CONSTRUCTIONS OF NEW q–CRYPTOMORPHISMS

EIMEAR BYRNE, MICHELA CERIA, AND RELINDE JURRIUS

Abstract. In the theory of classical matroids, there are several known equivalent axiomatic systems that define a matroid, which are described as matroid *cryptomorphisms*. A q-matroid is a q-analogue of a matroid where subspaces play the role of the subsets in the classical theory. In this article we establish cryptomorphisms of q-matroids. In doing so we highlight the difference between classical theory and its q-analogue. We introduce a comprehensive set of q-matroid axiom systems and show cryptomorphisms between them and existing axiom systems of a q-matroid. These axioms are described as the rank, closure, basis, independence, dependence, circuit, hyperplane, flat, open space, spanning space, non-spanning space, and bi-colouring axioms.

1. Introduction

The concept of a q-matroid goes back to Crapo [5], although it has only recently been taken up again as a research topic, having been rediscovered in [9]. As the term suggests, it arises as a *q-analogue* of matroid theory, wherein subspaces play the role of the subsets in the classical theory. The definition of a q-matroid with respect to a rank function can be read in [9]: a q-matroid consists of a vector space E together with an integer-valued, *bounded, monotonic increasing, semi-modular* rank function on the lattice of subspaces of E (see Definition 3). There have been a few other recent papers on this topic, especially in relation to rank metric codes. In [8, 13] the authors independently introduced the q-analogue of a polymatroid, namely a q-polymatroid. Their properties have been further studied in [2, 6].

In the theory of classical matroids, there are several known equivalent axiomatic systems that define a matroid, which are described as matroid *cryptomorphisms*. A full exposition of these is given in [3, 11]. This array of cryptomorphisms offers both insight to the structure of a matroid and versatility in applications: one description of a matroid may make it more amenable to a given application than another.

In this article we seek to establish a comprehensive collection of cryptomorphisms of q-matroids. In doing so we highlight the difference between classical theory and its q-analogue. Some cryptomorphisms have already been shown in [9]. In [4], it was shown that the axioms defining a collection of *flats* defines equivalently a q-matroid and conversely that a q-matroid with a given rank function determines a collection of flats. As an application, it was shown that a q-Steiner system yields a q-matroid (in fact a *q-perfect matroid design*) determined by a collection of flats and this was used to construct new *subspace designs*.

In Figure 1, twelve different equivalent axiom systems of q-matroids are shown, which are q-analogues of classical axiomatic systems. As we show in this paper, these systems all equivalently define a q-matroid and hence form a family of q-cryptomorphisms. These axioms are labelled as the *rank, closure, basis, independence, dependence, circuit, hyperplane, flat, open space, spanning space, non-spanning space*, and *bi-colouring axioms*.

Cryptomorphisms between the rank, independence and bases axioms were already proven in [9]. For independence and bases, it turns out there is an extra axiom needed in addition to the classical

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

Key words and phrases. q-analogue, q-matroid, cryptomorphism.

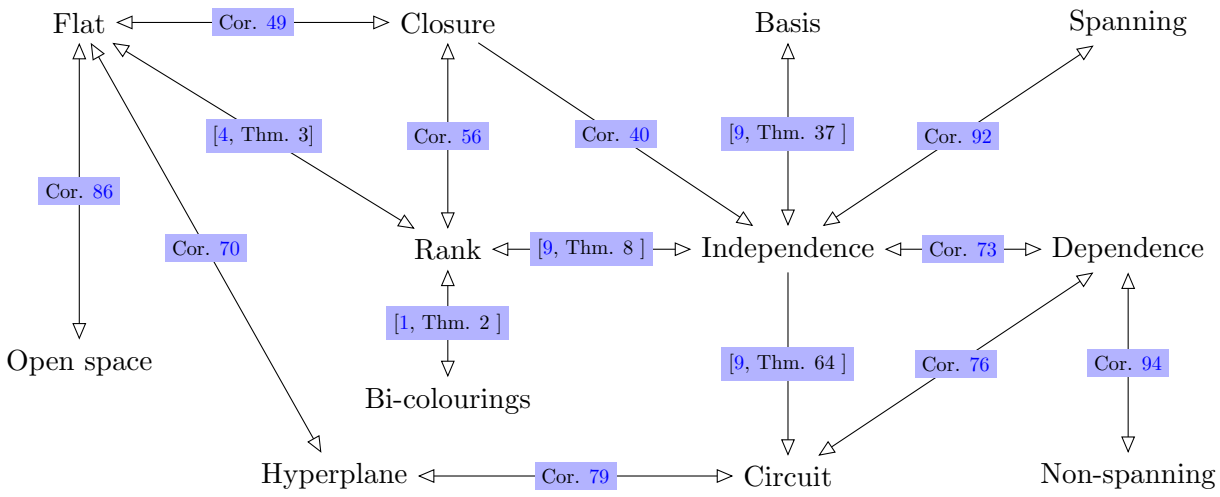


FIGURE 1. Cryptomorphisms

case: simply taking a straightforward q-analogue of the classical axioms is sometimes insufficient to find axioms for a q-matroid. A cryptomorphism between the rank and flat axioms was shown in [4] and that q-matroidal bi-colourings and the rank axioms equivalently define a q-matroid was shown in [1]. That the rank axioms imply the closure axioms was shown in [9], while at that time it was not clear that those closure axioms were sufficient to define a q-matroid. We answer this question affirmatively by showing that the closure and independence axioms are cryptomorphic.

It was shown that the circuit axioms proposed in [9] can be deduced from the independence axioms. Here we establish the converse by proving that the circuit and dependence axioms are cryptomorphic and that the dependence and independence axioms are cryptomorphic. However, we need a different axiom for the circuits than the one proposed in [9]. This is again an illustration that taking straightforward q-analogues of classical axioms is sometimes insufficient. We see this problem also arising in the case of the open space axioms. We furthermore show that the flat and hyperplane axioms are equivalent, from which we easily obtain cryptomorphisms with the open space axioms and the circuit axioms by dualization (and also via equivalence with the rank axioms).

In [11], various families are defined with respect to a given family of subsets, such as its *upper cone*, *lower cone*, *dual, opposite, max* and *min* families (see Definition 1). In Figure 2, we illustrate the relations between the different axiom systems in the context of these notions. These follow exactly as for subsets, although for the dual of a family, we take the orthogonal complement with respect to an inner product. Another difference to note is that for the left side of the diagram — bases, independence and spanning — four axioms are needed, contrary to the three axioms in the classical case. This difference between the classical case and the q-analogue does not appear for the other axiom systems in the diagram.

This paper is organised as follows. In Section 2 we outline all the different axiomatic systems that we will consider in this work. In Section 3 we present an infinite family of representable q-matroids derived from an $\mathbb{F}_{q^m}$-linear code and explicitly describe its bases, independent spaces, flats, circuits etc. In Section 4 we describe some variations on the independence, hyperplane and rank axiom systems. The remaining sections go through the various pairwise cryptomorphisms in turn. In Section 5 we show that the independence and closure axioms are cryptomorphic. In Sections 6 and 7 we prove cryptomorphisms between the closure function axioms and the independence and rank function axioms, respectively. In Sections 8 and 12 we establish the equivalence of the flat axioms

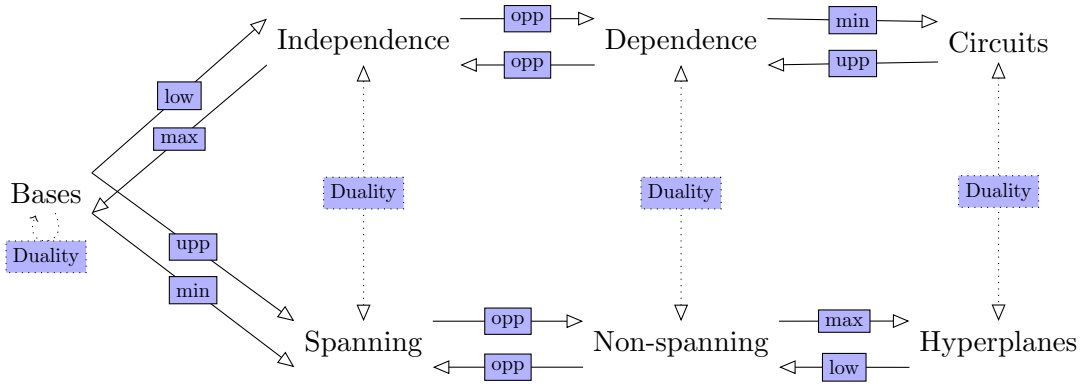


FIGURE 2. Cryptomorphisms with Duality

and the hyperplane and open space axioms respectively. In Sections 9 and 10, the dependence axioms are shown to be cryptomorphic to the independence and the circuit axioms, respectively. In Section 11 we note the cryptomorphism between the hyperplane axioms and circuit axioms and discuss cocircuits of a matroid. Finally, in Section 13, we deduce the spanning and non-spanning space axioms from the other axiom systems. In the appendix we list all relations between the various notions associated to q-matroids.

2. Preliminaries

Throughout this paper, n denotes a fixed positive integer and we denote by E a fixed n-dimensional vector space over an arbitrary field $\mathbb{F}$. We recall that if A is a subspace of E, its codimension in E is given by $\operatorname{codim}(A) = \dim(E) - \dim(A)$. We denote by $\mathcal{L}(E)$ the lattice of subspaces of E, for which the join of a pair of subspaces A and B is defined to be their vector space sum $A + B$ while their meet is defined to be their intersection $A \cap B$. For any $A, B \in \mathcal{L}(E)$ with $A \subseteq B$ we denote by $[A, B]$ the interval between A and B, that is, the lattice of all subspaces X with $A \subseteq X \subseteq B$. For $A \subseteq E$ we use the notation $\mathcal{L}(A)$ to denote the interval $[\{0\}, A]$.

For any subspace $X \in \mathcal{L}(E)$ we denote by $X^\perp$ the orthogonal complement of X in E with respect to the standard dot product:

$$X^\perp := \{y \in E : x \cdot y = 0 \ \forall x \in X\},$$

where $x \cdot y := \sum_{j=1}^{n} x_i y_i$ for any $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in E$.

Definition 1. Let $\mathcal{A} \subseteq \mathcal{L}(E)$. We define the following families of subspaces of E.

$$\begin{aligned}
\operatorname{upp}(\mathcal{A}) &:= \{X \in \mathcal{L}(E) : \exists A \in \mathcal{A}, A \subseteq X\},\\
\operatorname{low}(\mathcal{A}) &:= \{X \in \mathcal{L}(E) : \exists A \in \mathcal{A}, X \subseteq A\},\\
\max(\mathcal{A}) &:= \{X \in \mathcal{A} : X \nsubseteq A \text{ for any } A \in \mathcal{A}, A \neq X\},\\
\min(\mathcal{A}) &:= \{X \in \mathcal{A} : A \nsubseteq X \text{ for any } A \in \mathcal{A}, A \neq X\},\\
\operatorname{opp}(\mathcal{A}) &:= \{X \in \mathcal{L}(E) : X \notin \mathcal{A}\},\\
\mathcal{A}^\perp &:= \{X^\perp : X \in \mathcal{A}\}.
\end{aligned}$$

Definition 2. Let $\mathcal{A}$ be a collection of subspaces of E. For any subspace $X \in \mathcal{L}(E)$, we define the collection of **maximal subspaces of X in $\mathcal{A}$** to be the collection of subspaces

$$\max(X, \mathcal{A}) := \{A \in \mathcal{A} : A \subseteq X \text{ and } B \subset X, B \in \mathcal{A} \implies \dim(B) \leq \dim(A)\}.$$

In other words, $\max(X, \mathcal{A})$ is the set of subspaces of X in $\mathcal{A}$ that have maximal dimension over all such choices of subspaces.

The following defines a q-matroid in terms of a rank function (see [9]).

Definition 3. A q-matroid M is a pair (E, r) where r is an integer-valued function defined on the subspaces of E with the following properties:

(R1) For every subspace $A \in \mathcal{L}(E)$, $0 \leq r(A) \leq \dim A$.
(R2) For all subspaces $A \subseteq B \in \mathcal{L}(E)$, $r(A) \leq r(B)$.
(R3) For all A, B, $r(A+B) + r(A \cap B) \leq r(A) + r(B)$.

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

Definition 4. 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):

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

A subspace that is not an independent space of (E, r) is called a **dependent space** of the q-matroid (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. A **spanning space** of the q-matroid (E, r) is a subspace S such that $r(S) = r(E)$. A **non-spanning space** of the q-matroid (E, r) is a space that is not a spanning space. We write $\mathcal{S}_r$ to denote the set of spanning spaces of (E, r) and we write $\mathcal{N}_r$ to denote its set of non-spanning spaces. 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).

Definition 5. Let (E, r) be a q-matroid. For each $A \in \mathcal{L}(E)$, define $C_r(A) := \{x \in \mathcal{L}(E) : r(A+x) = r(A), \dim(x) = 1\}$. The **closure function** of a q-matroid (E, r) is the function defined by

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

Definition 6. A subspace A of a q-matroid (E, r) is called a **flat** if for all 1-dimensional subspaces $x \in \mathcal{L}(E)$ such that $x \nsubseteq A$ 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

$$\mathcal{F}_r := \{A \in \mathcal{L}(E) : r(A + x) > r(A) \ \ \forall x \in \mathcal{L}(E), x \nsubseteq A, \dim(x) = 1\}.$$

A subspace H is called a **hyperplane** if it is a maximal proper flat, i.e., if $H \neq E$ and the only flat that properly contains H is E. We write $\mathcal{H}_r$ to denote the set of hyperplanes of the q-matroid (E, r), that is

$$\mathcal{H}_r = \{A \in \mathcal{L}(E) : r(A) = r(M) - 1 \text{ and } r(A + x) > r(A) \ \ \forall x \in \mathcal{L}(E), x \nsubseteq A, \dim(x) = 1\}.$$

We now present several axiom systems. Some of these, such as the *independence axioms, flat axioms, circuit axioms* and *closure axioms* have been presented before, while others (namely the axioms of *open spaces* and *dependent spaces*) have not. In later sections we will establish that these are all cryptomorphisms of a q-matroid.

Definition 7. Let $\mathcal{I} \subseteq \mathcal{L}(E)$. We define the following **independence axioms**.

(I1) $\mathcal{I} \neq \varnothing$.
(I2) For all $I, J \in \mathcal{L}(E)$, if $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.
(I3) For all $I, J \in \mathcal{I}$ satisfying $\dim I < \dim J$, there exists a 1-dimensional subspace $x \subseteq J$, $x \nsubseteq I$ such that $I + x \in \mathcal{I}$.
(I4) For all $A, B \in \mathcal{L}(E)$ and $I, J \in \mathcal{L}(E)$ such that $I \in \max(\mathcal{I} \cap \mathcal{L}(A))$ and $J \in \max(\mathcal{I} \cap \mathcal{L}(B))$, there exists $K \in \max(\mathcal{I} \cap \mathcal{L}(A + B))$ such that $K \subseteq I + J$.

If $\mathcal{I}$ satisfies the independence axioms (I1)-(I4) we say that $(E, \mathcal{I})$ is a collection of **independent spaces**.

Definition 8. Let $\mathcal{B} \subseteq \mathcal{L}(E)$. We define the following **basis axioms**.

(B1) $\mathcal{B} \neq \varnothing$
(B2) For all $B_1, B_2 \in \mathcal{B}$, if $B_1 \subseteq B_2$, then $B_1 = B_2$.
(B3) For all $B_1, B_2 \in \mathcal{B}$ and for every subspace A of codimension 1 in B_1 satisfying $B_1 \cap B_2 \subseteq A$, there is a 1-dimensional subspace y of B_2 such that $A + y \in \mathcal{B}$.
(B4) For all $A, B \in \mathcal{L}(E)$, if I and J are maximal intersections of some members of $\mathcal{B}$ with A and B, respectively, there exists a maximal intersection of a basis and $A + B$ that is contained in $I + J$.

If $\mathcal{B}$ satisfies the bases axioms (B1)-(B4) we say that $(E, \mathcal{B})$ is a collection of **bases**.

Definition 9. Let $\mathcal{A} \subseteq \mathcal{L}(E)$. Let $A, B \in \mathcal{A}$. We say that B **covers** A in $\mathcal{A}$ if $A \subseteq B$ and for any $C \in \mathcal{A}$ such that $A \subseteq C \subseteq B$, then either $A = C$ or $B = C$.

Definition 10. Let $\mathcal{F} \subseteq \mathcal{L}(E)$. We define the following **flat axioms**.

(F1) $E \in \mathcal{F}$.
(F2) If $F_1 \in \mathcal{F}$ and $F_2 \in \mathcal{F}$, then $F_1 \cap F_2 \in \mathcal{F}$.
(F3) For all $F \in \mathcal{F}$ and $x \in \mathcal{L}(E)$ a 1-dimensional subspace not contained in F, there is a unique cover of F in $\mathcal{F}$ that contains x.

If $\mathcal{F}$ satisfies the flat axioms (F1)-(F3) we say that $(E, \mathcal{F})$ is a collection of **flats**.

Definition 11. Let $\mathcal{O} \subseteq \mathcal{L}(E)$. We define the following **open space axioms**.

(O1) $\{0\} \in \mathcal{O}$.
(O2) For all $O_1, O_2 \in \mathcal{O}$ it holds that $O_1 + O_2 \in \mathcal{O}$.
(O3) For each $O \in \mathcal{O}$ and each $X \in \mathcal{L}(E)$ such that $O \nsubseteq X$ and $\operatorname{codim}_E(X) = 1$, there exists a unique $O' \subseteq X \cap O$ such that O is a cover of O' in $\mathcal{O}$.

If $\mathcal{O}$ satisfies the open space axioms (O1)-(O3) we say that $(E, \mathcal{O})$ is a collection of **open spaces**.

Definition 12. Let $\mathcal{H} \subseteq \mathcal{L}(E)$. We define the following **hyperplane axioms**.

(H1) $E \notin \mathcal{H}$.
(H2) For all $H_1, H_2 \in \mathcal{H}$, if $H_1 \subseteq H_2$, then $H_1 = H_2$.
(H3) For all distinct $H_1, H_2 \in \mathcal{H}$, for each 1-dimensional space $x \in \mathcal{L}(E)$ there exists $H_3 \in \mathcal{H}$ such that $(H_1 \cap H_2) + x \subseteq H_3$.

If $\mathcal{H}$ satisfies the axioms (H1)-(H3), then we say that $(E, \mathcal{H})$ is a collection of **hyperplanes**.

Definition 13. Let $\mathcal{D} \subseteq \mathcal{L}(E)$. We define the following **dependence axioms**.

(D1) $\{0\} \notin \mathcal{D}$.
(D2) For all $D_1, D_2 \in \mathcal{L}(E)$, if $D_1 \in \mathcal{D}$ and $D_1 \subseteq D_2$, then $D_2 \in \mathcal{D}$.
(D3) For all $D_1, D_2 \in \mathcal{D}$ satisfying $D_1 \cap D_2 \notin \mathcal{D}$, if D is a space of codimension 1 in $D_1 + D_2$, then $D \in \mathcal{D}$.

