be a cyclic subspace of a q-matroid.

Definition 2.1. Let $A \in \mathcal{L}(E)$. We say that A is **cyclic** if $r(A) = r(B)$ for every $B \in \mathrm{Hyp}(A)$.

Equivalently, a space $A \in \mathcal{L}(E)$ is cyclic if $\mathrm{cl}(A) = \mathrm{cl}(B)$ for every $B \in \mathrm{Hyp}(A)$.

Example 2.2. A trivial example of a cyclic space is given by the circuits of M. Indeed, if C is a circuit and $D \in \mathrm{Hyp}(C)$, then $r(D) = \dim(D) = \dim(C) - 1 = r(C)$.

Lemma 2.3. Let $C_1, C_2, \ldots, C_\ell$ be a collection of cyclic subspaces of E. Then $C_1 + \cdots + C_\ell$ is also cyclic.

Definition 2.4. The **cyclic operator** of M is the function defined by

$$\mathrm{cyc}_r : \mathcal{L}(E) \to \mathcal{L}(E),\ A \mapsto \mathrm{cyc}_r(A) := \sum_{\substack{C \leq A \\ C \text{ is cyclic}}} C.$$

If it is clear from the context, we will write $\mathrm{cyc} := \mathrm{cyc}_r$ for the q-matroid M. We say that $A \in \mathcal{L}(E)$ is **cyclically closed** if

$$\mathrm{cyc}(A) = A.$$

From Lemma 2.3, we see that $\mathrm{cyc}(A)$ is cyclic and is the unique maximal cyclic susbpace of A.

A well-known construction of a q-matroid arises from the generator matrix of an $\mathbb{F}_{q^m}$-linear code; see [10, 11]. Let G be a $k \times n$ matrix over $\mathbb{F}_{q^m}$ and for every $U \in \mathcal{L}(\mathbb{F}_q^n)$, let A^U be a matrix whose columns form a basis of U. Then the map

$$r : \mathcal{L}(\mathbb{F}_q^n) \to \mathbb{Z},\ U \mapsto \mathrm{rk}(GA^U), \tag{1}$$

is the rank function of a q-matroid, which we denote by $M[G]$.

Example 2.5. Consider $\mathbb{F}_8 = \mathbb{F}_{2^3}$ and let $\alpha \in \mathbb{F}_8$ be a primitive element satisfying $\alpha^3 = \alpha + 1$. Let G be the following matrix with entries in $\mathbb{F}_8$,

$$G := \begin{pmatrix} 1 & \alpha & \alpha^2 & 1 \\ 0 & 1 & \alpha & 0 \end{pmatrix} \in \mathbb{F}_8^{2\times 4}.$$

Let r be the rank function of $M[G]$ and let $A_1 := \langle e_2, e_3 \rangle \in \mathcal{L}(\mathbb{F}_2^4)$. Then $r(A_1) = 1$ and for all $B \in \mathrm{Hyp}(A_1)$, we have that $r(B) = 1$, hence, for all $x \leq A_1$, $r(B + x) = r(B)$, i.e. A_1 is cyclically closed. On the other hand, $A_2 := \langle e_1 + e_2, e_3, e_4 \rangle$ is not cyclically closed, indeed $\mathrm{cyc}(A_2) = \langle e_1 + e_2 + e_4, e_3 \rangle$.

We now list some basic properties of the cyclic operator.

Theorem 2.6. For every $A, B \in \mathcal{L}(E)$, the cyclic operator satisfies the following properties.

(cyc1) $\mathrm{cyc}(A) \leq A$.

(cyc2) $A \leq B \Rightarrow \mathrm{cyc}(A) \leq \mathrm{cyc}(B)$.

(cyc3) $\mathrm{cyc}(\mathrm{cyc}(A)) = \mathrm{cyc}(A)$.

For every integer i, define the following set

$$N_i := \{A \in \mathcal{L}(E) \mid \nu(A) = i\}.$$

Theorem 2.7. Let $A \in \mathcal{L}(E)$ with $\nu(A) = a$. The following are equivalent.

(1) A is cyclic in M.

(2) A is minimal with respect to inclusion in N_a.

(3) $A^\perp$ is a flat of the dual q-matroid M^*.

(4) A is the vector space sum of the circuits contained in A.

Corollary 2.8. $A \in \mathcal{L}(E)$ is cyclic in M if and only if $(M|_A)^*$ does not contain a loop. Equivalently, $A \in \mathcal{L}(E)$ is cyclic in M if and only if $M|A$ has no coloops.

The collection of cyclic spaces of M forms a lattice, such that for every pair of cyclic spaces C_1, C_2, the join is defined by $C_1 \vee C_2 := C_1 + C_2$ and the meet is defined by $C_1 \wedge C_2 := \mathrm{cyc}(C_1 \cap C_2)$. Indeed, by Lemma 2.3, the sum of two cyclic spaces C_1, C_2 is cyclic. However, the intersection of a pair of cyclic spaces is not cyclic in general: for example the intersection of two circuits is independent and hence not cyclic.

Proposition 2.9. Let $A \in \mathcal{L}(E)$. Then $r(A) - r(\mathrm{cyc}(A)) = \dim(A) - \dim(\mathrm{cyc}(A))$.