If $\mathcal{D}$ satisfies the dependence axioms (D1)-(D3) we say that $(E, \mathcal{D})$ is a collection of **dependent spaces**.

Definition 14. Let $\mathcal{C} \subseteq \mathcal{L}(E)$. We define the following **circuit axioms**.

(C1) $\{0\} \notin \mathcal{C}$.
(C2) For all $C_1, C_2 \in \mathcal{C}$, if $C_1 \subseteq C_2$ $C_1 = C_2$.
(C3) For distinct $C_1, C_2 \in \mathcal{C}$ and any $X \in \mathcal{L}(E)$ of codimension 1 there is a circuit $C_3 \subseteq \mathcal{C}$ such that $C_3 \subseteq (C_1 + C_2) \cap X$.

If $\mathcal{C}$ satisfies the circuit axioms (C1)-(C3), we say that $(E, \mathcal{C})$ is a collection of **circuits**.

Note that the axiom (C3) listed here is different from the axiom (C3) as defined in [9, Theorem 64]. We will explain this in Section 11.

Definition 15. Let $\mathrm{cl} : \mathcal{L}(E) \to \mathcal{L}(E)$ be a map. We define the following **closure axioms**.

(Cl1) For every $A \in \mathcal{L}(E)$ it holds that $A \subseteq \mathrm{cl}(A)$.
(Cl2) For all $A, B \in \mathcal{L}(E)$, if $A \subseteq B$, then $\mathrm{cl}(A) \subseteq \mathrm{cl}(B)$.
(Cl3) For every $A \in \mathcal{L}(E)$ it holds that $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$.
(Cl4) For all $x, y, A \in \mathcal{L}(E)$ such that $\dim(x) = \dim(y) = 1$, if $y \subseteq \mathrm{cl}(A + x)$ and $y \nsubseteq \mathrm{cl}(A)$, then $x \subseteq \mathrm{cl}(A + y)$.

If $\mathrm{cl} : \mathcal{L}(E) \to \mathcal{L}(E)$ satisfies the closure axioms (Cl1)-(Cl4) , then we call it a **closure function**. We write (E, cl) to denote a vector space E together with a function cl satisfying the closure axioms.

Definition 16. Let $\mathcal{S} \subseteq \mathcal{L}(E)$. We define the following **spanning space axioms**.

(S1) $E \in \mathcal{S}$.
(S2) For all $I, J \in \mathcal{L}(E)$, if $J \in \mathcal{S}$ and $J \subseteq I$, then $I \in \mathcal{S}$.
(S3) For all $I, J \in \mathcal{S}$ such that $\dim J < \dim I$, there exists some $X \in \mathcal{L}(E)$ of codimension 1 in E satisfying $J \subseteq X$, $I \nsubseteq X$, and $I \cap X \in \mathcal{S}$.
(S4) For all $A, B \in \mathcal{L}(E)$ and $I, J \in \mathcal{L}(E)$ such that $I \in \min(\mathcal{S} \cap [A, E])$ and $J \in \min(\mathcal{S} \cap [B, E])$, there exists $K \in \min(\mathcal{S} \cap [A \cap B, E])$ such that $I \cap J \subseteq K$.

If $\mathcal{S}$ satisfies the independence axioms (S1)-(S4) we say that $(E, \mathcal{S})$ is a collection of **spanning spaces**.

Definition 17. Let $\mathcal{N} \subseteq \mathcal{L}(E)$. We define the following **non-spanning space axioms**.

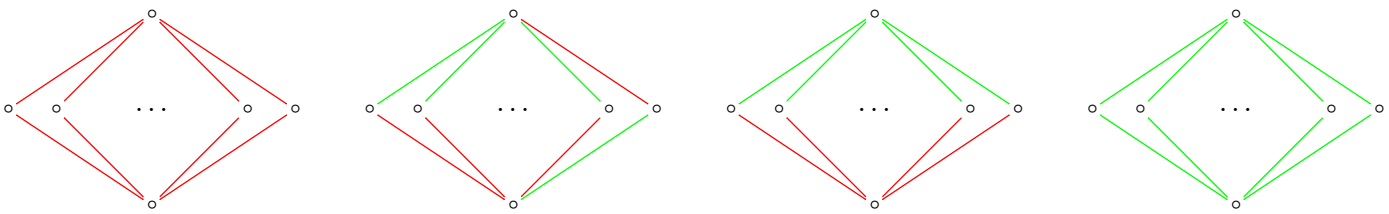
(N1) $E \notin \mathcal{N}$.
(N2) For all $N_1, N_2 \in \mathcal{L}(E)$, if $N_1 \in \mathcal{N}$ and $N_2 \subseteq N_1$, then $N_2 \in \mathcal{N}$.
(N3) For all $N_1, N_2 \in \mathcal{N}$ satisfying $N_1 + N_2 \notin \mathcal{N}$, if N is a space such that $N_1 \cap N_2$ has codimension 1 in N, then $N \in \mathcal{N}$.

If $\mathcal{N}$ satisfies the dependence axioms (N1)-(N3) we say that $(E, \mathcal{N})$ is a collection of **non-spanning spaces**.

Definition 18. Let $\mathcal{L}$ be a lattice. Intervals of length 1 in $\mathcal{L}$ are called **coverings** and intervals of length 2 are called **diamonds**. A **bi-clouring** of $\mathcal{L}$ is a function $\mathcal{L} \longrightarrow \{\mathrm{red}, \mathrm{green}\}$ that associates a colour (red or green) to every covering of $\mathcal{L}$.

Definition 19. A bi-colouring of the lattice $\mathcal{L}(E)$ is called **matroidal** if and only if each diamond is one of four types:

One	All coverings are red.
Mixed	Exactly one lower covering is green, and the covering above it is the only upper red covering.
Prime	All lower coverings are red, all upper coverings are green
Zero	All coverings are green



We conclude this section with the notion of a *dual matroid*, which we will use in Sections 11, 12 and 13.

Definition 20. Let $M = (E, r)$ be a q-matroid. Then $M^* = (E, r^*)$ is also a q-matroid, called the **dual q-matroid**, with rank function

$$r^*(A) = \dim(A) - r(E) + r(A^\perp).$$

We recall the following theorem from [9, Theorem 45].

Theorem 21. *The subspace $B \in \mathcal{L}(E)$ is a basis of the q-matroid M if and only if $B^\perp$ is a basis of the dual q-matroid M^*.*

3. An Infinite Family of Representable q-Matroids

We present a construction of an infinite family of q-matroids. For a specific choice of parameter sets, we will identify its independent and dependent spaces, spanning and non-spanning spaces, its circuits, hyperplanes, open spaces, bases, flats and characterize the rank and closure of each subspace. Before starting, we define what a representable q-matroid is.

Definition 22. Let $M = (E, r)$ be a q-matroid of rank k over a field $\mathbb{F}$. Let $A \subseteq E$ and let Y be a matrix with column space A. We say that M is **representable** over $\mathbb{F}$ if there exists a $k \times n$ matrix G over a finite extension field $\mathbb{L}/\mathbb{F}$ such that $r(A)$ is equal to the matrix rank of GY over $\mathbb{L}$.

We recall now a standard construction of a representable q-matroid over a finite field (see [9]). Let $E = \mathbb{F}_q^n$ and let k, m be positive integers. Let $h : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^k$ be an $\mathbb{F}_{q^m}$-epimorphism. We define the function

$$r : \mathcal{L}(E) \longrightarrow \mathbb{N}_0 : A \mapsto r(A) := \dim_{\mathbb{F}_{q^m}}(h(A)).$$

Then (E, r) is a q-matroid with rank function r; the rank of a subspace A is the dimension of its image under the epimorphism h. We have $r(E) = k$. The epimorphism h can be equivalently represented by a matrix G with respect to some choice of basis for $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_{q^m}^k$, while for each subspace $A \in \mathcal{L}(E)$, we have that $r(A)$ is the $\mathbb{F}_{q^m}$-rank of the matrix product GY for any matrix Y whose columns form a basis of A. We will denote this q-matroid by $M[G]$.

As a preparation for our construction, we describe the following setting. Let $m = ps$ for coprime integers p and s and let α be a primitive element of $\mathbb{F}_{q^m}$. Define $e := \frac{q^m-1}{q^s-1}$, so that α^e has order $q^s - 1$ in $\mathbb{F}_{q^m}^\times$ and in particular is a generator of the subfield $\mathbb{F}_{q^s}$. Consider the $\mathbb{F}_q$-spaces $G_i = \langle \alpha^i, \alpha^{i+e}, \ldots, \alpha^{i+(s-1)e} \rangle \subseteq \mathbb{F}_{q^m}$, defined for $1 \le i \le e$. There exist $f_j \in \mathbb{F}_q$ such that $\sum_{j=0}^{s-1} f_j \alpha^{i+je} = 0$, if and only if α^e is a root of a polynomial of degree at most $s-1$. This is clearly impossible, since α^e is a primitive element of $\mathbb{F}_{q^s}$, and so its minimal polynomial over $\mathbb{F}_q$ has degree s. It follows that G_i has $\mathbb{F}_q$-dimension equal to s. Moreover, the spaces G_i have trivial intersection. Indeed, for $1 \le i, j \le e$, there exist $f_k, g_k \in \mathbb{F}_q$ satisfying $\sum_{k=0}^{s-1} f_k \alpha^{i+ek} = \sum_{k=0}^{s-1} g_k \alpha^{j+ek}$ if and only if $\alpha^{i-j} = \dfrac{g(\alpha^e)}{f(\alpha^e)}$ for some polynomials $f(x), g(x) \in \mathbb{F}_q[x]$. This holds only if $\alpha^{i-j} \in \mathbb{F}_{q^s}$, which holds if and only if $(i-j)(q^s-1) \equiv 0 \mod q^m - 1$, in which case we must have $i = j$. Therefore, the collection of spaces $\mathcal{G} := \{G_i : 1 \le i \le e\}$ form a spread in $\mathbb{F}_{q^m}$. In fact $\mathcal{G}$ is a *Desarguesian spread* and this construction is well-known [12]. We will use $\mathcal{G}$ to characterise the ranks of spaces associated with an infinite family of representable q-matroids. Before we characterise this family, we will consider a particular example.

Example 23. Let $s \in \mathbb{N}$ be an odd integer and let $m = 2s$. Let $\alpha \in \mathbb{F}_{q^m}$ a primitive element. Take as a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ the elements $1, \alpha, \alpha^2, \ldots, \alpha^{2s-1}$ and consider the matrix

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{2s-1} \\ 1 & \alpha^{q^s} & (\alpha^{q^s})^2 & \ldots & (\alpha^{q^s})^{2s-1} \end{bmatrix}.$$

As outlined above, G determines a q-matroid $(\mathbb{F}_q^n, r)$, which clearly supports only the possible ranks $0, 1, 2$, as G itself has rank 2, so in particular, $r(\mathbb{F}_{q^m}^n) = 2$. As G has no all-zero columns, every 1-dimensional space of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ has rank 1. Let $e = \frac{q^m-1}{q^s-1} = q^s+1$. The collection of s-dimensional subspaces $G_i = \langle \alpha^i, \alpha^{e+i}, \ldots, \alpha^{(s-1)e+i} \rangle_{\mathbb{F}_q}$, for $1 \leq i \leq e$ form a spread of $\mathbb{F}_{q^m}$ as a vector space over $\mathbb{F}_q$. As will be shown in Theorem 25, $r(G_i) = 1$ for each i, while every other s-dimensional space has rank 2. Let us specify our example in a very small case. For $m = 6, q = 2$ we get a q-matroid M_6 with ground space $\mathbb{F}_{2^6}$ over $\mathbb{F}_2$. The spread $\mathcal{G}$ is a collection of $e = 2^3 + 1 = 9$ spaces of $\mathbb{F}_2$-dimension 3 and rank 1, which we denote by $G_1, \ldots, G_9$. We list these as the following binary vector spaces.

$$\begin{aligned}
G_1 &= \langle (0,1,0,0,0,0), (0,0,0,0,1,1), (0,1,1,1,1,0) \rangle_{\mathbb{F}_2}, \\
G_2 &= \langle (0,0,1,0,0,0), (1,1,0,0,0,1), (0,0,1,1,1,1) \rangle_{\mathbb{F}_2}, \\
G_3 &= \langle (0,0,0,1,0,0), (1,0,1,0,0,0), (1,1,0,1,1,1) \rangle_{\mathbb{F}_2}, \\
G_4 &= \langle (0,0,0,0,1,0), (0,1,0,1,0,0), (1,0,1,0,1,1) \rangle_{\mathbb{F}_2}, \\
G_5 &= \langle (0,0,0,0,0,1), (0,0,1,0,1,0), (1,0,0,1,0,1) \rangle_{\mathbb{F}_2}, \\
G_6 &= \langle (1,1,0,0,0,0), (0,0,0,1,0,1), (1,0,0,0,1,0) \rangle_{\mathbb{F}_2}, \\
G_7 &= \langle (0,1,1,0,0,0), (1,1,0,0,1,0), (0,1,0,0,0,1) \rangle_{\mathbb{F}_2}, \\
G_8 &= \langle (0,0,1,1,0,0), (0,1,1,0,0,1), (1,1,1,0,0,0) \rangle_{\mathbb{F}_2}, \\
G_9 &= \langle (0,0,0,1,1,0), (1,1,1,1,0,0), (0,1,1,1,0,0) \rangle_{\mathbb{F}_2}.
\end{aligned}$$

Each space G_i contains 7 distinct 2-dimensional spaces and no space is contained in two spread elements, so in total we have 63 2-dimensional spaces contained some G_i, which we denote by $D_1, \ldots, D_{63}$. Clearly $r(D_i) = 1$ for each $i \in \{1, \ldots, 63\}$.

In Table 1, we tabulate how the subspaces of each dimension in $\mathbb{F}_2^6$ are distributed, according to the different cryptomorphic definitions of a q-matroid. The closure function, independent spaces, circuits etc are all defined with respect to the given rank function.

As can be seen in Table 1, every space of dimension at most 1 has rank equal to its dimension, and so is independent. The zero space is also a flat, being equal to its closure, and is also a non-spanning space. The closure of a one dimensional space is exactly one space from among the $G_1, \ldots, G_9$, namely the specific spread element G_i that contains it.

As regards the spaces of dimension 2, they all have rank 2 and are independent, bases and spanning spaces, except for the 63 subspaces of the spread, $D_1, \ldots, D_{63}$, which are circuits and so are dependent, non-spanning, and open spaces.

Every 3-dimensional space is dependent, having dimension exceeding its rank. In particular, as noted before, each G_i has rank 1, while the remaining 3-spaces have rank 2. Among the 1395 spaces of dimension 3, 1332 are circuits except those 63 spaces that contain some D_i as a subspace. All spaces apart from $G_1, \ldots, G_9$ are spanning spaces. The spaces $G_1, \ldots, G_9$ are flats, non-spanning and are also the only hyperplanes of M_6. Any open space of dimension 3, being a sum of circuits, is either a circuit of dimension 3 or has the form $D_i + D_j$, which must therefore be a spread element since any two D_i, D_j are either contained in the same spread element, or have trivial intersection.

The 4- and 5-dimensional spaces are all dependent of rank 2 and there are no circuits nor flats among them. They are all spanning spaces. The 4-dimensional open spaces are the sum of open

dim / crypt	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Rank	0	1	2 except $r(D_1) = \cdots = r(D_{63}) = 1$	2 except $r(G_1) = \cdots = r(G_9) = 1$	2	2	2
Closure of a Space	0	$\mathrm{cl}(x) = G_i$ for $x \subseteq G_i$	$\mathrm{cl}(T) = \begin{cases} G_i & \text{if } T \subseteq G_i \\ E & \text{else} \end{cases}$	$\mathrm{cl}(T) = \begin{cases} G_i & \text{if } T = G_i \\ E & \text{else} \end{cases}$	E	E	E
Independent Spaces	yes	all	all except $D_1, \ldots, D_{63}$	none	none	none	no
Bases	no	none	all except $D_1, \ldots, D_{63}$	none	none	none	no
Spanning Spaces	no	none	all except $D_1, \ldots, D_{63}$	all except $G_1, \ldots, G_9$	all	all	yes
Circuits	no	none	$D_1, \ldots, D_{63}$	T such that $D_i \nsubseteq T$	none	none	no
Dependent Spaces	no	none	$D_1, \ldots, D_{63}$	all	all	all	yes
Non-spanning Spaces	yes	all	$D_1, ..., D_{63}$	$G_1, ..., G_9$	none	none	no
Flats	yes	none	none	$G_1, \ldots, G_9$	none	none	yes
Open Spaces	yes	none	$D_1, \ldots, D_{63}$	$G_1, \ldots, G_9$ and T such that $D_i \nsubseteq T$	all	all	yes
Hyperplanes	no	none	none	$G_1, \ldots, G_9$	none	none	no

TABLE 1. Defining Spaces of the q-Matroid.

spaces of dimension 2 and 3. Each one contains some D_i since every 4-space intersects some spread element in dimension at least 2, so all 4-dimensional sets are open. The 5-dimensional spaces are also all open, because they are sums of open spaces of dimension 2 and 3. Finally, the whole ground space is a dependent space of rank 2 and is not a circuit, but is a flat, a spanning space and an open space.

We will now illustrate the multiple axiom systems for this example. Some axioms are straightforward to check directly for all possibilities, but we do not go through all the details. In other cases we pick some of the more illuminating examples.

Rank: (R1) and (R2) clearly hold. Let us see an example for (R3), using G_1 and G_2. We know that $G_1 + G_2 = E$ and $G_1 \cap G_2 = \{0\}$. Therefore, $r(G_1+G_2)+r(G_1\cap G_2) = 2+0 = 2 \leq r(G_1)+r(G_2) = 1+1 = 2$.

Closure: That axioms (Cl1)-(Cl3) hold is immediate, as we can see from the table shown in Table 1. We'll show that (Cl4) holds. Let A, x, y be subspaces of $\mathbb{F}_2^6$ such that $\dim(x) = \dim(y) = 1$. Suppose that $y \subseteq \mathrm{cl}(x + A)$ and that $y \nsubseteq \mathrm{cl}(A)$. As observed in Table 1, for any subspace T we have $\mathrm{cl}(T) = E$ unless T is contained in a spread element G, in which case we have $\mathrm{cl}(T) = G$. Therefore, since $y \nsubseteq \mathrm{cl}(A)$, y and A are not both contained in the same spread element and hence $\mathrm{cl}(y + A) = E$. It follows that $x \subseteq \mathrm{cl}(y + A)$.

Independence: It is clear from Table 1 that (I1) and (I2) hold. We'll show that (I3) holds. All the independent spaces determined by the rank function of M_6 have dimension at most 2, so we need only consider some 1-dimensional subspace I and a two-dimensional space J, different from

$D_1, \ldots, D_{63}$. Since $J \neq D_i$ for any i, it is not contained in any spread element. In particular, $J \nsubseteq G$ where G is the unique spread element containing I. Therefore, there exists a 1-dimensional space $x \subseteq J$, $x \nsubseteq G$ and $x + I$ is a 2-dimensional space not contained in G, which is therefore independent.

Consider now (I4). Let A, B be subspaces of $\mathbb{F}_2^6$ and let I, J be maximal independent subspaces of A and B, respectively. Then $r(A) = \dim(I)$ and $r(B) = \dim(J)$. Any independent subspace of $A + B$ has dimension at most 2. If $\dim(I) = \dim(J) = 1$, then $r(A) = r(B) = 1$, so from Table 1, A and B are each contained in some spread element.

We have $\dim(I + J) = 2$ and further, $I + J$ is independent if and only if $I + J \neq D_\ell$ for any ℓ. If A and B are contained in distinct spread elements, then $I + J \neq D_\ell$ for any ℓ and so $I + J$ gives the required maximal independent subspace of $A + B$. If $A, B \subseteq G$ for a spread element G, then $r(A + B) = 1$ and both I and J are maximal independent subspaces of $A + B$. If $\dim(I) = 2$, then I is a maximal independent subspace of $A + B$. This proves that (I4) holds for the independent spaces of the q-matroid M_6.

Bases: That (B1) and (B2) hold is easy to see. Let $B_1 \neq B_2$ be a pair of distinct bases of the q-matroid M_6. Then the B_i are 2-dimensional spaces different from $D_1, \ldots, D_{63}$. Let $I = B_1 \cap B_2$. If $\dim(I) = 1$, then I is the only space of codimension-1 in B_1 that contains I, so set $A = I$. Otherwise, let A be any 1-dimensional space in B_1. In order to find a basis and see that (B3) holds, it is enough to add any 1-dimensional space not contained in the same spread element as A.

We illustrate an instance of (B4). Let $A = \langle (1,0,0,1,0,0) \rangle$ and let $B = \langle (1,0,0,1,0,0), (1,0,0,0,0,1), (1,0,0,0,0,0) \rangle$. The maximal intersection of A with a basis is $I = A$, while the maximal intersection of B with a basis is $J = \langle (1,0,0,1,0,0), (1,0,0,0,0,1) \rangle$ (J is a basis since it is a space of dimension 2 not contained in a spread element). Then $I + J = J$, which gives the required maximal intersection of a basis with $A + B = I + B = B$.

Circuits: The axioms (C1) and (C2) are trivially satisfied. We'll show an example of the axiom (C3). Let $C_1 = \langle (0,0,0,0,0,1), (0,0,1,0,1,0) \rangle$ and $C_2 = \langle (0,0,0,0,0,1), (1,0,0,1,0,0) \rangle$. Let $H = \langle (0,0,0,0,0,1) \rangle^\perp$. Then $(C_1 + C_2) \cap H$ contains the circuit, $C_3 = \langle (0,0,1,0,1,0), (1,0,0,1,0,0) \rangle$, as required.

Dependence: (D1) and (D2) hold trivially. To illustrate (D3), take for example, two dependent spaces D_i, D_j, $1 \leq i, j \leq 63$. Being circuits, their intersection is independent. If D_i, D_j come from the same spread element G_l, then their sum is G_l itself and any codimension-1 space in such a sum is dependent. If they come from two different spread elements G_l, G_m, their intersection is $\{0\}$, which is independent. Their sum has dimension 4 and hence any subspace of codimension 1 in $D_i + D_j$ is dependent.

Flats: From Table 1, E is a flat (so (F1) holds), $\{0\}$ is a flat and $G_1, \ldots, G_9$ are flats. This shows (F2) directly: the intersection of a flat F with E is F itself, the intersection with $\{0\}$ or between two spread elements is $\{0\}$. As regards (F3), if $F = \{0\}$ and we take a 1-dimensional space x, the unique cover of $F + x = x$ is the unique spread element containing x. If we choose F from among the spread elements $G_1, \ldots, G_9$ and pick any 1-dimensional space $x \nsubseteq F$ the cover of $x + F$ is E.

Hyperplanes: Since the only hyperplanes of the q-matroid M_6 are the spread elements $G_1, \ldots, G_9$, which are pairwise disjoint, axioms (H1) and (H2) hold vacuously. For any 1-dimensional space x and any i, j we have $(G_i \cap G_j) + x = x$, which is contained in some spread element G_ℓ.

Open Spaces: It is easy to see that (O1) and (O2) hold. As regards (O3), consider an open space O of dimension 3. Let $X \subseteq E$ of codimension 1. If $O = G_i$, then $O \cap X = D_j$, which is an open space covered by O. Otherwise, O does not contain any D_i, hence $O \cap X$ also does not. In that case we have that $\{0\} \subseteq O \cap X$ and O covers $\{0\}$.

Spanning Spaces: (S1) and (S2) are easy to verify by looking at Table 1. Let us look at (S3). We verify it in the case $J = \langle (0,1,0,0,0,0), (0,0,1,0,0,0) \rangle$ and $I = J + \langle (0,0,0,1,0,0) \rangle$. It is enough to take, as an example, $X = J + \langle (0,0,0,0,1,0), (0,0,0,0,0,1), (0,1,1,1,0,0) \rangle$. Of course $J \subseteq X$ and

$I \not\subseteq X$. Since $X \cap I = J$ we actually have a spanning space, as required by (S3). A very easy example for (S4) is given by taking $A = \langle(0,1,0,0,0,0)\rangle$, $B = \langle(0,0,1,0,0,0)\rangle$, which are both contained in $J = \langle(0,1,0,0,0,0),(0,0,1,0,0,0)\rangle$, their minimal containing spanning space. Their intersection is $\{0\}$ and the required minimal space is J itself.

Non-spanning Spaces: (N1), (N2) are easily read from the table. For (N3), we have that the only way for two non-spanning spaces N_1, N_2 to have $N_1 + N_2 \notin \mathcal{N}$ is if N_1 and N_2 are in different spread elements. So $N_1 \cap N_2 = \{0\}$ and N is a 1-dimensional space, which is a non-spanning space. ◊

We now continue with the characterization of our infinite family of representable q-matroids. First we require a well-known lemma [10, Lemma 3.51].

Lemma 24. *Let $\alpha_1, ..., \alpha_\ell \in \mathbb{F}_{q^m}$. We have:*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_\ell \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_\ell^q \\ \vdots & \cdots & \vdots & \vdots \\ \alpha_1^{q^{(\ell-1)}} & \alpha_2^{q^{(\ell-1)}} & \cdots & \alpha_\ell^{q^{(\ell-1)}} \end{vmatrix} = \alpha_1 \prod_{j=1}^{\ell-1} \prod_{c_1,\ldots,c_j \in \mathbb{F}_q} \left(\alpha_{j+1} - \sum_{k=1}^{j} c_k \alpha_k \right).$$

In particular, this determinant is nonzero if and only if $\alpha_1, \ldots, \alpha_\ell$ are linearly independent over $\mathbb{F}_q$.

We now describe the q-matroid $M[G] = (E, r)$ with rank function defined by $r(A) = \text{rank}(GY)$ for any matrix Y with column space equal to A.

Theorem 25. *Let p, s be a pair of coprime positive integers and let $m = ps$. Let $E = \mathbb{F}_{q^m}$ and let*

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{m-1} \\ 1 & \alpha^{q^s} & \alpha^{2q^s} & \cdots & \alpha^{(m-1)q^s} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{q^{(p-1)s}} & \alpha^{2q^{(p-1)s}} & \cdots & \alpha^{(m-1)q^{(p-1)s}} \end{pmatrix}.$$

Let $e := (q^m - 1)/(q^s - 1)$ and for each $i \in \{1, \ldots, e\}$, let $G_i := \langle \alpha^i, \alpha^{e+i}, \ldots, \alpha^{(s-1)e+i} \rangle_{\mathbb{F}_q}$. Let (E, r) be the q-matroid $M[G]$. Let A be a subspace of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let B be a basis of A over $\mathbb{F}_q$, and let $\mathcal{S} := \{j \in \{1, \ldots, e\} : B \cap G_j \neq \varnothing\}$. Let $\mu := \dim_{\mathbb{F}_{q^s}}(\langle \alpha^\ell : \ell \in \mathcal{S} \rangle)$. Then $r(A) = \min(p, \mu)$.

Proof. For each element $\theta \in \mathbb{F}_{q^m}$, we write $\Gamma(\theta)$ to denote the expression of θ as a vector of length m in $\mathbb{F}_q$ with respect to the basis $\{1, \alpha, \ldots, \alpha^{m-1}\}$. We also define $\Gamma(S) := \{\Gamma(s) : s \in S\}$ for any $S \subseteq \mathbb{F}_{q^m}$. Let $f(x) = \sum_{k=0}^{m-1} f_i x^i \in \mathbb{F}_q[x]$. Then $f(\alpha^t) = (1, \alpha^t, \ldots, \alpha^{t(m-1)}) \cdot (f_0, \ldots, f_{m-1})$ for any integer t. In particular, for the vector $f \in \mathbb{F}_q^m$, $(Gf)_j = f(\alpha^{q^{(j-1)s}})$ for $1 \leq j \leq p$. Now consider the space $G_i = \langle \alpha^i, \alpha^{i+e}, \ldots, \alpha^{i+(s-1)e} \rangle \subseteq \mathbb{F}_{q^m}$. Let Y be the $m \times s$ matrix whose j-th column is $\Gamma(\alpha^{i+(j-1)e})$. Then, using the fact that $(\alpha^e)^{q^s} = \alpha^e$, we have

$$\begin{aligned} GY &= \begin{pmatrix} \alpha^i & \alpha^{i+e} & \cdots & \alpha^{i+(s-1)e} \\ \alpha^{iq^s} & \alpha^{(i+e)q^s} & \cdots & \alpha^{(i+(s-1)e)q^s} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^{iq^{(p-1)s}} & \alpha^{(i+e)q^{(p-1)s}} & \cdots & \alpha^{(i+(s-1)e)q^{(p-1)s}} \end{pmatrix} = \begin{pmatrix} \alpha^i & \alpha^{i+e} & \cdots & \alpha^{i+(s-1)e} \\ \alpha^{iq^s} & \alpha^{iq^s+e} & \cdots & \alpha^{iq^s+(s-1)e} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^{iq^{(p-1)s}} & \alpha^{iq^{(p-1)s}+e} & \cdots & \alpha^{iq^{(p-1)s}+(s-1)e} \end{pmatrix} \\ &= \begin{pmatrix} \alpha^i & \alpha^i & \cdots & \alpha^i \\ \alpha^{iq^s} & \alpha^{iq^s} & \cdots & \alpha^{iq^s} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^{iq^{(p-1)s}} & \alpha^{iq^{(p-1)s}} & \cdots & \alpha^{iq^{(p-1)s}} \end{pmatrix} \text{diag}(1, \alpha^e, \alpha^{2e}, \ldots, \alpha^{(s-1)e}), \end{aligned}$$

which clearly has rank 1 over $\mathbb{F}_{q^m}$. Let V be an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension ℓ and let B be a basis of V over $\mathbb{F}_q$. Each element of B is contained in exactly one spread element $G_i \in$

$\mathcal{G}$. Write $B = B_{i_1} \cup \cdots \cup B_{i_t}$, where $B_{i_k} \subset G_{i_k}$ and the G_{i_k} are distinct. In particular, we have $\mathcal{S} = \{i_1, \ldots, i_t\}$. Each element of B_{i_k} has the form $\sum_{p=0}^{s-1} f_p \alpha^{i_k+pe} = \alpha^{i_k} f(\alpha^e)$ for some $f(x) \in \mathbb{F}_q[x]$. Let $B_{i_k} = \{\alpha^{i_k} f^{k,1}(\alpha^e), \ldots, \alpha^{i_k} f^{k,\ell_k}(\alpha^e)\}$ for some $f^{k,j}(x) \in \mathbb{F}_q[x]$ where B_{i_k} has order ℓ_k. Let $Y_k = [\Gamma(\alpha^{i_k} f^{k,1}(\alpha^e)), \ldots, \Gamma(\alpha^{i_k} f^{k,t_k}(\alpha^e))]$, for each k. Then

$$(GY_k)_{j,h} = \alpha^{i_k q^{(j-1)s}} f^{k,h}(\alpha^{eq^{(j-1)s}}) = \alpha^{i_k q^{(j-1)s}} f^{k,h}(\alpha^e).$$

Now let Y be the $m \times \ell$ matrix in $\mathbb{F}_q$ defined by $Y = [Y_1|\cdots|Y_t]$, so that $GY = [GY_1|\cdots|GY_t]$. We have

$$GY = \left(\begin{array}{ccc|c|ccc} \alpha^{i_1} f^{1,1}(\alpha^e) & \cdots & \alpha^{i_1} f^{1,t_1}(\alpha^e) & \cdots & \alpha^{i_t} f^{t,1}(\alpha^e) & \cdots & \alpha^{i_t} f^{1,\ell_1}(\alpha^e) \\ \alpha^{i_1 q^s} f^{1,1}(\alpha^e) & \cdots & \alpha^{i_1 q^s} f^{1,t_1}(\alpha^e) & \cdots & \alpha^{i_k q^s} f^{t,1}(\alpha^e) & \cdots & \alpha^{i_k q^s} f^{t,\ell_t}(\alpha^e) \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ \alpha^{i_1 q^{(p-1)s}} f^{1,1}(\alpha^e) & \cdots & \alpha^{i_1 q^{(p-1)s}} f^{1,t_1}(\alpha^e) & \cdots & \alpha^{i_k q^{(p-1)s}} f^{t,1}(\alpha^e) & \cdots & \alpha^{i_t q^{(p-1)s}} f^{t,\ell_t}(\alpha^e) \end{array}\right)$$

Since $f^{k,h}(\alpha^e) \neq 0$ for all k, h, GY is column equivalent to the matrix:

$$\left(\begin{array}{cccc|cccc|c|cccc} \alpha^{i_1} & 0 & \cdots & 0 & \alpha^{i_2} & 0 & \cdots & 0 & \cdots & \alpha^{i_t} & 0 & \cdots & 0 \\ \alpha^{i_1 q^s} & 0 & \cdots & 0 & \alpha^{i_2 q^s} & 0 & \cdots & 0 & \cdots & \alpha^{i_t q^s} & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ \alpha^{i_1 q^{s(p-1)}} & 0 & \cdots & 0 & \alpha^{i_2 q^{s(q-1)}} & 0 & \cdots & 0 & \cdots & \alpha^{i_t q^{s(q-1)}} & 0 & \cdots & 0 \end{array}\right).$$

Now let $S = \{s_1, \ldots, s_\mu\} \subseteq \mathcal{S}$ such that $\{\alpha^{s_1}, \ldots, \alpha^{s_\mu}\}$ is a basis of $\langle \alpha^\ell : \ell \in \mathcal{S} \rangle_{\mathbb{F}_{q^s}}$. Then by Lemma 24,

$$\left|\begin{array}{cccc} \alpha^{s_1} & \alpha^{s_2} & \cdots & \alpha^{s_\ell} \\ \alpha^{s_1 q^s} & \alpha^{s_2 q^s} & \cdots & \alpha^{s_\ell q^s} \\ \vdots & \cdots & \vdots & \vdots \\ \alpha^{s_1 q^{s(\ell-1)}} & \alpha^{s_2 q^{s(\ell-1)}} & \cdots & \alpha^{s_\ell q^{s(\ell-1)}} \end{array}\right| \neq 0,$$

where $\ell = \min(p, \mu)$. The result now follows. □

4. Equivalent Axiom Systems

In a number of cases a particular axiom system may have more than one equivalent set of axioms. This is certainly the case for the rank axioms, the hyperplane axioms and the independence axioms. Identifying these equivalences can be convenient for various proofs. Alternative axiom systems for the independent spaces and the bases were already given in [9, Propositions 16 and 40].

4.1. **Independent spaces.** We start with equivalent formulations of the independence axioms: we will show that (I4) can be replaced by either of the following alternative axioms.

- (I4') Let $A \in \mathcal{L}(E)$ and let $I \in \max(A, \mathcal{I})$. Let $B \in \mathcal{L}(E)$. Then there exists $J \in \max(A + B, \mathcal{I})$ such that in $J \subseteq I + B$.
- (I4") Let $A \in \mathcal{L}(E)$ and let $I \in \max(A, \mathcal{I})$. Let $x \in \mathcal{L}(E)$ be a 1-dimensional space. Then there exists $J \in \max(x + A, \mathcal{I})$ such that in $J \subseteq x + I$.

These statements are Propositions 14 and 13 of [9], respectively. The proofs in that paper assume the rank axioms, while here we will only use the independence axioms.

Theorem 26. *Let $\mathcal{I}$ be a collection of subspaces satisfying (I1)-(I3). Then the axiom systems (I1)-(I4), (I1)-(I4') and (I1)-(I4") are pairwise equivalent.*

Proof. Note first that by (I3), if $A \in \mathcal{L}(E)$ and $I, J \in \max(\mathcal{L}(A) \cap \mathcal{I})$, then $\dim(I) = \dim(J)$. Therefore, $\max(\mathcal{L}(U) \cap \mathcal{I}) = \max(U, \mathcal{I})$ for all $U \in \mathcal{L}(E)$. It is thus clear that (I4) implies (I4'), which implies (I4"). Suppose that (I4") holds. We will show that (I4') holds. Let $A, B \in \mathcal{L}(E)$ and let $I \in \max(A, \mathcal{I})$. Suppose that (I4') holds for all subspaces of dimension less than $\dim(B)$.

Let C be a subspace of B of codimension 1 in B and write $B = x + C$. By hypothesis, there exists $J \in \max(A+C, \mathcal{I})$ such that $J \subseteq I + C$. By (I4") there exists $J' \in \max(A+C+x, \mathcal{I}) = \max(A+B, \mathcal{I})$ such that $J' \subseteq J + x \subseteq I + C + x = I + B$.

Now suppose that (I4') holds. Let $A, B \in \mathcal{L}(E)$, let $I \in \max(A, \mathcal{I})$ and let $J \in \max(B, \mathcal{I})$. We claim there is member of $\max(A + B, \mathcal{I})$ that is contained in $I + J$. Since $J \in \max(B, \mathcal{I})$, by (I4') these exists $N \in \max(I + B, \mathcal{I})$ such that $N \subseteq I + J$. Again by (I4'), there exists $M \in \max(A + B, \mathcal{I})$ such that $M \subseteq I + B$. But $M \in \max(I + B, \mathcal{I})$, and hence M and N have the same dimension. It follows that N is the required maximal subspace of $A + B$ that is contained in $I + J$ and so (I4') implies (I4). The result follows. □

We will use (I4") to establish a cryptomorphism between the independence axioms and the closure axioms in Section 5.

The next lemma can be established by repeated applications of (I3). Its proof shows in particular that if I, J are subspaces of a collection $\mathcal{I} \subseteq \mathcal{L}(E)$ that satisfies the first 3 independence axioms, then if $\dim(J) > \dim(I)$ there exists a subspace $U \subseteq J$ such that $I + U \in \mathcal{I}$, $U \cap I = \{0\}$. This yields an axiom that is equivalent to (I3).