2.2 Cyclic Flats

In this subsection, we focus on *cyclic flats*, which are simultaneously cyclic spaces and flats, i.e. spaces that are both open and closed in the q-matroid M. We show that also the collection of cyclic flats of a q-matroid forms a lattice and we prove that this lattice, together with the rank values of the cyclic flats, uniquely determines the q-matroid.

Definition 2.10. $F \in \mathcal{L}(E)$ is a **cyclic flat** if $\mathrm{cyc}(F) = F$ and $\mathrm{cl}(F) = F$. In terms of the rank function, a cyclic flat F satisfies the following two properties:

1. $r(F + x) > r(F)$ for any $x \in \mathcal{L}(E)$, such that $x \not\leq F$.
2. $r(D) = r(F)$ for any $D \in \mathrm{Hyp}(F)$.

We write $\mathcal{Z}_r$ to denote the collection of cyclic flats of M. If it is clear from the context, we will simply write $\mathcal{Z}$.

The interaction between the cyclic and closure opertors is expressed in the following.

Lemma 2.11. Let $X \in \mathcal{L}(E)$.

1. If X cyclically closed in M, then $\mathrm{cl}(X) \in \mathcal{Z}$.
2. If X is a flat of M, then $\mathrm{cyc}(F) \in \mathcal{Z}$.

It follows immediately from Lemmas 2.11 that for every subspace $X \leq E$, we have

$$\mathrm{cl}(\mathrm{cyc}(X)) \in \mathcal{Z}$$
$$\mathrm{cyc}(\mathrm{cl}(X)) \in \mathcal{Z}.$$

Moreover, the following properties hold.

Lemma 2.12. Let cl^* and cyc^* denote the closure and cyclic operators with respect to the dual matroid $M^* = (E, r^*)$. For every $A \in \mathcal{L}(E)$ we have that

(1) $\mathrm{cyc}^*(A)^\perp = \mathrm{cl}(A^\perp)$ and $\mathrm{cyc}(A)^\perp = \mathrm{cl}^*(A^\perp)$.

(2) $\mathrm{cl}(\mathrm{cyc}(A)) \cap A = \mathrm{cyc}(A)$.

(3) $\mathrm{cyc}(\mathrm{cl}(A)) + A = \mathrm{cl}(A)$.

The next proposition shows that the collection of cyclic flats of a q-matroid forms a lattice under inclusion, which is not induced by the lattice of subspaces of the q-matroid nor the one of flats.

Proposition 2.13. The set $\mathcal{Z}$ of cyclic flats of a q-matroid forms a lattice under inclusion, where for any two cyclic flats F_1, F_2 the meet is defined by $F_1 \wedge F_2 := \mathrm{cyc}(F_1 \cap F_2)$ and the join is defined as $F_1 \vee F_2 := \mathrm{cl}(F_1 + F_2)$.

Combining Proposition 2.13 with Lemma 2.9, we get that for every pair of cyclic flats $X, Y \in \mathcal{Z}$,

$$r(X \vee Y) = r(\mathrm{cl}(X + Y)) = r(X + Y),$$
$$r(X \wedge Y) = r(\mathrm{cyc}(X \cap Y)) = r(X \cap Y) - \dim((X \cap Y)/(X \wedge Y)).$$

Brylowski outlined in [3, Proposition 2.1] an algorithm for constructing the lattice of flats of a matroid from its lattice of cyclic flats, along with the ranks of the cyclic flats. In [8, Section 5], the authors also showed how to reconstruct the lattice of flats from the lattice of cyclic flats,

along with their ranks. The same construction applies in the q-analogue. For each $X \in \mathcal{L}(E)$, define two cyclic flats

$$X^\vee := \bigvee_{\substack{Z:Z\in\mathcal{Z},\\ Z\leq X}} Z = \mathrm{cl}\left(\sum_{\substack{Z:Z\in\mathcal{Z},\\ Z\leq X}} Z\right) \leq \mathrm{cl}(X) \quad \text{and} \quad X^\wedge := \bigwedge_{\substack{Z:Z\in\mathcal{Z},\\ X\leq Z}} Z = \mathrm{cyc}\left(\bigcap_{\substack{Z:Z\in\mathcal{Z},\\ X\leq Z}} Z\right),$$

where $\vee$ and $\wedge$ denote the join and meet, respectively of the lattice $\mathcal{Z}$ and where the intersection of an empty set of spaces is equal to the whole space E. Clearly, if X is a cyclic flat then $X^\vee = X$. As in [8, Proposition 6], if $X^\vee \leq X$, we have that X is a flat if and only if for every cyclic flat A satisfying $X^\vee \lneq A \leq X^\wedge$,

$$\dim(X \cap A) - r(A) < \nu(X^\vee). \tag{2}$$

This property can be checked if $\mathcal{Z}$ and the ranks of its elements are known. Note that if this is the case, that is if X is a flat, then $X^\vee = \mathrm{cyc}(X)$. Hence, we draw the following conclusion.

Proposition 2.14. Every q-matroid M is uniquely determined by its lattice of cyclic flats along with their rank values.