Lemma 27. *Let $\mathcal{I}$ be a collection of spaces satisfying (I1)-(I3). Let $I \subseteq A \in \mathcal{L}(E)$ and let $I \in \mathcal{I}$. Then there exists a subspace M in $\mathcal{I}$ of maximal dimension in A, such that $I \subseteq M$.*

Proof. By (I1), $\max(A, \mathcal{I})$ is non-empty. Let $J \in \max(A, \mathcal{I})$. If $\dim(I) = \dim(J)$, then I itself is the required maximal subspace of A in $\mathcal{I}$, so suppose that $\dim(I) < \dim(J)$. Then by (I3), there exists $x \subseteq J, x \nsubseteq I$ such that $x + I \in \mathcal{I}$. If $\dim(x + I) = \dim(J)$, then $x + I$ is the required maximal subspace of A in $\mathcal{I}$ that contains I. Otherwise, iterative applications of (I3) yields a maximal subspace $M = I + U \in \mathcal{I}$ of A, with $U \subseteq J$ and $I \cap U = \{0\}$. □

We mention another result that doesn't introduce new equivalent independence axioms, but will arise later in Sections 5 and 9, when we establish cryptomorphisms between the independence and closure axioms and also between the independence and dependence axioms.

Lemma 28. *Let $\mathcal{I}$ be a collection of subspaces satisfying (I1)-(I3). Let A be a subspace of E and let $x \in \mathcal{L}(E), x \nsubseteq A$ be a 1-dimensional space. Let $I \in \max(A, \mathcal{I})$ and let $M \in \max(x + A, \mathcal{I})$. Then $\dim(M) \leq \dim(I) + 1$.*

Proof. Clearly, $\dim(I) \leq \dim(M)$. If $\dim(I) = \dim(M)$, then there's nothing to prove, so suppose that $\dim(I) < \dim(M)$. By Lemma 27, we may assume that $I \subseteq M$. Let m be a 1-dimensional space such that $m \subseteq M, m \nsubseteq I$. By (I2), $m + I \in \mathcal{I}$. By the maximality of I in A, we must have $m \nsubseteq A$ and so $A \subsetneq m + A \subseteq x + A$. Therefore, $m + A = x + A$.

We claim that $m + I = M$. Suppose otherwise and let m' be a 1-dimensional subspace of M that is not contained in $m + I$. Again by (I2), $m + m' + I \in \mathcal{I}$ and by the maximality of I in A we have $m' + m \nsubseteq A$. Then $A \subsetneq m' + m + A \subseteq x + A$, so $m' + m + A = x + A = m + A$ and hence $m' \subseteq m + A$. Therefore, $m' = \langle \bar{m} + \bar{a} \rangle$ for some $\bar{m} \in m$ and $\bar{a} \in A$. If $\bar{m} = 0$, then we get the contradiction $m' \subseteq A$. If $\bar{a} = 0$, then we arrive at the contradiction $m' = m$. Therefore, $m + m' + I = m + a + I$ for some 1-dimensional subspace $a \subseteq A, a \nsubseteq I$, which by (I2) means that $a + I \in \mathcal{I}$, with contradicts $I \in \max(A, \mathcal{I})$. It follows that $M = m + I$ and that $\dim(M) = \dim(I) + 1$. □

4.2. **Rank function.** The following theorem gives an alternative set of axioms for the rank function. This will be used in Section 7 to show the cryptomorphism between the rank and closure functions. Throughout this section, let r be an integer-valued function defined on the subspaces of E. We have the following axioms.

(R1') $r(\{0\}) = 0$.
(R2') $r(A) \leq r(A + x) \leq r(A) + 1$.

(R3') If $r(A) = r(A+x) = r(A+y)$, then $r(A+x+y) = r(A)$.

These axioms are sometimes called *local* rank axioms, which explains why we will use a lot of mathematical induction to get to the *global* versions.

Before proving the equivalence between these axioms and the axioms of the rank function of a q-matroid, we state and prove some preliminary results. The first lemma is Proposition 6 from [9]. However, the proof in that paper assumes r satisfies (R1), (R2), (R3). Here, we want to use the lemma to prove these axioms, so we re-do the proof of the lemma using (R1'), (R2'), (R3') instead.

Lemma 29. *Let r be an integer-valued function defined on the subspaces of E satisfying (R1'), (R2'), (R3'). Let $A, B \in \mathcal{L}(E)$. If $r(A+x) = r(A)$ for all 1-dimensional spaces $x \subseteq B$, then $r(A) = r(A+B)$.*

Proof. We prove this by induction on $k = \dim B - \dim(A \cap B)$. For $k = 0, 1, 2$ we have 1-dimensional spaces $x, y \subseteq B$ such that $A + x + y = A + B$ (the sum does not need to be direct). Suppose $r(A+x) = r(A)$ for all 1-dimensional spaces $x \subseteq B$, so in particular, $r(A) = r(A+x) = r(A+y)$. By (R3'), this means $r(A) = r(A+x+y) = r(A+B)$. Now assume the lemma holds for all A, B with $\dim B - \dim(A \cap B) < k$. Suppose $r(A+x) = r(A)$ for all 1-dimensional spaces $x \subseteq B$. Let $B' \subseteq B$ of codimension 2 and let $x, y \subseteq B$ 1-dimensional subspaces such that $A + B = A + B' + x + y$. Apply the induction hypothesis to A and B': this gives $r(A+B') = r(A)$. Apply the induction hypothesis also to A and $B' + x$ and to A and $B' + y$, this gives $r(A) = r(A+B'+x) = r(A+B'+y)$. Now we can use (R3') on x, y and $A + B'$, giving

$$r(A) = r(A+B') = r(A+B'+x) = r(A+B'+y) = r(A+B'+x+y) = r(A+B).$$

This proves the induction step, and thus the lemma. □

The next Lemma is the q-analogue of Lemma 2.47 of [7].

Lemma 30. *Let r be an integer-valued function defined on the subspaces of E satisfying (R1'), (R2'), (R3'). Let $A, B \in \mathcal{L}(E)$. If $A \subseteq B$, then for all 1-dimensional subspaces $x \in \mathcal{L}(E)$ we have that $r(A+x) - r(A) \geq r(B+x) - r(B)$.*

Proof. We will prove this statement for $\dim B = \dim A + 1$, and the general statement then follows by induction. Let $B = A + y$. From (R2') we know that both sides of the inequality are either 0 or 1. If the left hand side is 1, the inequality is always true, so assume $r(A+x) = r(A)$. We will show that $r(A+y+x) - r(A+y) = 0$. By (R2'), $r(A+y)$ is equal to either $r(A)$ or $r(A)+1$. If $r(A) = r(A+y)$, then by (R3') $r(A) = r(A+y+x)$ so in particular, $r(A+y+x) - r(A+y) = 0$. If $r(A+y) = r(A)+1$, then we have $r(A)+1 = r(A+x)+1 = r(A+y) \leq r(A+y+x)$. On the other hand, again by (R2'), $r(A+y+x)$ is either equal to $r(A+x)$ or to $r(A+x)+1$. We conclude that $r(A+y+x) = r(A+x)+1$ and again $r(A+y+x) - r(A+y) = 0$. □

We now prove the alternative rank axioms.

Theorem 31. *Let r be an integer-valued function defined on the subspaces of E. Then r is the rank function of a q-matroid (E, r) if and only if r satisfies the axioms (R1'), (R2'), (R3').*

Proof. To prove this theorem, we have to prove that (R1), (R2), (R3) $\Leftrightarrow$ (R1'), (R2'), (R3').
First, assume r satisfies (R1), (R2), (R3). (R1') follows directly from (R1) with $A = \{0\}$. From (R2) it follows that $r(A) \leq r(A+x)$. Lemma 3 from [9] in combination with (R1') gives that $r(A+x) \leq r(A)+1$. Together this proves (R2'). (R3') is Proposition 7 from [9].
Now we consider the other implication. Assume r satisfies (R1'), (R2'), (R3').
For (R1'), let $A = x_1 + x_2 + \cdots + x_n$ with $n = \dim A$. Start with (R1') and apply (R2') n times. We do something similar for (R2): let $B = A + x_1 + \cdots + x_k$ with $k = \dim B - \dim A$. Now apply (R2') k times.

We will prove (R3) by induction on $\dim B - \dim(A \cap B) = k$. Denote $A \cap B = C$.
First, let $k = 0$, so $C \subseteq A$. Then we have $r(A + C) + r(A \cap C) = r(A) + r(B)$ so (R3) holds. Next, assume that (R3) holds for all A and B with $\dim B - \dim(A \cap B) < k$. Let $B' \subseteq B$ of codimension 1 such that $A \cap B = A \cap B'$ and let x be a 1-dimensional subspace such that $B' + x = B$. Then, by the induction hypothesis and the lemma above, we have

$$\begin{aligned} r(A+B) + r(A \cap B) &= r(A + B' + x) + r(A \cap (B' + x)) \\ &= r(A + B' + x) + r(A \cap B') \\ &\leq r(A + B' + x) - r(A + B') + r(A) + r(B') \\ &\leq r(B' + x) - r(B') + r(A) + r(B') \\ &= r(A) + r(B). \end{aligned}$$

This proves (R3), and thus completes our proof. □

4.3. **Hyperplanes.** We prove a stronger version of the hyperplane axiom (H3). We will use this axiom in Section 8 when we prove the cryptomorphism between flats and hyperplanes.

Let $\mathcal{H}$ be a collection of subspaces of E.

(H3') For each $H_1, H_2 \in \mathcal{H}$, $H_1 \neq H_2$, let $x, y \subseteq E$ be 1-dimensional spaces with $x \nsubseteq H_1, H_2$ and $y \subseteq H_1$, $y \nsubseteq H_2$. Then there is an hyperplane H_3 such that $(H_1 \cap H_2) + x \subseteq H_3$ and $y \nsubseteq H_3$.

Theorem 32. *Let $\mathcal{H}$ be a family of subspaces of E.*
The family $\mathcal{H}$ satisfies the axioms (H1), (H2), (H3) if and only if it satisfies (H1), (H2), (H3').

Proof. One direction is clear, since (H3') implies (H3). We will show the converse. Suppose that axioms (H1), (H2), (H3) hold for $\mathcal{H}$. We proceed by induction on the codimension of $H_1 \cap H_2$.
It cannot be that $\operatorname{codim}(H_1 \cap H_2) = 0$ since if so, then $H_1 = H_2 = E$, which violates (H1). Similarly, $\operatorname{codim}(H_1 \cap H_2) \neq 1$, since then one of H_1, H_2 must be equal to E. The assertion holds void then in these two cases. Suppose now $\operatorname{codim}(H_1 \cap H_2) = d \geq 2$ and that for codimension $d-1$ the assertion holds true. Let us prove it for codimension d.
Let $H_1, H_2 \in \mathcal{H}$, $H_1 \neq H_2$ and let x, y two spaces of dimension one such that $x \nsubseteq H_1, H_2$ and $y \subseteq H_2$, $y \nsubseteq H_1$. Using (H3) we can say that there is a hyperplane $H_3 \supseteq (H_1 \cap H_2) + x$. If $y \nsubseteq H_3$ we are done, so therefore we suppose $y \subseteq H_3$. This implies $\operatorname{codim}(H_2 \cap H_3) < \operatorname{codim}(H_1 \cap H_2)$. Moreover, since $H_1 \nsubseteq H_3$, there is a one-dimensional subspace $z \subseteq H_1$ such that $z \nsubseteq H_2, H_3$. Therefore, we can apply the induction hypothesis, finding $H_4 \in \mathcal{H}$ such that $x \nsubseteq H_4 \supseteq (H_2 \cap H_3) + z$. Since $x \nsubseteq H_1, H_4$, $y \subseteq H_4$, $y \nsubseteq H_1$ and $\operatorname{codim}(H_1 \cap H_4) < \operatorname{codim}(H_1 \cap H_2)$ we can use (H3') again by the induction hypothesis, and we get a new hyperplane $H_5 \in \mathcal{H}$ such that $y \nsubseteq H_5 \supseteq (H_1 \cap H_4) + x \supseteq (H_1 \cap H_2) + x$, from which the result follows. □

Remark 33. In the case of classical matroids, the statement of (H3') is often formulated as follows:

(H3') For every $H_1, H_2 \in \mathcal{H}$ such that $H_1 \neq H_2$ and for every $x \notin H_1 \cup H_2$, $y \in H_2 \setminus H_1$ there exists $H_3 \in \mathcal{H}$ such that $y \notin H_3 \supseteq (H_1 \cap H_2) \cup x$.

The condition $x \notin H_1 \cup H_2$ in the classical case is equivalent to saying that $x \notin H_1$ and $x \notin H_2$. However, in the q-analogue, saying that $x \nsubseteq H_1 + H_2$ is clearly not the same as saying $x \nsubseteq H_1$ and $x \nsubseteq H_2$. We point out that the latter is what we consider in the q-analogue.

5. Independent Spaces and the Closure Function

The goal of this section is to prove that a function satisfying the closure axioms of Definition 15 gives rise to a family of independent spaces satisfying the independence axioms of Definition 7. We use this to prove a cryptomorphic description of a q-matroid in terms of its closure function, As might be expected, the generalisation of the cryptomorphism in the q-analogue is non-trivial in this case.

Lemma 34. *Let* cl *be a closure function on* E *and let* $A, B \in \mathcal{L}(E)$*. If* $A \subseteq \mathrm{cl}(B)$*, then* $\mathrm{cl}(A) \subseteq \mathrm{cl}(B)$*. In particular, if* $B \subseteq A \subseteq \mathrm{cl}(B)$*, then* $\mathrm{cl}(A) = \mathrm{cl}(B)$*.*

Proof. By (Cl2), we have that $\mathrm{cl}(A) \subseteq \mathrm{cl}(\mathrm{cl}(B))$. By (Cl3), $\mathrm{cl}(\mathrm{cl}(B)) = \mathrm{cl}(B)$. Combined with applying (Cl2) to $A \subseteq B$, we get equality $\mathrm{cl}(A) = \mathrm{cl}(B)$. □

Lemma 35. *Let* $x \in \mathcal{L}(E)$ *be a* 1*-dimensional space. If* $x \subseteq \mathrm{cl}(A)$*, then* $\mathrm{cl}(A) = \mathrm{cl}(A + x)$*.*

Proof. We have $x \subseteq \mathrm{cl}(A)$ and also $A \subseteq \mathrm{cl}(A)$, hence $A + x \subseteq \mathrm{cl}(A)$. This implies $\mathrm{cl}(A + x) \subseteq \mathrm{cl}(A)$. But since $A \subseteq A + x$, we have also that $\mathrm{cl}(A) \subseteq \mathrm{cl}(A + x)$. Hence equality holds. □

We will apply Lemmas 34 and 35 frequently and not necessarily with direct reference to them.

Definition 36. Let cl be a closure function on E. We say that $I \in \mathcal{L}(E)$ is an independent space of (E, cl) if, for each subspace $A \subseteq I$ with $\mathrm{codim}_I(A) = 1$, we have $\mathrm{cl}(A) \neq \mathrm{cl}(I)$. We write $\mathcal{I}_{\mathrm{cl}}$ to denote the set of independent spaces of (E, cl).

Lemma 37. *Let* cl *be a closure function on* E *and let* $I, J \in \mathcal{L}(E), I \subseteq J$ *satisfy* $\dim(J) = \dim(I)+1$*. If* $I \in \mathcal{I}_{\mathrm{cl}}$ *and* $J \notin \mathcal{I}_{\mathrm{cl}}$*, then* $\mathrm{cl}(I) = \mathrm{cl}(J)$*.*

Proof. Since $J \notin \mathcal{I}_{\mathrm{cl}}$, there is a subspace $A \subseteq J$ such that $\mathrm{codim}_J(A) = 1$ and $\mathrm{cl}(A) = \mathrm{cl}(J)$. If $I = A$ we are done, so suppose therefore that $A \neq I$ and let $U = A \cap I$. Then $\mathrm{codim}_J(U) = 2$ and $\mathrm{codim}_I(U) = \mathrm{codim}_A(U) = 1$, so there exist 1-dimensional spaces $x, y \subseteq J$ such that $I = U + y$ and $A = U + x$. Now, $y \subseteq \mathrm{cl}(J) = \mathrm{cl}(A) = \mathrm{cl}(U + x)$. On the other hand, since I is independent, by definition we have $\mathrm{cl}(U) \subsetneq \mathrm{cl}(I)$. If $y \subseteq \mathrm{cl}(U)$, then $\mathrm{cl}(U) = \mathrm{cl}(U+y) = \mathrm{cl}(I)$, yielding a contradiction. So $y \notin \mathrm{cl}(U)$. By (Cl4) we have

$$y \subseteq \mathrm{cl}(x + U) \text{ and } y \notin \mathrm{cl}(U) \implies x \subseteq \mathrm{cl}(U + y) = \mathrm{cl}(I),$$

which implies that $\mathrm{cl}(I) = \mathrm{cl}(I + x) = \mathrm{cl}(J)$. The result follows. □

Lemma 38. *Let* $I \in \mathcal{L}(E)$*.*

(1) $I \in \mathcal{I}_{\mathrm{cl}}$ *if and only if every proper subspace* U *of* I *satisfies* $\mathrm{cl}(U) \subsetneq \mathrm{cl}(I)$*.*
(2) Let $A \subseteq I$ *such that* $\mathrm{codim}_I(A) = 1$*. If there exists* $x \subseteq I$*, satisfying* $I = x + A$ *and* $x \subseteq \mathrm{cl}(A)$*, then* $I \notin \mathcal{I}_{\mathrm{cl}}$*.*

Proof. Let $U \subsetneq I$. There exists a subspace W of co-dimension one in I such that $U \subseteq W \subseteq I$. Then by (Cl2) we have $\mathrm{cl}(U) \subseteq \mathrm{cl}(W) \subseteq \mathrm{cl}(I)$. If $I \in \mathcal{I}_{\mathrm{cl}}$, then $\mathrm{cl}(U) \subseteq \mathrm{cl}(W) \subsetneq \mathrm{cl}(I)$. Conversely, if every proper subspace of I has closure strictly contained in $\mathrm{cl}(I)$, then in particular this is true of every subspace of co-dimension 1 in I, and so $I \in \mathcal{I}_{cl}$ by definition. This establishes (1).

Let x be a 1-dimensional subspace of I such that $x + A = I$. If $x \subseteq \mathrm{cl}(A)$, then $\mathrm{cl}(A) = \mathrm{cl}(x + A) = \mathrm{cl}(I)$, and hence $I \notin \mathcal{I}_{\mathrm{cl}}$. This establishes (2). □

Theorem 39. *Let* (E, cl) *be a closure function. Then* $(E, \mathcal{I}_{\mathrm{cl}})$ *satisfies the axioms (I1)-(I4).*

Proof. Consider first (I1): the space $\{0\}$ does not have any subspaces of codimension 1, so the property in the definition of independence holds vacuously. Hence $\{0\} \in \mathcal{I}_{\mathrm{cl}}$ and thus (I1) holds.

We now show (I2). Let $I \in \mathcal{I}_{\mathrm{cl}}$ and $I' \subseteq I$. We will show that $I' \in \mathcal{I}_{\mathrm{cl}}$. Let $A' \subseteq I'$ be a subspace of codimension one. Let $A \subseteq I$ be a subspace of codimension one satisfying $A' = A \cap I'$. There is a 1-dimensional space $x \subseteq I'$, $x \notin A$ such that $I' = A' + x$ and $I = A + x$. We claim that $\mathrm{cl}(A') \neq \mathrm{cl}(I')$. Suppose not. Then $\mathrm{cl}(I') = \mathrm{cl}(A') \subseteq \mathrm{cl}(A)$ by (Cl2). Since $x \subseteq I'$, it follows that $x \subseteq \mathrm{cl}(A)$. But then $\mathrm{cl}(A) = \mathrm{cl}(A + x) = \mathrm{cl}(I)$, which contradicts the fact that $I \in \mathcal{I}_{\mathrm{cl}}$. Therefore, $\mathrm{cl}(I') \neq \mathrm{cl}(A')$ and $I' \in \mathcal{I}_{\mathrm{cl}}$.

Now Let $I, J \in \mathcal{I}_{\mathrm{cl}}$ such that $\dim J > \dim I$. We will show that there exists a 1-dimensional space $x \subseteq J$, $x \notin I$ such that $x + I \in \mathcal{I}_{\mathrm{cl}}$. This will establish (I3).

Suppose that (I3) fails for the pair I, J. That is, suppose that for any 1-dimensional $x \subseteq J$, $x \nsubseteq I$, we have $x + I \notin \mathcal{I}_{\mathrm{cl}}$. Then from (Cl1) and Lemma 37 (which requires (Cl4)), we have that $\mathrm{cl}(x + I) = \mathrm{cl}(I)$ and so in particular, $x \subseteq \mathrm{cl}(I)$ for every $x \subseteq J$, $x \nsubseteq I$. It follows that $J \subseteq \mathrm{cl}(I)$ and hence $\mathrm{cl}(J) \subseteq \mathrm{cl}(I)$, by (Cl2). Now suppose further that $\dim(I \cap J)$ is maximal over all such pairs that fail (I3).

We first note that $I \nsubseteq \mathrm{cl}(U)$ for any proper subspace U of J, since otherwise by the independence of J we would have $I \subseteq \mathrm{cl}(U) \subsetneq \mathrm{cl}(J)$, which yields the contradiction $\mathrm{cl}(J) \subseteq \mathrm{cl}(I) \subsetneq \mathrm{cl}(J)$. Since $\dim(J) > \dim(I)$, there exists a subspace A of codimension 1 in J such that $I \cap J = I \cap A$. Since $I \nsubseteq \mathrm{cl}(A)$, there exists some $b \subseteq I$, $b \nsubseteq \mathrm{cl}(A)$. We claim that $b + A \in \mathcal{I}_{\mathrm{cl}}$. As $A \subsetneq J$, by (I2) A is independent. If $b + A$ is not independent, we may apply Lemma 37 to deduce that $b \subseteq \mathrm{cl}(b + A) = \mathrm{cl}(A)$, which contradicts our choice of $b \subseteq I, b \nsubseteq \mathrm{cl}(A)$. Write $J' = b + A$. Then as we have just shown, $J' \in \mathcal{I}_{\mathrm{cl}}$ and $\dim(J') = \dim(J) > \dim(I)$. Now $b \nsubseteq \mathrm{cl}(A)$, so in particular, $b \nsubseteq A$ and hence $b \nsubseteq A \cap I = J \cap I$. Moreover, we have $b + (J \cap I) = b + (A \cap I) \subseteq (b + A) \cap I = J' \cap I$, from which we deduce that $\dim(J' \cap I) > \dim(J \cap I)$. By the maximality of $\dim(J \cap I)$ in our hypothesis, it must now be the case that J' and I satisfy (I3). That is, there exists $x \subseteq J'$, $x \notin I$ such that $x + I$ is independent. Now $x \subseteq J' = b + A$, so $x = \langle \bar{b} + \bar{a} \rangle$ for some $\bar{b} \in b$, and $\bar{a} \in A$. Then $x + I = \langle \bar{b} + \bar{a} \rangle + I = a + I$ for some $a \subseteq A \subseteq J$, since $b \subseteq I$. But this contradicts our assumption that (I3) fails for I and J. We deduce that (I3) holds for I and J and hence holds true in general.

We will establish that (I4") holds. By Lemma 26, this will show that (Cl1)-(Cl4) are sufficient to prove that the axiom (I4) holds for $\mathcal{I}_{\mathrm{cl}}$.

(I4") Let $A \in \mathcal{L}(E)$ and let $I \in \max(A, \mathcal{I}_{\mathrm{cl}})$. Let $x \in \mathcal{L}(E)$ be a 1-dimensional space. We will show that $x + A$ has a maximal independent subspace contained in $x + I$.

If $A = I$, then any subspace of $x + A$ is a subspace of $x + I$, so the result holds. Suppose then that $I \subsetneq A$. If $x \subseteq A$, then $\max(x + A, \mathcal{I}_{\mathrm{cl}}) = \max(A, \mathcal{I}_{\mathrm{cl}})$ and so I is the required member of $\max(x + A, \mathcal{I}_{\mathrm{cl}})$ contained $x + I$. Therefore, for the remainder we assume that $x \notin A$. Again by the maximality of I in A, $a + I \notin \mathcal{I}_{\mathrm{cl}}$ for every 1-dimensional space $a \subseteq A, a \nsubseteq I$. Therefore, by Lemma 37, $\mathrm{cl}(a + I) = \mathrm{cl}(I)$ for every $a \subseteq A$ and so by (Cl2) and (Cl3), $A \subseteq \mathrm{cl}(I)$.

Let $M \in \max(x + A, \mathcal{I}_{\mathrm{cl}})$. By Lemma 27, we may choose M such that $I \subseteq M$. If $M = I$, then I itself gives the required subspace of $x + I$ in $\max(x + A, \mathcal{I}_{\mathrm{cl}})$, so assume that $I \subsetneq M$, i.e. that $\dim(M) > \dim(I)$. In particular, this means that $M \nsubseteq A$, by the maximality of I in A.

By Lemma 28, $\dim(M) = \dim(I) + 1$. If $x + I \in \mathcal{I}_{cl}$, then $\dim(x + I) = \dim(M)$, so $x + I \in \max(x + A, \mathcal{I})$ and (I4) holds. We now assume that $x + I \notin \mathcal{I}_{\mathrm{cl}}$.

Since $x + I \notin \mathcal{I}_{\mathrm{cl}}$, by Lemma 37, we have $\mathrm{cl}(x + I) = \mathrm{cl}(I)$. Therefore $x \subseteq \mathrm{cl}(I)$ and as we showed above, $A \subseteq \mathrm{cl}(I)$ and so $x + A \subseteq \mathrm{cl}(I)$. In particular, $M = m + I \subseteq x + A \subseteq \mathrm{cl}(I)$ and so $\mathrm{cl}(M) = \mathrm{cl}(I)$, which by Lemma 37 contradicts the independence of M. We deduce that $x + I \in \mathcal{I}_{\mathrm{cl}}$ and hence (I4) holds. □

Corollary 40. *Let (E, cl) be a closure function and let $(E, \mathcal{I})$ be a collection of independent spaces.*

(1) (E, cl) determines a q-matroid (E, r) whose set of independent spaces is $\mathcal{I}_{\mathrm{cl}}$ and whose closure function satisfies $\mathrm{cl}_r = \mathrm{cl}$.

(2) Define a function $r_{\mathcal{I}} : \mathcal{L}(E) \longrightarrow \mathbb{Z} : A \mapsto \max\{\dim(I) : I \in \mathcal{I}, I \subseteq A\}$. Then $(E, r_{\mathcal{I}})$ is a q-matroid whose closure function is $\mathrm{cl}_{\mathcal{I}}$ and whose set of independent spaces is $\mathcal{I}$.

Proof. We have a closure function (E, cl), which from Theorem 39 yields a collection of independent spaces $(E, \mathcal{I}_{\mathrm{cl}})$. From [9, Theorem 8], $(E, \mathcal{I}_{\mathrm{cl}})$ yields a q-matroid (E, r) with rank function defined by $r(A) := \max\{\dim I : I \in \mathcal{I}_{\mathrm{cl}}, I \subseteq A\}$ for each $A \in \mathcal{L}(E)$, and whose independent spaces coincide with $\mathcal{I}_{\mathrm{cl}}$. Recall that the closure function of (E, r) is defined by $\mathrm{cl}_r(A) := \sum_{x \in C_r(A)} x$, where $C_r(A) = \{x \in \mathcal{L}(E) : \dim(x) = 1, r(A + x) = r(A)\}$. We claim that $\mathrm{cl}_r(A) = \mathrm{cl}(A)$ for each $A \in \mathcal{L}(E)$. Let $A \in \mathcal{L}(E)$ and let $I \in \max(A, \mathcal{I}_{\mathrm{cl}})$. Then $r(A) = r(I) = \dim(I)$ by definition. Also, $I + a \notin \mathcal{I}_{\mathrm{cl}}$ for

any $a \subseteq A, a \nsubseteq I$ and so from Lemma 37 we have $a \subseteq \mathrm{cl}(a+I) = \mathrm{cl}(I)$. Since a was chosen arbitrarily in A, by (Cl2) we get $\mathrm{cl}(A) = \mathrm{cl}(I)$.

Let x be a 1-dimensional space such that $x \subseteq \mathrm{cl}(A)$, $x \nsubseteq A$. Clearly $x \subseteq \mathrm{cl}(I) = \mathrm{cl}(A)$, so $x+I \notin \mathcal{I}_{\mathrm{cl}}$ and hence by (I4), $I \in \max(x+A, \mathcal{I}_{\mathrm{cl}})$. Then $r(A) = r(I) = \dim I = r(A+x)$ and so $x \subseteq \mathrm{cl}_r(A)$. Therefore $\mathrm{cl}(A) \subseteq \mathrm{cl}_r(A)$. Now suppose that $x \subseteq \mathrm{cl}_r(A), x \nsubseteq A$. Then $r(I) = r(A) = r(A+x) \geq r(I+x) \geq r(I)$ and so $x + I \notin \mathcal{I}$. Again by Lemma 37 we have $x \subseteq \mathrm{cl}(x+A) = \mathrm{cl}(I) = \mathrm{cl}(A)$ and so $\mathrm{cl}(A) = \mathrm{cl}_r(A)$. This proves (1).

By [9, Theorem 8], $(E, r_{\mathcal{I}})$ is a q-matroid with collection of independent spaces equal to $\mathcal{I}$. Define a map $\mathrm{cl}_{\mathcal{I}} := \mathrm{cl}_r$. By [9, Theorem 68], $\mathrm{cl}_{\mathcal{I}}$ is a closure function, which proves (2). □

6. Flats and the Closure Function

We now establish that the flat axioms and the closure axioms are cryptomorphic.

Definition 41. Let $(E, \mathcal{F})$ be a collection of subspaces containing E. For each subspace $A \in \mathcal{L}(E)$, we define

$$\mathrm{cl}_{\mathcal{F}}(A) := \bigcap \{F : F \in \mathcal{F}, A \subseteq F\}.$$

Lemma 42. *Let $(E, \mathcal{F})$ be a collection of subspaces satisfying (F1) and (F2) and let A be a subspace of E. Then $\mathrm{cl}_{\mathcal{F}}(A) \in \mathcal{F}$.*

Proof. By (F1), $E \in \mathcal{F}$ and $A \in \mathcal{L}(E)$, so $\mathrm{cl}_{\mathcal{F}}(A)$ is well defined. Observe that $\mathrm{cl}_{\mathcal{F}}(A)$ is a finite-dimensional subspace of E. Define $\mathcal{F}_A := \min(\{F \in \mathcal{F} : A \subseteq F\})$. Clearly,

$$\mathrm{cl}_{\mathcal{F}}(A) = \bigcap \{F : F \in \mathcal{F}, A \subseteq F\} = \bigcap \{F : F \in \mathcal{F}_A\}$$

since every member of $\{F \in \mathcal{F} : A \subseteq F\}$ contains a member of $\mathcal{F}_A$. Let $F_1, F_2 \in \mathcal{F}_A$. Then $A, \mathrm{cl}_{\mathcal{F}}(A) \subseteq F_1, F_2$ and by (F2), $F_1 \cap F_2 \in \mathcal{F}$. This implies $F_1 = F_2$, so $|\mathcal{F}_A| \leq 1$. If $\mathcal{F}_A$ is empty, then for any subspace $F \in \mathcal{F}$ that contains A there exists a subspace $F' \in \mathcal{F}$, $F' \subsetneq F$ and so we could construct the infinite chain of subspaces of E, which contradicts the fact that E is finite dimensional. Therefore, $\mathrm{cl}_{\mathcal{F}}(A) = F$ for the unique $F \in \mathcal{F}$ satisfying $\mathcal{F}_A = \{F\}$. □

Before stating and proving the cryptomorphism, we prove a result about closure that will also be used later on in the cryptomorphism between rank and closure.

Lemma 43. *Let* cl *be a closure function on E and let $A, B \in \mathcal{L}(E)$. If $\mathrm{cl}(A) \subseteq \mathrm{cl}(B) \subseteq \mathrm{cl}(A+x)$, then $\mathrm{cl}(A) = \mathrm{cl}(B)$ or $\mathrm{cl}(B) = \mathrm{cl}(A+x)$.*

Proof. First, note that if $x \subseteq A$, then $\mathrm{cl}(A) = \mathrm{cl}(A+x)$ by Lemma 35. This implies $\mathrm{cl}(A) = \mathrm{cl}(B) = \mathrm{cl}(A+x)$ and proves the statement.
Assume $x \nsubseteq A$ and suppose, towards a contradiction, that $\mathrm{cl}(A) \subsetneq \mathrm{cl}(B) \subsetneq \mathrm{cl}(A+x)$. Assume also that $x \subseteq \mathrm{cl}(B)$. Since $A \subseteq \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$, we have $A + x \subseteq \mathrm{cl}(B)$. Then Lemma 34 gives that $\mathrm{cl}(A+x) \subseteq \mathrm{cl}(B) \subsetneq \mathrm{cl}(A+x)$, a contradiction. So it needs to be that $x \notin \mathrm{cl}(B)$.
Let $y \in \mathcal{L}(E)$ be a 1-dimensional space such that $y \subseteq \mathrm{cl}(B)$, $y \nsubseteq \mathrm{cl}(A)$. Then $y \subseteq \mathrm{cl}(A+x)$ and axiom (Cl4) gives that $x \subseteq (A+y)$. On the other hand, since both $A \subseteq \mathrm{cl}(B)$ and $y \subseteq \mathrm{cl}(B)$, we have that $A + y \subseteq \mathrm{cl}(B)$ and Lemma 34 gives $\mathrm{cl}(A+y) \subseteq \mathrm{cl}(B)$. This gives a contradiction with $x \subseteq \mathrm{cl}(B)$. In the end, we conclude that it can not happen that $\mathrm{cl}(A) \subsetneq \mathrm{cl}(B) \subsetneq \mathrm{cl}(A+x)$, hence the lemma holds. □

Theorem 44. *Let (E, cl) be a closure function and let $\mathcal{F}_{\mathrm{cl}} := \{F \in \mathcal{L}(E) : \mathrm{cl}(F) = F\}$. Then $(E, \mathcal{F}_{\mathrm{cl}})$ is a collection of flats.*

Proof. We will show that $\mathcal{F}_{\mathrm{cl}}$ satisfies (F1), (F2), and (F3). The condition (F1) holds trivially. Now let $F_1, F_2 \in \mathcal{F}_{\mathrm{cl}}$. Clearly $F_1 \cap F_2 \subseteq \mathrm{cl}(F_1 \cap F_2)$. Now $F_1 \cap F_2 \subseteq F_1, F_2$, so by (Cl2) and (Cl3) we have $\mathrm{cl}(F_1 \cap F_2) \subseteq \mathrm{cl}(F_1) = F_1, \mathrm{cl}(F_2) = F_2$. It follows that $F_1 \cap F_2 = \mathrm{cl}(F_1 \cap F_2)$ and hence (F2) holds.

Now let $F \in \mathcal{F}_{\mathrm{cl}}$ and let $x \in \mathcal{L}(E), x \notin F$ have dimension 1. By Lemma 43, the flat $\mathrm{cl}(F+x)$ is a cover of F.

We claim that $\mathrm{cl}(x+F)$ is unique. Let F_1 be a cover of F that contains x. Let $y \subseteq F_1$, $y \nsubseteq F$. Then $y+F \subseteq F_1$, so by (Cl2) it follows that $\mathrm{cl}(y+F) \subseteq F_1$, and since $F \neq \mathrm{cl}(y+F)$ it follows that $F_1 = \mathrm{cl}(y+F)$. We now claim that $\mathrm{cl}(x+F) \cap \mathrm{cl}(y+F) = F$. Let z be a 1-dimensional subspace of $\mathrm{cl}(x+F) \cap \mathrm{cl}(y+F)$ and suppose that $z \nsubseteq F$. Then by (Cl4) we have $z \subseteq \mathrm{cl}(x+F)$ and $z \nsubseteq F$, which implies that $x \subseteq \mathrm{cl}(z+F)$. Similarly, $y \subseteq cl(z+F)$. But then, applying (Cl2) and (Cl3) , we have $\mathrm{cl}(z+F) \subseteq \mathrm{cl}(x+F), \mathrm{cl}(y+F) \subseteq \mathrm{cl}(z+F)$, and so $\mathrm{cl}(x+F) = \mathrm{cl}(y+F) = \mathrm{cl}(z+F)$. We deduce that $\mathrm{cl}(x+F)$ is the required unique flat of $\mathcal{F}_{\mathrm{cl}}$ that contains x and covers F. Therefore (F3) holds. □

Theorem 45. *Let $(E, \mathcal{F})$ be a collection of flats and let $\mathrm{cl}_{\mathcal{F}} : \mathcal{L}(E) \to \mathcal{L}(E)$ be the map defined by $\mathrm{cl}_{\mathcal{F}}(A) := \bigcap\{F \in \mathcal{F} : A \subseteq F\}$ for each subspace $A \in \mathcal{L}(E)$. Then $(E, \mathrm{cl}_{\mathcal{F}})$ is a closure function.*

Proof. We will prove that $\mathrm{cl}_{\mathcal{F}}$ satisfies the axioms (Cl1)-(Cl4). Clearly $A \subseteq \bigcap\{F \in \mathcal{F} : A \subseteq F\} = \mathrm{cl}_{\mathcal{F}}(A)$ for any subspace $A \in \mathcal{L}(E)$, so (Cl1) holds. If $A \subseteq B$ are subspaces of E, then any flat F containing B also contains A so $\mathrm{cl}_{\mathcal{F}}(A) \subseteq \mathrm{cl}_{\mathcal{F}}(B)$ and thus (Cl2) holds. Let A be a subspace of E. We claim that $\mathrm{cl}_{\mathcal{F}}(\mathrm{cl}_{\mathcal{F}}(A)) = \mathrm{cl}_{\mathcal{F}}(A)$. By Lemma 42, $\mathrm{cl}_{\mathcal{F}}(A)$ is itself a flat. In particular, $\mathrm{cl}_{\mathcal{F}}(F) = F$ for any $F \in \mathcal{F}$. Therefore $\mathrm{cl}_{\mathcal{F}}(\mathrm{cl}_{\mathcal{F}}(A)) = \mathrm{cl}_{\mathcal{F}}(A)$ and so (Cl3) holds.