Proof. By the algorithm outlined above, the lattice of cyclic flats along with their ranks uniquely determines the lattice of flats of M. By [4], M is uniquely determined by its lattice of flats. □

The next example illustrates how the reconstruction algorithm works.

Example 2.15. Consider the finite field $\mathbb{F}_{2^3} = \mathbb{F}_2[\alpha]$, where $\alpha^3 = \alpha + 1$. Let $G \in \mathbb{F}_{2^3}^{2\times 4}$ be the matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}.$$

Let $M[G] = (\mathbb{F}_2^4, r)$ be the q-matroid associated to G. The only cyclic flat except for $\langle 0\rangle$ is $\langle e_2, e_3, e_4\rangle$; this simple lattice is shown in Figure 1. We have $\mathrm{cyc}(E) = \langle e_2, e_3, e_4\rangle$, which means that $(M[G])^*$ has a loop, by Corollary 2.8.

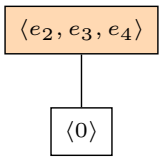

Figure 1: Lattice of cyclic flats of the matroid $M[G]$ from Example 2.15.

Now, we can apply the reconstruction result from the above discussion to obtain all the flats of $M[G]$. Take for instance the space $F = \langle e_1\rangle$. Then $F^\vee = \langle 0\rangle \leq F$ and $F^\wedge = \mathrm{cyc}(E) = \langle e_2, e_3, e_4\rangle$. Then the only cyclic flat A, satisfying $F^\vee \lneq A \leq F^\wedge$ is $\mathrm{cyc}(E)$. We can then verify that (2) is satisfied, i.e.

$$0 - 1 = \dim(\langle e_1\rangle \cap \langle e_2, e_3, e_4\rangle) - r(\langle e_2, e_3, e_4\rangle) < \nu(\langle 0\rangle) = 0.$$

Hence, we conclude that $F = \langle e_1\rangle$ is a flat and $\langle 0\rangle = F^\vee = \mathrm{cyc}(F)$. Moreover, by applying Proposition 2.9, we have that $r(F) = 1$.
For another example, let $B = \langle e_2, e_3\rangle$. Then, as above, $B^\vee = \langle 0\rangle$ and $B^\wedge = \mathrm{cyc}(E) = \langle e_2, e_3, e_4\rangle$. Then the only cyclic flat A, satisfying $B^\vee \lneq A \leq B^\wedge$ is $\mathrm{cyc}(E)$. However, this time we have that

$$1 = 2 - 1 = \dim(\langle e_2, e_3\rangle \cap \langle e_2, e_3, e_4\rangle) - r(\langle e_2, e_3, e_4\rangle) > \nu(\langle 0\rangle) = 0,$$

hence, B is not a flat. With this procedure we can reconstruct the flats of $M[G]$. We list them below, together with their ranks.

$$\begin{aligned}
&\text{rank } r = 0: && \langle 0\rangle.\\
&\text{rank } r = 1: && \langle e_1\rangle, \langle e_1+e_2\rangle, \langle e_1+e_3\rangle, \langle e_1+e_4\rangle, \langle e_1+e_2+e_3\rangle,\\
& && \langle e_1+e_2+e_4\rangle, \langle e_1+e_3+e_4\rangle, \langle e_1+e_2+e_3+e_4\rangle, \langle e_2,e_3,e_4\rangle.\\
&\text{rank } r = 2: && E.
\end{aligned}$$

We conclude this section by providing a characterization in terms of cyclic flats of a well-known family of q-matroids, namely the family of *uniform q-matroids* (c.f [11]). To this end, we denote by $0_{\mathcal{Z}} := \mathrm{cl}(\langle 0\rangle)$ the minimal element and by $1_{\mathcal{Z}} := \mathrm{cyc}(E)$ the maximal element of the lattice of cyclic flats of M.

Definition 2.16. Let $1 \leq k \leq n$. For each $U \in \mathcal{L}(E)$, define $r(U) := \min\{k, \dim(U)\}$. Then (E, r) is a q-matroid. It is called the **uniform q-matroid on E of rank k** and is denoted by $U_{k,n}$.

Proposition 2.17. Let $M = (E, r)$ be a q-matroid of rank k, for $0 < k < n$. Then the following are equivalent.

1. $M = U_{k,n}$.
2. $\mathcal{Z}_r$ contains only two elements, $0_{\mathcal{Z}_r} = \langle 0\rangle$ and $1_{\mathcal{Z}_r} = E$. Moreover $r(1_{\mathcal{Z}_r}) = k$.

3 The Rank Function and Cyclic Flats

We now propose a q-cryptomorphism based on cyclic flats, inspired by Sims' work [15], who proved that any finite lattice is isomorphic to the lattice of cyclic flats of a finite matroid.

Definition 3.1. Let $\mathcal{Z}$ be a collection of subspaces of E and suppose that $(\mathcal{Z}, \leq, \vee, \wedge)$ is a lattice with join and meet operations $\vee$ and $\wedge$, such that for every $Z_1, Z_2 \in \mathcal{Z}$, we have that $Z_1 + Z_2 \leq Z_1 \vee Z_2$ and $Z_1 \wedge Z_2 \leq Z_1 \cap Z_2$, respectively. Let $f : \mathcal{Z} \to \mathbb{Z}$ be a map. We define the following **cyclic flat** axioms.