Let $x, y \in \mathcal{L}(E)$ be subspaces of dimension 1. Suppose that $y \subseteq \mathrm{cl}_{\mathcal{F}}(A+x)$, $y \nsubseteq \mathrm{cl}_{\mathcal{F}}(A)$. We claim that $x \subseteq \mathrm{cl}_{\mathcal{F}}(A+y)$. Suppose to the contrary that $x \nsubseteq \mathrm{cl}_{\mathcal{F}}(A+y)$. Then $\mathrm{cl}_{\mathcal{F}}(A) \subsetneq \mathrm{cl}_{\mathcal{F}}(x+A)$ and $\mathrm{cl}_{\mathcal{F}}(A) \subsetneq \mathrm{cl}(y+A)$. By (F3) there is a unique flat $F \in \mathcal{F}$ that covers A and contains x. By (Cl2) and (Cl3) we have $A+x \subset \mathrm{cl}_{\mathcal{F}}(A+x) \subset F$ and so $F = \mathrm{cl}_{\mathcal{F}}(A+x)$. Similarly $\mathrm{cl}_{\mathcal{F}}(A+y)$ is the unique cover of A that contains y.

Now $y \subset \mathrm{cl}_{\mathcal{F}}(A+x)$ and $y \subseteq \mathrm{cl}_{\mathcal{F}}(A)$ by hypothesis and clearly $y \subseteq \mathrm{cl}_{\mathcal{F}}(A+y)$, so in particular y is contained in two flats that cover A. Again by (F3), this means that $\mathrm{cl}_{\mathcal{F}}(A+x) = \mathrm{cl}_{\mathcal{F}}(A+y)$, contradicting $x \notin \mathrm{cl}_{\mathcal{F}}(A+y)$. We deduce that $x \subseteq \mathrm{cl}_{\mathcal{F}}(A+y)$. This establishes that (Cl4) holds. □

Lemma 46. *Let (E, cl) be a closure function and let $(E, \mathcal{F})$ be a collection of flats.*

(1) For each subspace $A \in \mathcal{L}(E)$, it holds that $\mathrm{cl}(A) = \bigcap\{B \in \mathcal{L}(E) : A \subseteq B, B = \mathrm{cl}(B)\}$.

(2) For each subspace $F \in \mathcal{L}(E)$, it holds that $F \in \mathcal{F} \Leftrightarrow F = \bigcap\{K \in \mathcal{F} : F \subseteq K\}$.

Proof. Let A be a subspace of E. Let $\mathcal{A} := \{B \in \mathcal{L}(E) : A \subseteq B, B = \mathrm{cl}(B)\}$. Since $A \subseteq \mathrm{cl}(A)$ by (Cl2), and since $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$ by (Cl3), we have $\mathrm{cl}(A) \in \mathcal{A}$ and hence $\bigcap\{B : B \in \mathcal{A}\} \subseteq \mathrm{cl}(A)$. Conversely, if $B \in \mathcal{A}$, then $A \subseteq B$ and $\mathrm{cl}(B) = B$. Therefore, by (Cl2) and (Cl3) we have $\mathrm{cl}(A) \subseteq \mathrm{cl}(B) = B$, so $\mathrm{cl}(A)$ is contained in the intersection of all members of $\mathcal{A}$ and we have $\mathrm{cl}(A) = \bigcap\{B : B \in \mathcal{A}\}$. This shows that (1) holds.

For each subspace $A \in \mathcal{L}(E)$, define $\mathcal{F}(A) := \{K \in \mathcal{F} : A \subseteq K\}$. If $F \in \mathcal{F}$, then $F \in \mathcal{F}(F)$ and so $\bigcap\{K : K \in \mathcal{F}(F)\} \subseteq F$. On the other hand, every member of $\mathcal{F}(F)$ contains F, by definition, so $F \subseteq \bigcap\{K : K \in \mathcal{F}(F)\}$. Therefore, if $F \in \mathcal{F}$, then $F = \bigcap\{K : K \in \mathcal{F}(F)\}$. Conversely, $F = \bigcap\{K : K \in \mathcal{F}(F)\}$ is a flat by Lemma 42. This shows that (2) holds. □

Definition 47. Given a family of flats $(E, \mathcal{F})$ the function

$$r_{\mathcal{F}} : \mathcal{L}(E) \longrightarrow \mathbb{Z}$$

is defined as follows. For any $A \in \mathcal{L}(E)$, $r_{\mathcal{F}}(A)$ is the length of the longest chain between $\mathrm{cl}_{\mathcal{F}}(\{0\})$ and $\mathrm{cl}_{\mathcal{F}}(A)$.

We recall the following result from [4, Theorem 3].

Theorem 48. *Let $(E, \mathcal{F})$ be a family of flats and let (E, r) be a q-matroid. Then $(E, r_{\mathcal{F}})$ is a q-matroid whose family of flats is equal to $\mathcal{F}$. Conversely,*

$$\mathcal{F}_r := \{A \in \mathcal{L}(E) : r(A+x) > r(A)\ \forall x \in \mathcal{L}(E), \dim(x) = 1, x \notin A\},$$

is a collection of flats for the matroid $(E, r_{\mathcal{F}_r})$.

Corollary 49. *Let* (E, cl) *be a closure function and let* $(E, \mathcal{F})$ *be a collection of flats. Let* $\mathcal{F}_{\mathrm{cl}}$ *and* $\mathrm{cl}_{\mathcal{F}}$ *be defined as in Theorem 44 and 45.*

(1) (E, cl) *determines a q-matroid with closure function* cl *and collection of flats* $\mathcal{F}_{\mathrm{cl}}$.
(2) $(E, \mathcal{F})$ *determines a q-matroid with collection of flats* $\mathcal{F}$ *and closure function* $\mathrm{cl}_{\mathcal{F}}$.

Proof. We have a closure function (E, cl), which from Theorem 44, yields the collection of flats $(E, \mathcal{F}_{\mathrm{cl}})$. By Theorem 49 $(E, \mathcal{F}_{\mathrm{cl}})$ determines a q-matroid (E, r) with flats $\mathcal{F}_r = \mathcal{F}_{\mathrm{cl}} = \{F \in \mathcal{L}(E) : \mathrm{cl}(F) = F\}$. We claim that $\mathrm{cl} = \mathrm{cl}_r$. Let A be a subspace of E. Recall that $\mathrm{cl}_r(A) := \sum_{x \in C_r(A)} x$, where $C_r(A) = \{x \in \mathcal{L}(E) : \dim(x) = 1, r(A + x) = r(A)\}$. It is thus clear that $\mathrm{cl}_r(A) \in \mathcal{F}_r = \mathcal{F}_{\mathrm{cl}}$. If $A \subseteq F \in \mathcal{F}_r$, then $\mathrm{cl}_r(A) \subseteq \mathrm{cl}_r(F) = F$, by the definition of $\mathcal{F}_{\mathrm{cl}}$. Therefore, by Lemma 46 (1), we have $\mathrm{cl}_r(A) = \bigcap\{F \in \mathcal{F}_{\mathrm{cl}} : \mathrm{cl}_r(A) \subseteq F\} = \bigcap\{F \in \mathcal{F}_{\mathrm{cl}} : A \subseteq F\}$. On the other hand, from Lemma 46 (2) we have $\mathrm{cl}(A) = \bigcap\{B \in \mathcal{L}(E) : \mathrm{cl}(B) = B, A \subseteq B\} = \bigcap\{B \in \mathcal{F}_{\mathrm{cl}} : A \subseteq B\}$, and so $\mathrm{cl}_r(A) = \mathrm{cl}(A)$. This proves (1).

We have a collection of flats $(E, \mathcal{F})$, which by Theorem 44 (2) determines a closure function $(E, \mathrm{cl}_{\mathcal{F}})$, with $\mathrm{cl}_{\mathcal{F}}(A) := \{F \in \mathcal{F} : A \subseteq F\}$ for $A \in \mathcal{L}(E)$. By Corollary 40, $(E, \mathrm{cl}_{\mathcal{F}})$ determines a q-matroid (E, r) such that $\mathrm{cl}_r = \mathrm{cl}_{\mathcal{F}}$. Now any $A \in \mathcal{F}_r$ if and only if $A = \mathrm{cl}_r(A) = \mathrm{cl}_{\mathcal{F}}(A)$ and so A is a flat of (E, r) if and only if $A = \cap\{F \in \mathcal{F} : A \subseteq F\}$, which by Lemma 46 (2) holds if and only if $F \in \mathcal{F}$. It follows that $(E, \mathcal{F})$ and $(E, \mathrm{cl}_{\mathcal{F}})$ determine the same q-matroid with flats $\mathcal{F}$ and closure function $\mathrm{cl}_{\mathcal{F}}$. This proves (2). □

7. The Rank and Closure Functions

In this section we prove the cryptomorphism between rank and closure. The main task is to describe the rank function in terms of the closure function.

Definition 50. Let cl be a closure function on E. Define a function $r_{\mathrm{cl}} : \mathcal{L}(E) \to \mathcal{L}(E)$ by

$$r_{\mathrm{cl}}(A) = \min\{\dim(I) : \mathrm{cl}(I) = \mathrm{cl}(A), I \subseteq A\}.$$

Definition 51. Let $A \in \mathcal{L}(E)$. A space $I \subseteq A$ such that $\mathrm{cl}(I) = \mathrm{cl}(A)$ and $r_{\mathrm{cl}}(A) = \dim I$ is called a *basis* for A.

Let us prove some partial results we need in the proof of the cryptomorphism.

Lemma 52. *Let* cl *be a closure function on* E *and let* $A \in \mathcal{L}(E)$. *Then* $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(\mathrm{cl}(A))$.

Proof. We have that $r_{\mathrm{cl}}(\mathrm{cl}(A)) = \min\{\dim I : \mathrm{cl}(I) = \mathrm{cl}(\mathrm{cl}(A)), I \subseteq \mathrm{cl}(A)\} = \min\{\dim I : \mathrm{cl}(I) = \mathrm{cl}(A), I \subseteq \mathrm{cl}(A)\}$. On the other hand, $r_{\mathrm{cl}}(A) = \min\{\dim I : \mathrm{cl}(I) = \mathrm{cl}(A), I \subseteq A\}$. The set in the definition of $r_{\mathrm{cl}}(A)$ is a subset of the set in the definition of $r_{\mathrm{cl}}(\mathrm{cl}(A))$ and because of (Cl1), the elements of minimal dimension are the same. So $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(\mathrm{cl}(A))$. □

Lemma 53. *Let* cl *be a closure function on* E *and let* $A, B \in \mathcal{L}(E)$. *If* $A \subseteq B$ *and* $\mathrm{cl}(A) = \mathrm{cl}(B)$, *then* A *contains a basis for* B.

Proof. Let I be a basis for A, so $\mathrm{cl}(I) = \mathrm{cl}(A)$. Since also $\mathrm{cl}(A) = \mathrm{cl}(B)$, we have that $\mathrm{cl}(I) = \mathrm{cl}(B)$. Also, by the previous lemma, $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(B) = \dim I$. So I is a basis of B. □

Lemma 54. *Let* cl *be a closure function on* E *and let* $A \in \mathcal{L}(E)$. *If* I *is a basis for* A *and* J *is a basis for* B, *then* $A + B$ *has a basis contained in* $I + J$.

Proof. This statement follows directly from the proof of Theorem 39. There we use the closure axioms to prove (I4), which is the same statement as this lemma. □

We now have all ingredients for the cryptomorphism between closure and rank.

Theorem 55. *Let (E, cl) be a closure function. Then (E, r_{cl}) satisfies the axioms (R1)-(R3).*

Proof. Recall that we proved in Theorem 31 that the axioms (R1),(R2),(R3) are equivalent to (R1'),(R2'),(R3'). We will prove the latter.
It follows straight from the definition that $r_{\mathrm{cl}}(\{0\}) = 0$, because $\{0\}$ only has subspaces of dimension 0. This proves (R1'). For (R2') we have to show that $r_{\mathrm{cl}}(A) \leq r_{\mathrm{cl}}(A + x) \leq r_{\mathrm{cl}}(A) + 1$.
First, suppose there is a basis J of $A + x$ such that $J \subseteq A$. Then $\mathrm{cl}(J) \subseteq \mathrm{cl}(A)$ because of (Cl2) but $\mathrm{cl}(J) = \mathrm{cl}(A + x)$ by definition, so again by (Cl2) we have that $\mathrm{cl}(A) = \mathrm{cl}(A + x)$. This means that also $r_{\mathrm{cl}}(\mathrm{cl}(A)) = r_{\mathrm{cl}}(\mathrm{cl}(A + x))$ and because of Lemma 52 we have that $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(A + x)$.
Next, assume that there is no basis J of $A + x$ such that $J \subseteq A$. Then, without loss of generality, we can write $J = J' + x$ with $J' = J \cap A$. We claim that J' is a basis for A. Assuming this claim, we have that $r_{\mathrm{cl}}(A + x) = \dim J = \dim(J') + 1 = r_{\mathrm{cl}}(A) + 1$. Together with the case $J \subseteq A$ we have proven (R2').
We must prove the claim that J' is a basis for A. We do this is two steps: first we show that $\mathrm{cl}(J') = \mathrm{cl}(A)$, then we show $\dim J' = r_{\mathrm{cl}}(A)$. Because $J' \subseteq A$, we have that $\mathrm{cl}(J') \subseteq \mathrm{cl}(A)$. Suppose, towards a contradiction, that there is a 1-dimensional subspace y such that $y \subseteq \mathrm{cl}(A)$ but $y \nsubseteq \mathrm{cl}(J')$. Then $y \subseteq \mathrm{cl}(A+x) = \mathrm{cl}(J'+x)$ but $y \nsubseteq \mathrm{cl}(J')$, so according to (Cl4) $x \subseteq \mathrm{cl}(J'+y)$. Because $J' + y \subseteq \mathrm{cl}(A)$, this means $x \subseteq \mathrm{cl}(A)$. But if both x and J' are in $\mathrm{cl}(A)$, also $J' + x = J \subseteq \mathrm{cl}(A)$, and then we would have the equality $\mathrm{cl}(A) = \mathrm{cl}(A + x)$. However, we assumed there was no basis for $A + x$ contained in A. This means we have a contraction, so there is no $y \subseteq \mathrm{cl}(A)$ that is not in $\mathrm{cl}(J')$. Hence $\mathrm{cl}(J') = \mathrm{cl}(A)$.
Now all that is left to show is that $\dim J' = r_{\mathrm{cl}}(A)$. Because $\mathrm{cl}(J') = \mathrm{cl}(A)$, we have that $\dim J' \geq r(A)$. Assume, towards a contradiction, that $\dim J' > r_{\mathrm{cl}}(A)$, so J' is not a basis for A. According to Lemma 53, there is an $I \subseteq J'$ that is a basis for A. We have that $\mathrm{cl}(I) = \mathrm{cl}(A)$ and $x \notin \mathrm{cl}(A)$ by assumption, so $\mathrm{cl}(A) \subsetneq \mathrm{cl}(I+x)$. On the other hand, $\mathrm{cl}(I+x) \subseteq \mathrm{cl}(J'+x) = \mathrm{cl}(J) = \mathrm{cl}(A+x)$. Together this gives that $\mathrm{cl}(A) \subsetneq \mathrm{cl}(I + x) \subseteq \mathrm{cl}(A + x)$ and by Lemma 43, this implies $\mathrm{cl}(I + x) = \mathrm{cl}(A + x)$. But this is a contradiction with $J' + x = J$ being a basis of $A + x$. Hence, $\dim J' = r_{\mathrm{cl}}(A)$ and J' is a basis for A, as was required to be shown.
Finally, we show that if $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(A + x) = r_{\mathrm{cl}}(A + y)$, then $r_{\mathrm{cl}}(A + x + y) = r_{\mathrm{cl}}(A)$. We need only show this for $\dim(A + x + y) = \dim(A) + 2$ as the other cases clearly hold. Suppose $r_{\mathrm{cl}}(A) = r_{\mathrm{cl}}(A + x) = r_{\mathrm{cl}}(A + y)$. Then by the proof of (R2'), A, $A + x$ and $A + y$ have a common basis $I \subseteq A$. Apply Lemma 54 to $A + x$ and $A + y$: this gives that $A + x + y$ has a basis contained in $I + I = I$. Hence $r_{\mathrm{cl}}(A + x + y) \leq r_{\mathrm{cl}}(A + x) = r_{\mathrm{cl}}(A + y)$ and by (R2'), equality holds. This proves (R3'). □

Corollary 56. *Let* cl *be a closure function and let r_{cl} be defined as in Definition 50. Then (E, r_{cl}) is a q-matroid with closure function $\mathrm{cl}_{r_{\mathrm{cl}}} = \mathrm{cl}$. Conversely, if (E, r) is a q-matroid, then (E, cl_r) is a closure function and $r = r_{\mathrm{cl}_r}$.*

Proof. It is proven in [9, Theorem 68] that if (E, r) is a q-matroid, then (E, cl_r) is a closure function. From Theorem 55 we know that if (E, cl) is a closure function, then (E, r_{cl}) is a q-matroid with rank function as in Definition 50. The only thing that remains to be proved is that rank and closure compose correctly, namely $\mathrm{cl} \to r \to \mathrm{cl}'$ implies $\mathrm{cl} = \mathrm{cl}'$ and $r \to \mathrm{cl} \to r'$ implies $r = r'$. The first of these compositions was proven in Corollary 49. For the second composition, given a rank function r, define $\mathrm{cl}_r(A)$ as in Definition 5. Then let $r'(A) = r_{\mathrm{cl}_r}(A) = \min\{\dim(I) : \mathrm{cl}_r(I) = \mathrm{cl}_r(A), I \subseteq A\}$. Let $J \subseteq A$ be such that $r(A) = \dim(J) = r(J)$. We know that J has minimal dimension with this property. Then $J \subseteq \mathrm{cl}_r(A)$ and $\mathrm{cl}_r(J) = \mathrm{cl}_r(A)$ by Lemma 34. So by minimality of J, $r'(A) = \dim(J) = r(A)$. □

8. Flats and Hyperplanes

In this section, we prove the cryptomorphism relating flats and hyperplanes. We start with assuming a collection of flats and deriving a collection of hyperplanes.

Definition 57. Let $(E, \mathcal{F})$ be a collection of flats. We define a collection of subspaces of E by

$$\mathcal{H}_{\mathcal{F}} := \{H \in \mathcal{F} : \nexists H' \in \mathcal{F} \text{ such that } H \subsetneq H' \subsetneq E \text{ and } H \neq E\}.$$

Our first aim is to prove that $\mathcal{H}_{\mathcal{F}}$ is a collection of hyperplanes. We first recall the following result from [4, Section 3].

Proposition 58. *The members of a collection of flats form a semimodular lattice under inclusion, where for any two flats F_1 and F_2 the meet is defined to be $F_1 \wedge F_2 := F_1 \cap F_2$ and the join $F_1 \vee F_2$ is the smallest flat containing $F_1 + F_2$. This implies that the lattice of flats satisfies the Jordan-Dedekind property, that is: all maximal chains between two fixed elements of the lattice have the same finite length.*

We will show some partial results that we use in the proofs of Theorem 62 and Corollary 70.

Lemma 59. *Let $F \in \mathcal{F}$. Then $F \notin \mathcal{H}_{\mathcal{F}}$ if and only if F has at least two covers in $\mathcal{F}$.*

Proof. It follows directly from the definition that if $H \in \mathcal{H}_{\mathcal{F}}$, then is has only the cover E, since E is the maximal element in the lattice of flats. For the other direction, suppose that $F \in \mathcal{F}$ has only one cover. By axiom (F3) there is a unique cover of F for every $x \notin F$ that contains x. If there is only one cover, this cover needs to contain all $x \subseteq E$, $x \notin F$, as well as F itself. This means the one cover of F is E, and hence $F \in \mathcal{H}_{\mathcal{F}}$. □

Proposition 60. *Let $F \in \mathcal{F}$. Then F is the intersection of all $H \in \mathcal{H}_{\mathcal{F}}$ such that $F \subseteq H$.*

Proof. We follow the proof for the classical case as given in [7, Proposition 2.56]. For every $F \in \mathcal{F}$, let $F = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_n = E$ be a maximal chain between F and E. The length of a maximal chain is well defined by Proposition 58 and we denote this length it by $n(F)$. (This is in fact the **corank** or **nullity** of F.) We proceed by induction on $n(F)$.
If $n(F) = 0$, then $F = E$ and it is the intersection of an empty subset of $\mathcal{H}_{\mathcal{F}}$. If $n = 1$, then $F \in \mathcal{H}_{\mathcal{F}}$. Now let $F \in \mathcal{F}$ with $n(F) = k+1$, $k \geq 1$ and assume that every flat with $n(F) \leq k$ is the intersection of the members of $\mathcal{H}_{\mathcal{F}}$ containing it. Let $I \subseteq \mathcal{H}_{\mathcal{F}}$ be the collection of members of $\mathcal{H}_{\mathcal{F}}$ containing F. Clearly $F \subseteq \bigcap_{H \in I} H$. We will prove the other inclusion by contradiction.

Suppose there is a 1-dimensional $x \subseteq E$ such that $x \subseteq H$ for all $H \in I$ and $x \notin F$. Because F is not in $\mathcal{H}_{\mathcal{F}}$, it has at least two covers by Lemma 59. Since x is contained in a unique cover of F by axiom (F3), there is a cover F' of F that does not contain x. Let $J \subseteq \mathcal{H}_{\mathcal{F}}$ be the members of $\mathcal{H}_{\mathcal{F}}$ that contain F'. Then $J \subseteq I$, because every member of $\mathcal{H}_{\mathcal{F}}$ that contains F' contains $F \subseteq F'$ as well. Clearly, $n(F') = k$, so by the induction hypothesis, $F' = \bigcap_{H \in J} H$. Since $x \notin F'$, there is an $H \in J$ such that $x \notin H$. But this is a contradiction of the fact that x is contained in all members of I and $J \subseteq I$. We conclude that $F \subseteq \bigcap_{H \in I} H$ and hence equality holds. □

The above shows that the lattice of flats is co-atomic. We point out the next direct consequence of the proof of Proposition 60.

Lemma 61. *Let $F \in \mathcal{F}$ and $F \neq E$. Then there exists an $H \in \mathcal{H}_{\mathcal{F}}$ containing F.*

Now we can conclude the first part of our goal, the cryptomorphism from flats to hyperplanes.

Theorem 62. *Let $(E, \mathcal{F})$ be a collection of flats and define a collection $\mathcal{H}_{\mathcal{F}}$ as in Definition 57. Then $(E, \mathcal{H}_{\mathcal{F}})$ is a collection of hyperplanes.*

Proof. We will show that $\mathcal{H}_{\mathcal{F}}$ satisfies the axioms (H1), (H2), (H3). By definition, E is not contained in $\mathcal{H}_{\mathcal{F}}$, which proves (H1). For (H2), let $H_1, H_2 \in \mathcal{H}_{\mathcal{F}}$ satisfy $H_1 \subseteq H_2$. Towards a contradiction, assume $H_1 \subsetneq H_2$. Since $E \notin \mathcal{H}_{\mathcal{F}}$ by (H1) and $H_2 \in \mathcal{H}_{\mathcal{F}}$ by assumption, we have that $H_2 \neq E$. So for H_1, we have $H_1 \subsetneq H_2 \subsetneq E$ and therefore $H_1 \notin \mathcal{H}_{\mathcal{F}}$. This is a contradiction, so $H_1 = H_2$.
Now we will prove (H3). Consider two distinct members H_1, H_2 of $\mathcal{H}_{\mathcal{F}}$ and a 1-dimensional subspace

$x \in \mathcal{L}(E)$. We need to find an $H_3 \in \mathcal{H}_\mathcal{F}$ such that $(H_1 \cap H_2) + x \subseteq H_3$. By construction of $\mathcal{H}_\mathcal{F}$ we have that $H_1, H_2 \in \mathcal{F}$ and so by (F2), $F := H_1 \cap H_2 \in \mathcal{F}$. If $x \subseteq F$, then $F + x = F$ and this is contained in some $H_3 \in \mathcal{H}_\mathcal{F}$ by Lemma 61. If $x \nsubseteq F$,, then by (F3) there is a unique $F' \in \mathcal{F}$ covering F and containing x. Since F' is a flat, again by Lemma 61 it is contained in some $H_3 \in \mathcal{H}_\mathcal{F}$. This proves that $H_3 \in \mathcal{H}_\mathcal{F}$ satisfies (H3). □

Conversely, we will start with a collection of hyperplanes and show that this collection determines a collection of flats.

Definition 63. Let $(E, \mathcal{H})$ be a collection of hyperplanes. Define a collection of subspaces of E:

$$\mathcal{F}_\mathcal{H} := \left\{ \bigcap \mathcal{H}' : \mathcal{H}' \subseteq \mathcal{H} \right\}.$$

We will prove that $\mathcal{F}_\mathcal{H}$ satisfies axioms (F1)-(F3), having proved some preliminary results. Until stated otherwise, we will assume that $\mathcal{H}$ is a collection of hyperplanes.

Lemma 64. *Let $\mathcal{H}', \mathcal{H}'' \subseteq \mathcal{H}$. Suppose $\mathcal{H}' \subseteq \mathcal{H}''$ and let $F_1 := \bigcap \mathcal{H}'$ and $F_2 := \bigcap \mathcal{H}''$. Then $F_2 \subseteq F_1$.*

Proof. By construction, we have that

$$F_2 = \bigcap \mathcal{H}'' = \left(\bigcap \mathcal{H}' \right) \cap \left(\bigcap (\mathcal{H}'' \setminus \mathcal{H}') \right) = F_1 \cap \left(\bigcap (\mathcal{H}'' \setminus \mathcal{H}') \right)$$

and thus $F_2 \subseteq F_1$. □

Lemma 65. *Let $F_1, F_2 \in \mathcal{F}_\mathcal{H}$ with $F_2 \subseteq F_1$. Let $\mathcal{H}' \subseteq \mathcal{H}$ be such that $F_1 = \bigcap \mathcal{H}'$. Then there is a $\mathcal{H}'' \subseteq \mathcal{H}$ such that $F_2 = \bigcap \mathcal{H}''$ and $I \subseteq J$.*

Proof. Let $\mathcal{H}''$ be the subset of $\mathcal{H}$ such that $F_2 \subseteq H$ for all $H \in \mathcal{H}''$. Since all the elements of $\mathcal{H}$ containing F_1 form a subset of all elements of $\mathcal{H}$ containing F_2, and $\mathcal{H}'$ is a subset of all elements of $\mathcal{H}$ containing F_1, we have that $\mathcal{H}' \subseteq \mathcal{H}''$. □

Proposition 66. *Let $F_1, F_2 \in \mathcal{F}_\mathcal{H}$ where F_1 is a cover of F_2 in $\mathcal{F}_\mathcal{H}$. Then there is an $H \in \mathcal{H}$ such that $F_2 = F_1 \cap H$.*

Proof. Let $\mathcal{H}'$ be the set of all elements of $\mathcal{H}$ containing F_1 so we can write $F_1 = \bigcap \mathcal{H}'$. By Lemma 65 there is a $\mathcal{H}''$ such that $F_2 = \bigcap \mathcal{H}''$ and $\mathcal{H}' \subseteq \mathcal{H}''$. Because $\mathcal{H}'$ contains all the members of $\mathcal{H}$ containing F_1 and $F_2 \subsetneq F_1$, $\mathcal{H}'$ is a proper subset of $\mathcal{H}''$. Let H be a member of $\mathcal{H}'' \backslash \mathcal{H}'$ and let $F' = F_1 \cap H$. Then $F' \subsetneq F_1$ because H does not contain F_1. Write $\mathcal{H}''' = \mathcal{H}' \cup \{H\}$, so $F' = \bigcap \mathcal{H}'''$. By Lemma 64 we have that $F_2 \subseteq F'$. Combining gives that $F_2 \subseteq F' \subsetneq F_1$. But $F_2 \subseteq F_1$ is a cover, so $F_2 = F'$ and thus $F_2 = F_1 \cap H$. □

Note that the converse of this statement is not true: if $F_1 \cap H = F_2$, then F_1 need not cover F_2. The following example illustrates this.

Example 67. Let us consider $E = (\mathbb{F}_2)^5$ and denote by e_i, $1 \leq i \leq 5$ the element in the canonical basis of E with 1 in position i and zeroes in all the other positions. Consider the uniform q-matroid $U_{4,5}(\mathbb{F}_2)$ of rank 4 on E (see [9, Example 4]). Clearly all 3-subspaces are hyperplanes. If we consider $F_1 = \langle e_1, e_2, e_3 \rangle$ this is then a hyperplane and so also a flat. Take then $H_1 = \langle e_2, e_3, e_4 \rangle$ and $H_2 = \langle e_2, e_4, e_5 \rangle$. Let $F' := F_1 \cap H_1$ and $F_2 := F_1 \cap H_2$. Then we have $F_2 \subsetneq F' \subsetneq F_1$ and the number of hyperplanes over F_2 is one more the number of hyperplanes over F_1. Therefore $F_1 \neq F_2$ and F_1 is not a cover of F_2. ♢

In the next lemma we use the hyperplane axiom (H3'). Recall that in Theorem 32 it is proven that the axioms (H1), (H2), (H3') are an equivalent set of axioms for a collection of hyperplanes.

Lemma 68. *Let $F \in \mathcal{F}_{\mathcal{H}}$ and let $\mathcal{H}'' \subseteq \mathcal{H}$ be the set of elements of $\mathcal{H}$ containing F. Let x be a 1-dimensional space not contained in F. Let $\mathcal{H}' \subseteq \mathcal{H}''$ be the set of all elements of $\mathcal{H}''$ containing x. For each $H' \in \mathcal{H}'' \setminus \mathcal{H}'$, let $F' = (\bigcap \mathcal{H}') \cap H'$. Then $F' = F$.*

Proof. Suppose by contradiction that there is $H' \in \mathcal{H}'' \setminus \mathcal{H}'$, with $F' \neq F$. In particular $F' \supsetneq F$ and there should be a y, $\dim(y) = 1$, such that $y \nsubseteq F$ but $y \subseteq F'$. Since $F' = (\bigcap \mathcal{H}') \cap H'$, then $y \subseteq H$ for each $H \in \mathcal{H}'$ and $y \subseteq H'$. For H', then, we know that does not contain x but it contains y. All the H contain y too. But y is not in F so there is some $H_u \in \mathcal{H}'' \setminus \mathcal{H}'$ such that $y \nsubseteq H_u$. Consider H and H_u. We know that $x \nsubseteq H', H_u$ and $y \subseteq H'$, $y \nsubseteq H_u$. By (H3') there is a hyperplane $\overline{H}$ containing $(H_u \cap H') + x$, but $y \nsubseteq \overline{H}$. Therefore $\overline{H}$ contains F and x so it should be an element of $\mathcal{H}'$, contradicting that all elements of $\mathcal{H}'$ contain y. □

After all this ground work, we can now prove the cryptomorphism from hyperplanes to flats.

Theorem 69. *Let $(E, \mathcal{H})$ be a collection of hyperplanes and define a collection $\mathcal{F}_{\mathcal{H}}$ as in Definition 63. Then $(E, \mathcal{F}_{\mathcal{H}})$ is a collection of flats.*

Proof. We will prove that $\mathcal{F}_{\mathcal{H}}$ satisfies the flat axioms (F1),(F2),(F3). E is a flat since it is the empty intersection of hyperplanes, hence (F1) holds. Let $F_1 := \bigcap \mathcal{H}'$ and $F_2 := \bigcap \mathcal{H}''$ two elements in $\mathcal{F}_{\mathcal{H}}$. Then $F_1 \cap F_2 = \bigcap_{H \in \mathcal{H}' \cup \mathcal{H}''} H$ and so $F_1 \cap F_2 \in \mathcal{F}$. This proves (F2).
Now we come to (F3). We have a flat $F \in \mathcal{F}_{\mathcal{H}}$ and $x \notin F$. We want to prove the existence of a unique F' which contains x and covers F. We take $\mathcal{H}''$, the set of all hyperplanes containing F and we consider the intersection F' of all the hyperplanes in $\mathcal{H}''$ which also contain x. Now we can use the Lemma 68 to see that such a flat is a cover: being $x \notin F$ there is also an element of $\mathcal{H}''$ not containing x but for all of them the intersection is F.
The uniqueness of the flat covering F and containing x can be easily proved by contradiction.
Suppose there is another flat F'' covering F and containing x. Then, by (F2), $F''' := F' \cap F''$ is a flat, which obviously contains F and x and it is contained in F' and F''. This contradicts the fact that F' covers F. We therefore conclude that F' is unique. This completes the proof of (F3). □

Corollary 70. *Let $(E, \mathcal{F})$ be a collection of flats and let $(E, \mathcal{H})$ be a collection of hyperplanes.*

(1) $(E, \mathcal{F})$ determines a q-matroid with collection of flats $\mathcal{F}$ and collection of hyperplanes $\mathcal{H}_{\mathcal{F}}$.
(2) $(E, \mathcal{H})$ determines a q-matroid with collection of hyperplanes $\mathcal{H}$ and collection of flats $\mathcal{F}_{\mathcal{H}}$.

Proof. To prove (1), we show that $\mathcal{F}_{\mathcal{H}_{\mathcal{F}}} = \mathcal{F}$. Let $F \in \mathcal{F}$. We have to prove that $F \in \mathcal{F}_{\mathcal{H}_{\mathcal{F}}}$. From Proposition 60 we know that F is the intersection of all members of $\mathcal{H}_{\mathcal{F}}$ containing F. This intersection is in $\mathcal{F}_{\mathcal{H}_{\mathcal{F}}}$ by definition, so $F \in \mathcal{F}_{\mathcal{H}_{\mathcal{F}}}$.

For the other inclusion, start with $F \in \mathcal{F}_{\mathcal{H}_{\mathcal{F}}}$. We can find a finite chain $F \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_k \subsetneq E$ of flats of $\mathcal{F}_{\mathcal{H}_{\mathcal{F}}}$ by using axiom (F3) multiple times. By Proposition 66 we can find a hyperplane $H_1 \in \mathcal{H}_{\mathcal{F}}$ such that $F = F_1 \cap H_1$. In the same way we find $H_i \in \mathcal{H}_{\mathcal{F}}$ such that $F_{i-1} = F_i \cap H_i$ for all $1 \leq i \leq k$. This gives that $F = \bigcap_{i \in \{1,\ldots,k\}} H_i$, a finite intersection. By applying the axiom (F2) multiple (but a finite number of) times, we get that $F \in \mathcal{F}$. This shows $\mathcal{F}_{\mathcal{H}_{\mathcal{F}}} \subseteq \mathcal{F}$ and hence equality holds.
To show $\mathcal{H}_{\mathcal{F}_{\mathcal{H}}} = \mathcal{H}$ for part (2), let $H \in \mathcal{H}$ and let $I = \{H\} \subseteq \mathcal{H}$. Then $H = \bigcap_{H' \in I} H'$ hence $H \in \mathcal{F}_{\mathcal{H}}$. We need to show that $H \in \mathcal{H}_{\mathcal{F}_{\mathcal{H}}}$. This is the case if there is no flat in $\mathcal{F}_{\mathcal{H}}$ that covers H and is not equal to E. This is impossible, since H is the intersection of only one hyperplane. Therefore, $\mathcal{H} \subseteq \mathcal{H}_{\mathcal{F}_{\mathcal{H}}}$. Now suppose that $H \in \mathcal{H}_{\mathcal{F}_{\mathcal{H}}}$. Then H is a maximal element of $\mathcal{F}_{\mathcal{H}} = \{\bigcap_{H \in I} : I \subseteq \mathcal{H}\}$. But then in particular, $H \in \mathcal{H}$. It follows that $\mathcal{H}_{\mathcal{F}_{\mathcal{H}}} = \mathcal{H}$.
We know from Theorem 48 that $(E, \mathcal{F})$ determines a q-matroid with $r = r_{\mathcal{F}}$ and $\mathcal{F} = \mathcal{F}_{r_{\mathcal{F}}}$. It

follows from the above that also $(E, \mathcal{H})$ defines a q-matroid with $\mathcal{H} = \mathcal{H}_{\mathcal{F}_r}$. It follows directly from Definition 6 that $\mathcal{H}_{\mathcal{F}_r} = \mathcal{H}_r$. Hence we have a q-matroid in both parts (1) and (2). □

9. Dependence and Independence

We now establish that the independence axioms and the dependence axioms are cryptomorphic. It is worth noting at this point that while we require the four axioms (I1)-(I4) in order to define a q-matroid, the three dependence axioms (D1)-(D3) are sufficient.

Theorem 71. *Let $(E, \mathcal{I})$ be a collection of independent spaces. Let $\mathcal{D} = \text{opp}(\mathcal{I})$. Then $\mathcal{D}$ is a collection of dependent spaces.*

Proof. By (I1), $\mathcal{I}$ is non-empty. Let $I \in \mathcal{I}$. Then $0 \in \mathcal{I}$ by (I2), so $0 \notin \mathcal{D}$ and (D1) holds. Let $D_1 \in \mathcal{D}$ and let $D_1 \subseteq D_2 \in \mathcal{L}(E)$. Then $D_2 \notin \mathcal{I}$ by (I2), so (D2) holds.

Now let $D_1, D_2 \in \mathcal{D}$ such that $D_1 \cap D_2 \in \mathcal{I}$. By Lemma 27, there exist $I_1 \in \max(D_1, \mathcal{I})$ and $I_2 \in \max(D_2, \mathcal{I})$ such that $D_1 \cap D_2 \subseteq I_1, I_2$ and clearly $I_i \subseteq D_i$ for $i = 1, 2$. Then we have $D_1 \cap D_2 = I_1 \cap I_2$. Moreover, $\dim(I_1) \leq \dim(D_1) - 1$ and $\dim(I_2) \leq \dim(D_2) - 1$ since $I_i \notin \mathcal{D}$ for $i = 1, 2$.