(Z1) $f(0_{\mathcal{Z}}) = 0$.

(Z2) For every $F, G \in \mathcal{Z}$ such that $G < F$, we have:

$$0 < f(F) - f(G) < \dim(F) - \dim(G).$$

(Z3) For every $F, G \in \mathcal{Z}$ we have:

$$f(F) + f(G) \geq f(F \vee G) + f(F \wedge G) + \dim((F \cap G)/(F \wedge G)).$$

If $(\mathcal{Z}, f)$ satisfies the cyclic flat axioms, we say that $\mathcal{Z}$ is a collection of **cyclic flats** with respect to f.

For the rest of this section, let $M = (E, r)$ be a fixed q-matroid. The following is a preliminary result useful to show that the lattice of cyclic flats satisfies (Z1)–(Z3).

Theorem 3.2. Let $\mathcal{Z}$ be the lattice of cyclic flats of M and let $f : \mathcal{Z} \to \mathbb{Z}$, be the map defined by $f(F) = r(F)$ for all $F \in \mathcal{Z}$. Then $(\mathcal{Z}, f)$ is a collection of cyclic flats with respect to f, i.e. $(\mathcal{Z}, f)$ satisfies (Z1)–(Z3).

As an immediate consequence of Theorem 3.2, we have the following.

Corollary 3.3. Let F, G be two distinct cyclic flats of M, then

$$r(F) - r(G) < \dim(F) - \dim(F \cap G). \tag{3}$$

Definition 3.4. Let $\mathcal{Z}$ be a collection of subspaces of E, and let $f : \mathcal{L}(E) \longrightarrow \mathbb{N}_0$ be a map. We define $f_{\mathcal{Z}} : \mathcal{L}(E) \longrightarrow \mathbb{N}_0$ to be the function defined by

$$f_{\mathcal{Z}}(A) := \min\{f(F) + \dim((A+F)/F) \mid F \in \mathcal{Z}\}, \text{ for all } A \in \mathcal{L}(E). \tag{4}$$

Lemma 3.5. Let $(\mathcal{Z}, f)$ be a lattice of cyclic flats. Then, for every $F, G \in \mathcal{Z}$, we have

$$f(F \vee G) \leq f(G) + \dim(F/(F \cap G)). \tag{5}$$

It is straightforward to check that if $(\mathcal{Z}, f)$ is a lattice of cyclic flats of E then f and $f_{\mathcal{Z}}$ both agree on $\mathcal{Z}$, as we show in the following proposition.

Proposition 3.6. Let $(\mathcal{Z}, f)$ be a lattice of cyclic flats. Then, for every $A \in \mathcal{Z}$, we have $f_{\mathcal{Z}}(A) = f(A)$.

Proposition 3.7. Let $(\mathcal{Z}, f)$ be a lattice of cyclic flats. Then $f_{\mathcal{Z}}$ satisfies the axioms (R1)–(R3). In particular, $(E, f_{\mathcal{Z}})$ is a q-matroid.

Theorem 3.8. Let $(\mathcal{Z}, f)$ be a lattice of cyclic flats. Then $\mathcal{Z}$ is the lattice of cyclic flats of the q-matroid $M_{\mathcal{Z}} := (E, f_{\mathcal{Z}})$.

We summarize the previous results as the following corollary, which gives in turn a new q-cryptomorphism.

Corollary 3.9. Let (E, r) be a q-matroid and $(\mathcal{Z}, \leq, \vee, \wedge)$ be a lattice of subspaces of E.

(1) If $\mathcal{Z}$ is the lattice of cyclic flats of (E, r) then $(\mathcal{Z}, r)$ satisfies the cyclic flat axioms (Z1)-(Z3). In particular, $(E, r_{\mathcal{Z}})$ is a q-matroid satisfying $r_{\mathcal{Z}}(A) = r(A)$ for all $A \in \mathcal{Z}$.

(2) If $(\mathcal{Z}, f)$ satisfies the cyclic flat axioms (Z1)-(Z3) then $\mathcal{Z}$ is the collection of cyclic flats of the q-matroid $(E, f_{\mathcal{Z}})$. In particular, $\mathcal{Z} = \mathcal{Z}_{f_{\mathcal{Z}}}$.

(3) If $\mathcal{Z}$ is the lattice of cyclic flats of E, then $(E, r) = (E, r_{\mathcal{Z}})$.

Proof. The first statement of Part (1) follows from Theorem 3.2. The next statement is a consequence of Proposition 3.6 and Theorem 3.7. Part (2) is the statement of Theorem 3.8. Part (3) can be deduced by Parts (1) and (2) combined with Proposition 2.14. □

4 Rank-Metric Codes and q-Matroids

We establish a connection between the supports of the codewords of a rank-metric code and the open spaces of its associated q-matroid. In the classical theory, matroids were introduced by Whitney in [17] in order to generalize the notion of independence in linear algebra. Similarly, we show how the concept of q-matroidal independence generalizes a notion of independence for an $\mathbb{F}_q$-subspace over $\mathbb{F}_{q^m}$.

Consider the vector space $\mathbb{F}_{q^m}^n$, endowed with the following **rank distance**, defined as $\mathrm{d}_{\mathrm{rk}}(u, v) := \mathrm{rk}(u - v)$ for every $u, v \in \mathbb{F}_{q^m}^n$, where given $v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$

$$\mathrm{rk}(v) := \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q}.$$

Definition 4.1. An $\mathbb{F}_{q^m}$-linear subspace $\mathcal{C}$ of the metric space $\mathbb{F}_{q^m}^n$ is called a **rank-metric code**. We say that $\mathcal{C}$ is an $[n,k]_{q^m/q}$ code, if k is the dimension of $\mathcal{C}$ over $\mathbb{F}_{q^m}$. A matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ of rank k whose rows generate $\mathcal{C}$ is called a **generator matrix**. The **dual code** $\mathcal{C}^\perp$ of $\mathcal{C}$ is the $[n,n-k]_{q^m/q}$ rank-metric code comprising vectors orthogonal to all the vectors in $\mathcal{C}$ with respect to the standard dot product defined by $x\cdot y = \sum_{j=1}^n x_j y_j$ for all $x,y \in \mathbb{F}_{q^m}^n$. Finally, we say that an $[n,k]_{q^m/q}$ rank-metric code $\mathcal{C}$ is **non-degenerate** if the columns of any generator matrix for $\mathcal{C}$ are linearly independent over $\mathbb{F}_q$.

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

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

The **support** of v is the column space of $\Gamma(v)$ for any basis Γ; we denote it by $\sigma(v)$.

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ rank-metric code and let G be a generator matrix of $\mathcal{C}$. For every $U \le \mathbb{F}_q^n$, define the space

$$\mathcal{C}_U := \{v \in \mathcal{C} \mid \sigma(v) \le U^\perp\}.$$

Moreover, consider the following function:

$$r : \mathcal{L}(\mathbb{F}_q^n) \to \mathbb{Z},\ U \mapsto k - \dim_{\mathbb{F}_{q^m}}(\mathcal{C}_U). \tag{6}$$

Note that for any $U \le \mathbb{F}_q^n$, $r(U) = \mathrm{rk}(GA^U)$, where A^U is a matrix whose columns form a basis of U. In fact, r is the same rank function as defined in (1) and it is independent of the choice of generator matrix G. $(\mathbb{F}_q^n, r)$ is called the **q-matroid associated to $\mathcal{C}$** and is denoted by $M_\mathcal{C}$.

Definition 4.2. A q-matroid $M = (\mathbb{F}_q^n, r)$ of rank k is **representable** if there exists some positive integer m and an $[n,k]_{q^m/q}$ rank-metric code $\mathcal{C}$ such that $M = M_\mathcal{C}$.

Definition 4.3. An $[n,k]_{q^m/q}$ **system** is an n-dimensional $\mathbb{F}_q$-space $\mathcal{U} \le \mathbb{F}_{q^m}^k$ with the property that $\langle \mathcal{U}\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$. When the parameters are not relevant, we simply call such an object a **q-system**. Moreover, two $[n,k]_{q^m/q}$ systems $\mathcal{U}$ and $\mathcal{U}'$ are equivalent if there exists an $\mathbb{F}_{q^m}$-isomorphism $\phi \in \mathrm{GL}(k,q^m)$ such that $\phi(\mathcal{U}) = \mathcal{U}'$.

There is a correspondence between equivalence classes of non-degenerate $[n,k]_{q^m/q}$ rank-metric codes and equivalence classes of $[n,k]_{q^m/q}$ systems. We briefly explain this connection; for more details we refer the interested reader to [1, 14].

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ non-degenerate rank-metric code with generator matrix G. Then the $\mathbb{F}_q$-span $\mathcal{U}$ of the columns of G is an $[n,k]_{q^m/q}$ system, it is isomorphic to $\mathbb{F}_q^n$ and we call it the **q-system associated to $\mathcal{C}$**. Conversely, if $\mathcal{U} \le \mathbb{F}_{q^m}^k$ is an $[n,k]_{q^m/q}$-system and $G \in \mathbb{F}_{q^m}^{k\times n}$ is a matrix whose columns form a basis of $\mathcal{U}$, then clearly, the rows of G generate an $[n,k]_{q^m/q}$ rank-metric code.

We recall the following result which provides a natural description of the supports of codewords of $\mathcal{C}$ in the q-system $\mathcal{U}$ associated to $\mathcal{C}$.

Theorem 4.4. [12, Theorem 3.1] Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ non-degenerate rank-metric code and let $\mathcal{U}$ be the $\mathbb{F}_q$-span of the columns of a generator matrix G. Consider the isomorphism

$$\psi_G : \mathbb{F}_q^n \to \mathcal{U},\quad v \mapsto vG^\top. \tag{7}$$

For every $u \in \mathbb{F}_{q^m}^k$ we have that

$$\psi_G^{-1}(\mathcal{U} \cap \langle u\rangle^\perp) = \sigma(uG)^\perp.$$

In the following, we use the terminology "linear basis" of a subspace $V \leq \mathbb{F}_q^n$ to refer to a basis of V as a vector space. This is to distinguish to the notion of basis in the q-matroid sense.

Definition 4.5. Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ rank-metric code with generator matrix G and $\mathcal{U}$ be the $\mathbb{F}_q$-span of the columns of G. An $\mathbb{F}_q$-subspace $V \leq \mathcal{U}$ is called $\mathbb{F}_{q^m}$**-independent** if

$$\dim_{\mathbb{F}_{q^m}}(V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}) = \dim_{\mathbb{F}_q}(V),$$

i.e. the vectors in one (and hence in any) linear basis of V are linearly independent over $\mathbb{F}_{q^m}$.

Thanks to Definition 4.5, we immediately obtain the q-analogue of a well-known result in classical matroid theory; see for instance [13, Theorem 1.1.1].

Theorem 4.6. Let $G \in \mathbb{F}_{q^m}^{k\times n}$ be a full rank matrix whose columns are linearly independent over $\mathbb{F}_q$ and let $\mathcal{U}$ be the $\mathbb{F}_q$-span of the columns of G. Let $\psi_G : \mathbb{F}_q^n \to \mathcal{U},\ v \mapsto vG^\top$. Let $M[G] = (\mathbb{F}_q^n, r)$. The following hold.

1. If $\mathcal{I} := \{I \leq \mathcal{U} \mid I \text{ is } \mathbb{F}_{q^m}\text{-independent}\}$, then $(\mathcal{U}, \mathcal{I})$ is a q-matroid.
2. $\{\psi_G(I) \leq \mathcal{U} \mid I \in \mathcal{I}_r\} = \mathcal{I}$.

Let $\mathcal{C}$ be the $[n,k]_{q^m/q}$ non-degenerate rank-metric code generated by a matrix $G \in \mathbb{F}_q^{k\times n}$, and let $M_\mathcal{C} = (\mathbb{F}_q^n, r)$ be its associated q-matroid. Recall that $M_\mathcal{C}^* = M_{\mathcal{C}^\perp}$, where $\mathcal{C}^\perp$ is the dual code of $\mathcal{C}$; see [11]. The rest of this section is devoted to establishing the connection between the supports of the codewords of $\mathcal{C}$ and $M_\mathcal{C}^*$.

Definition 4.7. A nonzero codeword $c \in \mathcal{C}$ is called **minimal** if for every $c' \in \mathcal{C}$ we have that

$$\sigma(c') \leq \sigma(c) \Leftrightarrow c = \lambda c', \quad \text{for some } \lambda \in \mathbb{F}_{q^m}^*.$$

Lemma 4.8. For every codeword $v \in \mathcal{C}^\perp$, the support $\sigma(v) \leq \mathbb{F}_q^n$ is a dependent space of $M_\mathcal{C}$.

Remark 4.9. The converse of Lemma 4.8 is in general not true. For example, let $v \in \mathcal{C}^\perp$ such that $\mathrm{rk}_{\mathbb{F}_q}(v)$ is maximal over all members of $\mathcal{C}^\perp$. Let U be any subspace of $\mathbb{F}_q^n$ that properly contains $\sigma(v)$. Then U is a dependent space of $M_\mathcal{C}$ since it contains $\sigma(v)$, which is dependent by Lemma 4.8. But by our choice of v, there is no word $u \in \mathcal{C}^\perp$ with $\sigma(u) = U$.

However, we can say that every dependent space D of $M_\mathcal{C}$ contains the support of a codeword of $\mathcal{C}^\perp$. In particular, we have the following result, which immediately follows from Lemma 4.8 and the definitions of circuit and minimal codeword.

Lemma 4.10. A subspace $C \leq \mathbb{F}_q^n$ is a circuit of $M_\mathcal{C}$ if and only if C is the support of a minimal codeword in $\mathcal{C}^\perp$.

Theorem 4.11. Let $c \in \mathcal{C}^\perp$ and let $V = \sigma(c)$. Then V is a cyclic space in $M_\mathcal{C}$.

Corollary 4.12. Let $c \in \mathcal{C}$ be any codeword and let $\{c_1, \ldots, c_t\} \subseteq \mathcal{C}$ be the set of all minimal codewords in $\mathcal{C}$ whose supports are contained in $\sigma(c)$. Then

$$\sigma(c) = \sum_{i=1}^{t} \sigma(c_i).$$

Note that the converse of Theorem 4.11 is not true in general, as Example 4.13 shows.

Example 4.13. Let $\mathcal{C}$ be the $[5,3]_{2^3/2}$ rank-metric code with generator matrix

$$G = \begin{pmatrix} 1 & \alpha & 1 & 0 & \alpha^2 \\ 0 & 1 & \alpha^5 & \alpha^2 & \alpha \\ 0 & 0 & 1 & \alpha^4 & \alpha \end{pmatrix},$$

where $\alpha^3 = \alpha + 1$. The dual code $\mathcal{C}^\perp$ is a $[5,2]_{2^3/2}$ code. Let $M_{\mathcal{C}} = (\mathbb{F}_2^5, r)$ be the q-matroid associated to $\mathcal{C}$. Note that if $c, c' \in \mathcal{C}^\perp$ and $c = \lambda c'$ for some $\lambda \in \mathbb{F}_{2^3}^*$, then $\sigma(c) = \sigma(c')$. There are 9 distinct supports for the codewords of $\mathcal{C}^\perp$ and those are all cyclic spaces in $M_{\mathcal{C}}$, by Theorem 4.11. Moreover, there are 11 cyclic spaces in $M_{\mathcal{C}}$, which are listed below according to their dimensions.

Dimension 0 : $A_0 := 0$.

Dimension 2 : $A_1 := \langle e_1 + e_4 + e_5, e_2 + e_4 \rangle$, $A_2 := \langle e_1 + e_3, e_4 \rangle$,
$A_3 := \langle e_3 + e_5, e_1 + e_2 + e_4 + e_5 \rangle$.

Dimension 3 : $A_4 := \langle e_3 + e_5, e_2, e_4 \rangle$, $A_5 := \langle e_2, e_1 + e_5, e_3 + e_4 + e_5 \rangle$,
$A_6 := \langle e_1 + e_5, e_2 + e_4, e_3 + e_4 + e_5 \rangle$, $A_7 := \langle e_1 + e_5, e_2, e_3 + e_5 \rangle$,
$A_8 := \langle e_1 + e_4 + e_5, e_2, e_3 + e_4 + e_5 \rangle$, $A_9 := \langle e_1 + e_5, e_2 + e_3 + e_5, e_4 \rangle$.

Dimension 4 : $A_{10} := \langle e_1 + e_5, e_2, e_3 + e_5, e_4 \rangle$.

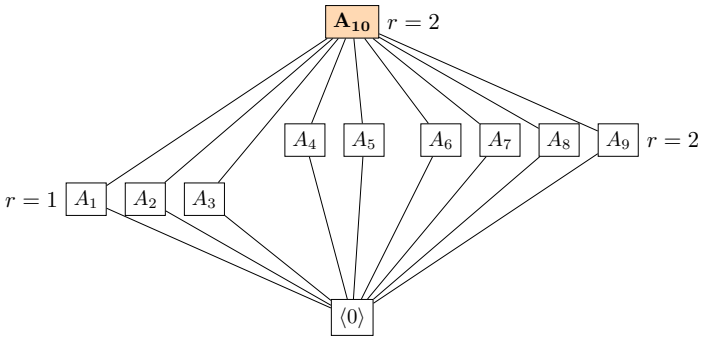

Figure 2: The lattice of cyclic spaces of $M_{\mathcal{C}}$ from Example 4.13.

The space A_{10} is the only cyclic space that is not the support of any codeword in $\mathcal{C}^\perp$. All the cyclic spaces except from A_0 and A_{10} are circuits. Indeed, one can easily observe each codeword in $\mathcal{C}^\perp$ is minimal and has support exactly one of the spaces $A_1, \ldots, A_9$. With the aid of MAGMA, we checked that the q-matroid $M_{\mathcal{C}}$ has 88 flats and that among these only 5 are also cyclic, namely A_0, A_1, A_2, A_3 and A_{10}.

Now, consider the matroid $M_{\mathcal{C}^\perp}$, associated to the code $\mathcal{C}^\perp$ and denote its rank function by r^*. First of all note that $M_{\mathcal{C}^\perp}$ contains the loop $L := \langle e_1 + e_3 + e_5 \rangle$, which is itself cyclic. In $M_{\mathcal{C}^\perp}$ there are in total 88 cyclic spaces and among them 65 are also supports of codewords in $\mathcal{C}$. Finally, there are 11 flats in $M_{\mathcal{C}^\perp}$, which are listed below.

Dimension 1 : $F_0 := \langle e_1 + e_3 + e_5 \rangle$.

Dimension 2 : $F_1 := \langle e_1 + e_3 + e_5, e_4 \rangle$, $F_2 := \langle e_1 + e_3 + e_5, e_4 + e_5 \rangle$,
$F_3 := \langle e_1 + e_3 + e_5, e_2 + e_3 \rangle$, $F_4 := \langle e_3 + e_5, e_1 \rangle$,
$F_5 := \langle e_1 + e_3 + e_5, e_2 + e_3 + e_4 \rangle$, $F_6 := \langle e_1 + e_4 + e_5, e_3 + e_4, e_3 + e_4 \rangle$.

Dimension 3 : $F_7 := \langle e_1 + e_5, e_2 + e_4 + e_5, e_3 \rangle$, $F_8 := \langle e_1 + e_3, e_2, e_5 \rangle$,
$F_9 := \langle e_1 + e_4, e_2 + e_4, e_3 + e_4 + e_5 \rangle$.

Dimension 5 : $F_{10} := \mathbb{F}_2^5$.

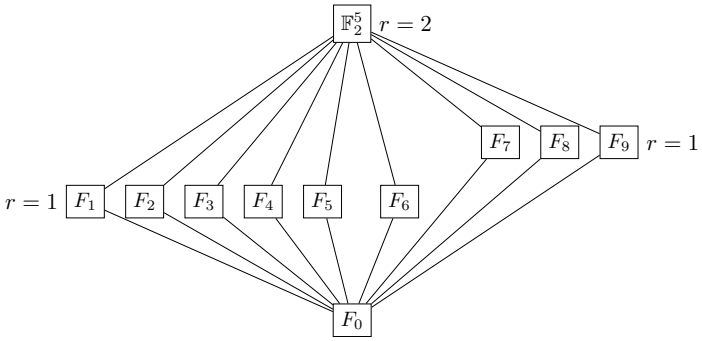

Figure 3: Lattice of flats of the matroid $M_{\mathcal{C}^\perp}$ from Example 4.13.

The lattice of flats of $M_{\mathcal{C}^\perp}$ can be found in Figure 3.

It is not difficult to see that all the flats in Figure 3 are the orthogonal complements of the cyclic spaces of Figure 2, as Theorem 2.7 states. Clearly, the cyclic flats of $M_{\mathcal{C}^\perp}$ are the orthogonal complement of the cyclic flats in $M_{\mathcal{C}}$; see Figure 4. In particular, $A_{10}^\perp = F_0$, $A_1^\perp = F_7$, $A_2^\perp = F_8$ and $A_3^\perp = F_9$.

Finally, using MAGMA, we found that there are exactly 33 minimal codewords in $\mathcal{C}$. The supports of these codewords are circuits in $M_{\mathcal{C}^\perp}$. Consider $Z := \langle e_1+e_5, e_2+e_5, e_3+e_5, e_4+e_5\rangle$ and observe that Z is a cyclic space that is not a circuit (since its rank is 2 and it is not the support of a minimal codeword of $\mathcal{C}$). Z contains exactly 3 circuits, namely $\langle e_1+e_3, e_2+e_5\rangle$, $\langle e_2+e_3+e_4+e_5, e_1+e_5\rangle$ and $\langle e_1+e_4, e_2+e_4\rangle$. It is easy to see that Z is actually equal to the sum of the circuits it contains, as stated in Corollary 4.12.

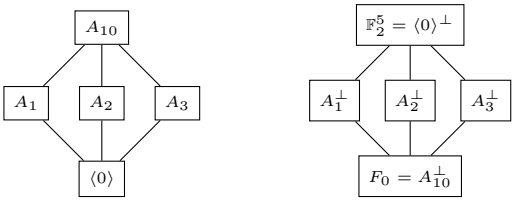

Figure 4: The lattices of the cyclic flats of the q-matroids $M_{\mathcal{C}}$ and $M_{\mathcal{C}^\perp}$ from Example 4.13.

References

[1] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *Journal of Combinatorial Theory, Series A*, 192:105658, 2022.

[2] J. E. Bonin and A. De Mier. The lattice of cyclic flats of a matroid. *Annals of combinatorics*, 12(2):155–170, 2008.

[3] T. H. Brylawski. An affine representation for transversal geometries. *Studies in Applied Mathematics*, 54(2):143–160, 1975.

[4] E. Byrne, M. Ceria, S. Ionica, R. Jurrius, and E. Saçıkara. Constructions of new matroids and designs over $\mathbb{F}_q$. *Designs, Codes and Cryptography*, pages 1–23, 2022.

[5] E. Byrne, M. Ceria, and R. Jurrius. Constructions of new q-cryptomorphisms. *Journal of Combinatorial Theory, Series B*, 153:149–194, 2022.

[6] H. Crapo. *On the theory of combinatorial independence*. PhD thesis, Massachusetts Institute of Technology, Department of Mathematics, 1964.

[7] J. N. Eberhardt. Computing the Tutte polynomial of a matroid from its lattice of cyclic flats. *The Electronic Journal of Combinatorics*, 21(3):P3–47, 2014.

[8] R. Freij-Hollanti, M. Grezet, C. Hollanti, and T. Westerbäck. Cyclic flats of binary matroids. *Advances in Applied Mathematics*, 127:102165, 2021.

[9] H. Gluesing-Luerssen and B. Jany. q-polymatroids and their relation to rank-metric codes. *Journal of Algebraic Combinatorics*, pages 1–29, 2022.

[10] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani. Rank-metric codes and q-polymatroids. *Journal of Algebraic Combinatorics*, 52:1–19, 2020.

[11] R. Jurrius and G. Pellikaan. Defining the q-analogue of a matroid. *The Electronic Journal of Combinatorics*, 25(3), 2018.

[12] A. Neri, P. Santonastaso, and F. Zullo. The geometry of one-weight codes in the sum-rank metric. *Journal of Combinatorial Theory, Series A*, 194:105703, 2023.

[13] J. Oxley. *Matroid Theory*. Oxford University Press, second edition, 2011.

[14] T. H. Randrianarisoa. A geometric approach to rank metric codes and a classification of constant weight codes. *Designs, Codes and Cryptography*, 88(7):1331–1348, 2020.

[15] J. A. Sims. An extension of Dilworth's theorem. *Journal of the London Mathematical Society*, 2(3):393–396, 1977.

[16] T. Westerbäck, R. Freij-Hollanti, T. Ernvall, and C. Hollanti. On the combinatorics of locally repairable codes via matroid theory. *IEEE Transactions on Information Theory*, 62(10):5296–5315, 2016.

[17] H. Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57(3):509–533, 1935.