Let $D \subseteq D_1 + D_2$ have codimension one in $D_1 + D_2$. Suppose now, towards a contradiction, that $D \in \mathcal{I}$. By (I4), $D_1 + D_2$ has a maximal independent subspace V contained in $I_1 + I_2$, which, by maximality, satisfies $\dim(V) \geq \dim(D) = \dim(D_1 + D_2) - 1$. Therefore, $\dim(D_1 + D_2) - 1 \leq \dim(V) \leq \dim(D_1 + D_2) - 1$, and so $\dim(D_1 + D_2) - 1 = \dim(V) \leq \dim(I_1 + I_2)$. We have

$$\begin{aligned}
\dim(D_1 + D_2) - 1 &\leq \dim(I_1 + I_2), \\
&= \dim(I_1) + \dim(I_2) - \dim(I_1 \cap I_2), \\
&\leq \dim(D_1) + \dim(D_2) - \dim(D_1 \cap D_2) - 2, \\
&= \dim(D_1 + D_2) - 2,
\end{aligned}$$

yielding the required contradiction. It follows that (D3) holds. □

Theorem 72. *Let $(E, \mathcal{D})$ be a collection of dependent spaces. Let $\mathcal{I} = \text{opp}(\mathcal{D})$. Then $\mathcal{I}$ is a family of independent spaces.*

Proof. Since $\{0\} \notin \mathcal{D}$, $\{0\} \in \mathcal{I}$ and so (I1) holds. If $J \in \mathcal{I}$ and $I \subseteq J$, then from (D2) it must be the case that $I \in \mathcal{I}$, so (I2) holds.

Now let $I, J \in \mathcal{I}$ such that $\dim(I) < \dim(J)$. We will apply induction on $\dim(I/(I \cap J))$. If $\dim(I/(I \cap J)) = 0$, then $I \subseteq J$ and so clearly (I3) holds for the pair I, J. Now let k be a non-negative integer and suppose that (I3) holds for all subspaces $U, V \in \mathcal{I}$ satisfying $\dim(V) > \dim(U)$ and $\dim(U/(U \cap V)) \leq k$. Suppose that $\dim(I/(I \cap J)) = k+1$. We claim that there exists $x \subseteq J, x \notin I$ such that $x + I \in \mathcal{I}$.

Let I_1 be a subspace of codimension one in I that contains $I \cap J$. Then $I_1 \cap J = I \cap J$, $\dim(J) > \dim(I_1)$ and by (I2), $I_1 \in \mathcal{I}$. Since

$$\dim(I_1/(I_1 \cap J)) = \dim(I_1) - \dim(I_1 \cap J) = \dim(I) - 1 - \dim(I \cap J) = k,$$

by the induction hypothesis (I3) holds for the pair I_1, J; that is, there exists a 1-dimensional space $a \subseteq J, a \notin I_1$ such that $I_2 = a + I_1 \in \mathcal{I}$. We have $a \subseteq J, a \notin I_1$ and so $a \notin I_1 \cap J = I \cap J$. Clearly, $\dim(I_2) = \dim(I)$. We have $I_2 \cap J = (a + I_1) \cap J = a + (I_1 \cap J) = a + (I \cap J)$, and $a \notin I \cap J$, so $\dim(I_2 \cap J) = \dim(I \cap J) + 1$. Therefore,

$$\dim(I_2/(I_2 \cap J)) = \dim(I_2) - \dim(I_2 \cap J) = \dim(I) - \dim(I \cap J) - 1 = k,$$

hence again by hypothesis, there exists a 1-dimensional space $b \subseteq J$, $b \notin I_2$ such that $I_3 = b + I_2 \in \mathcal{I}$. Clearly, $a \notin I$. Also, $b \subseteq J, b \notin I_2$ and since $a + (I \cap J) = I_2 \cap J$, it follows that $b \notin a + I$. Therefore, $a+I \neq b+I$ and so we have $(a+I) \cap (b+I) = I \in \mathcal{I}$. If both $a+I, b+I \in \mathcal{D}$, then by (D3) every subspace of codimension 1 in $a+b+I$ is dependent. Now $\dim(a+b+I) = \dim(I)+2$ and $\dim(I_3) = \dim(I_1)+2$,

so $\operatorname{codim}_{a+b+I}(I_3) = 1$, so in particular this implies that $I_3 \in \mathcal{D}$, which contradicts $I_3 \in \mathcal{I}$. We deduce that at least one of $a + I$ or $b + I$ is in $\mathcal{I}$. This establishes (I3).

Let A be a subspace of E and let $x \in \mathcal{L}(E)$ be a 1-dimensional space. Let $I \in \max(A, \mathcal{I})$. We claim that there exists a member of $\max(x + A, \mathcal{I})$ contained in $x + I$. This will prove that (I4) holds, by Lemma 26. If $A = I$, then any subspace of $x + A$ is a subspace of $x + I$, so the result holds. Suppose then that $I \subsetneq A$. If $x \subseteq A$, then $\max(x + A, \mathcal{I}) = \max(A, \mathcal{I})$ and so I is the required member of $\max(x + A, \mathcal{I})$ contained $x + I$. Therefore, for the remainder we assume that $x \nsubseteq A$.

Let $M \in \max(x + A, \mathcal{I})$. By Lemma 27, we may choose M such that $I \subseteq M$. If $M = I$, then I gives the required subspace in $\max(x + A, \mathcal{I})$, so assume that $I \subsetneq M$, i.e. that $\dim(M) > \dim(I)$. In particular, this means that $M \nsubseteq A$, by the maximality of I in A. Furthermore, $y + I \notin \mathcal{I}$ for any 1-dimensional space $y \subseteq A, y \nsubseteq I$.

By Lemma 28, $\dim(M) = \dim(I) + 1$ and so $M = m + I$ for some 1-dimensional space $m \nsubseteq A$.

If $x \subseteq M$, then as $x \nsubseteq I$ and since $\operatorname{codim}_M(I) = 1$, we have $M = m + I = x + I$ and M gives the subspace satisfying (I4), so suppose that $x \nsubseteq M$. If $x + I \in \mathcal{I}$, then $x + I \in \max(x + A, \mathcal{I})$, so suppose otherwise, i.e. that $x + I \in \mathcal{D}$. We have $m + I \in \max(x + A, \mathcal{I})$ and $m \subseteq x + A$, $m \nsubseteq A$. Therefore, $m = \langle \bar{x} + \bar{a} \rangle$ for $x = \langle \bar{x} \rangle$ and a 1-dimensional subspace $a = \langle \bar{a} \rangle \subseteq A$. By the maximality of I in A, $a + I \in \mathcal{D}$. Now $(x + I) \cap (a + I) = I \in \mathcal{I}$, since $x \nsubseteq A$ and I has codimension 1 in both $a + I$ and $x + I$. Then by (D3), every subspace of codimension 1 in $a + x + I$ is a member of $\mathcal{D}$. But as $m + I \subseteq x + a + I$ is independent, by assumption, and as it has codimension 1 in $x + a + I$, we arrive at a contradiction. We deduce that $\dim(M) = \dim(I)$ and so (I4) holds. □

Corollary 73. *Let $(E, \mathcal{I})$ be a collection of independent spaces and let $(E, \mathcal{D})$ be a collection of dependent spaces. Suppose that $\mathcal{D} = \operatorname{opp}(\mathcal{I})$. Then $(E, \mathcal{I})$ and $(E, \mathcal{D})$ each determine the same q-matroid (E, r) such that $\mathcal{D}$ is the collection $\mathcal{D}_r$ of dependent spaces of (E, r) and $\mathcal{I}$ is the collection of independent spaces $\mathcal{I}_r$ of (E, r).*

Proof. By [9, Theorem 8], $(E, \mathcal{I})$ determines a q-matroid (E, r) such that $\mathcal{I} = \mathcal{I}_r$. Since $\mathcal{D} = \operatorname{opp}(\mathcal{I})$, we have $D \in \mathcal{D}$ if and only if $D \notin \mathcal{I}_r$ and in particular $\mathcal{D}$ must be the set of dependent spaces of (E, r). □

10. Dependent Spaces and Circuits

Recall that for a collection of subspaces $\mathcal{S}$ of E that $\min(\mathcal{S}) = \{A \in \mathcal{S} : B \nsubseteq A, \text{ any } B \in \mathcal{S}, A \neq B\}$.

Lemma 74. *Let $(E, \mathcal{D})$ be a collection of dependent spaces. Let $\mathcal{C} = \min(\mathcal{D})$. Then $(E, \mathcal{C})$ is a collection of circuits of E.*

Proof. Since $\mathcal{C} = \min(\mathcal{D})$, we have $\mathcal{C} \subseteq \mathcal{D}$. Therefore, $\{0\} \notin \mathcal{C}$ by (D1), which gives (C1). Let $C_1, C_2 \in \mathcal{C}$ such that $C_1 \subseteq C_2$. By the definition of $\min(\mathcal{D})$, C_1 is not properly contained in any other member of $\mathcal{C}$. It follows that $C_1 = C_2$ so that (C2) holds.

Now let $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$ we claim that every space of codimension 1 in $C_1 + C_2$ contains a circuit. Since $C_1 \neq C_2$, we have $C_1 \cap C_2 \subsetneq C_1, C_2$, therefore, by (C2) we have $C_1 \cap C_2 \notin \mathcal{C}$ and in particular is not a dependent space. Then by (D3), there is a space $D \in \mathcal{D}$ of codimension 1 in $C_1 + C_2$. Let $C_3 \in \mathcal{D}$ be a subspace of D such that no member of $\mathcal{D}$ is contained in C_3. Such a space clearly exists since E has finite dimension. Then $C_3 \in \min(\mathcal{D}) = \mathcal{C}$ and so (C3) holds. □

Lemma 75. *Let $(E, \mathcal{C})$ be a collection of circuits. Let $\mathcal{D} = \operatorname{upp}(\mathcal{C})$. Then $(E, \mathcal{D})$ is a collection of dependent subspaces of E.*

Proof. By (C1), $\{0\} \notin \mathcal{C}$ and so in particular $\{0\} \notin \mathcal{D}$ and so (D1) holds. If $D_1 \subseteq D_2$ and $D_1 \in \mathcal{D}$, then there exists $C \in \mathcal{C}$ contained in D_1, by the definition of $\operatorname{upp}(\mathcal{D})$, and so $C \subseteq D_2$ which gives $D_2 \in \mathcal{D}$. This shows that (D2) holds. Now let $D_1, D_2 \in \mathcal{D}$ such that $D_1 \cap D_2 \notin \mathcal{D}$. Let H be a subspace of codimension 1 in E. We claim that $(D_1 + D_2) \cap H \in \mathcal{D}$.

There is no circuit contained in $D_1 \cap D_2$ by definition of $\mathrm{upp}(\mathcal{C})$. Let C_1 and C_2 be circuits contained in D_1 and D_2, respectively. We have $C_1 \neq C_2$, since otherwise $D_1 \cap D_2$ contains a circuit.

By (C3), there exitst a circuit $C_3 \subseteq (C_1 + C_2) \cap H$. Then clearly $(D_1 + D_2) \cap H \in \mathcal{D}$, since $C_3 \subseteq (C_1 + C_2) \cap H \subseteq (D_1 + D_2) \cap H$ implies $(D_1 + D_2) \cap H \in \mathrm{upp}(\mathcal{C}) = \mathcal{D}$. □

Corollary 76. *Let $(E, \mathcal{D})$ be a collection of dependent spaces and let $(E, \mathcal{C})$ be a collection of circuits such that $\mathcal{D} = \mathrm{upp}(\mathcal{C})$. Then $(E, \mathcal{D})$ and $(E, \mathcal{C})$ both each determine a q-matroid (E, r) whose collection of dependent spaces is $\mathcal{D}$ and whose collection of circuits is $\mathcal{C}$.*

Proof. By Corollary 73, $(E, \mathcal{D})$ determines a q-matroid whose dependent spaces comprise $\mathcal{D}$. The result now follows since $\mathcal{C} = \min(\mathcal{D})$. □

11. Hyperplanes and (Co)circuits

We will prove a cryptomorphism between cocircuits and hyperplanes, implying a cryptomorphism between hyperplanes and circuits. We call $\mathcal{C}^*$ the family of **cocircuits** of a q-matroid.

Theorem 77. *Let $\mathcal{C}^*$ and $\mathcal{H}$ be two families of subspaces of E such that $\mathcal{C}^* = \mathcal{H}^\perp$. Then $(E, \mathcal{H})$ is a collection of hyperplanes if and only if $(E, \mathcal{C}^*)$ is a collection of circuits.*

Proof. Suppose $\mathcal{H}$ is a collection of hyperplanes, so it satisfies the hyperplane axioms. Since $\mathcal{C}^* = \mathcal{H}^\perp$, we get that $\mathcal{C}^*$ satisfies the circuit axioms by taking orthogonal complements in all the hyperplane axioms. Since $(\mathcal{H}^\perp)^\perp = \mathcal{H}$, we get the other implication by taking orthogonal complements again. □

Remark 78. Recall that in Theorem 32 we proved that the axioms (H1), (H2), (H3) are equivalent to the axioms (H1), (H2), (H3'). From the theorem above it follows that the axioms (C1), (C2), (C3) are equivalent to the axioms (C1), (C2), (C3'), with (C3') equal to the following:

(C3') For distinct $C_1, C_2 \in \mathcal{C}$ and any $X, Y \in \mathcal{L}(E)$ of codimension 1 with $X \not\supseteq C_1, C_2$, $Y \supseteq C_1$, $Y \not\supseteq C_2$, there is a circuit $C_3 \subseteq \mathcal{C}$ such that $C_3 \subseteq (C_1 + C_2) \cap X$ and $Y \not\supseteq C_3$.

Corollary 79. *Let $(E, \mathcal{H})$ be a collection of hyperplanes and let $(E, \mathcal{C}^*)$ be a collection of circuits such that $\mathcal{C}^* = \mathcal{H}^\perp$. Then $(E, \mathcal{H})$ and $(E, \mathcal{C}^*)$ both each determine a q-matroid (E, r) whose collection of hyperplanes is $\mathcal{H}$ and whose collection of cocircuits is $\mathcal{C}^*$.*

Proof. By Corollary 70, $(E, \mathcal{H})$ determines a q-matroid whose hyperplanes comprise $\mathcal{H}$. The result now follows since $\mathcal{C}^* = \mathcal{H}^\perp$. □

As the result above suggest, cocircuits are closely related to circuits. This is made precise by the results below. First we prove a small lemma.

Lemma 80. *A hyperplane is a maximal space with respect to not containing a basis.*

Proof. A hyperplane H has rank $r(M) - 1$ and is rank-maximal because it is a flat. This means that for all 1-dimensional spaces $x \not\subseteq H$ we have that $r(H + x) = r(H) + 1 = r(M)$ and thus $H + x$ contains a basis. □

Proposition 81. *The circuits of the matroid M are the cocircuits of the dual matroid M^*.*

Proof. We follow Proposition 3.18 of [7]. We use that for subspaces if $A \subseteq B$, then $B^\perp \subseteq A^\perp$. The following are equivalent (see Theorem 21 and Lemma 80):

$$
\begin{aligned}
C \text{ is a circuit of } M &\Leftrightarrow C \text{ is a minimal dependent space in } M \\
&\Leftrightarrow C \text{ is minimal with respect to not being contained in any basis } B \text{ of } M \\
&\Leftrightarrow C^\perp \text{ is maximal with respect to not containing any } B^\perp \\
&\Leftrightarrow C^\perp \text{ is maximal with respect to not containing a basis } B^\perp \text{ of } M^* \\
&\Leftrightarrow C^\perp \text{ is a hyperplane of } M^* \\
&\Leftrightarrow C \text{ is a cocircuit of } M^*
\end{aligned}
$$

□

From this proposition it follows directly that the circuits of a q-matroid are a collection of circuits.

Corollary 82. *Let $(E, \mathcal{C}^*)$ be the collection of cocircuits of a q-matroid M. Then $(E, \mathcal{C})$ is the collection of circuits of M^*.*

Remark 83. In [9, Theorem 64] the following statement, which is a variation on (C3), is proven for a q-matroid:

$\overline{\text{(C3)}}$ For distinct $C_1, C_2 \in \mathcal{C}$ and any 1-dimensional subspace $x \subseteq C_1 \cap C_2$, there is a circuit $C_3 \subseteq \mathcal{C}$ such that $C_3 \subseteq C_1 + C_2$ and $x \nsubseteq C_3$.

This is, at first sight, a more straightforward q-analogue of the axiom for classical matroids. For classical matroids, the two statements are equivalent, but we will see that for q-matroids they are not. We will see a similar issue with the axiom (O3) for open spaces in Remark 89.

However, $\overline{\text{(C3)}}$ is a weaker version of the axiom (C3) we have proven above, as we will show. Let C_1, C_2 be distinct circuits and let x be a 1-dimensional space contained in $C_1 \cap C_2$. Then there is a space $X \in \mathcal{L}(E)$ of codimension 1 that intersects trivially with x. Apply (C3) to C_1, C_2 and X: this gives a circuits $C_3 \subseteq (C_1 + C_2) \cap X$. This is clearly a circuit contained in $C_1 + C_2$ that does not contain x. So (C3) implies $\overline{\text{(C3)}}$. The implication does not go the other way: it can be that $C_1, C_2 \nsubseteq X$ but $C_1 \cap C_2 \subseteq X$. In that case, the statement above does not imply the existence of a circuit $C_3 \subseteq (C_1 + C_2) \cap X$. We illustrate this in the next example.

Example 84 (Example 10 of [9])**.** Let $E = \mathbb{F}_2^4$ and let $I \in \mathcal{L}(E)$ be the subspace given by

$$I = \left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle.$$

Let $\mathcal{I}$ be the family of subspaces of E that contains I and all subspaces of I. As is pointed out in [9], $\mathcal{I}$ satisfies the independence axioms (I1)-(I3) but not (I4). Let $\mathcal{C}_\mathcal{I} = \min(\text{opp}(\mathcal{I}))$, that is, the family of 'circuits' implied by $\mathcal{I}$. Let us examine $\mathcal{C}_\mathcal{I}$. It contains all 1-dimensional subspaces of E that are not in I; we call them *loops*. Any 4- and 3-dimensional subspace of E contains a loop, hence none of these is a member of $\mathcal{C}_\mathcal{I}$. Every 2-dimensional subspaces of E either contains a loop, or is equal to I, so none of these is a member of $\mathcal{C}_\mathcal{I}$. Hence $\mathcal{C}_\mathcal{I}$ only contains loops.

It is clear that $\mathcal{C}_\mathcal{I}$ satisfies the circuits axioms (C1) and (C2). Since all pairs of members of $\mathcal{C}_\mathcal{I}$ intersect trivially, $\mathcal{C}_\mathcal{I}$ satisfies $\overline{\text{(C3)}}$ as well. This shows that (C1), (C2) ,$\overline{\text{(C3)}}$ can not be a full axiom system for a q-matroid, as was also noted in the discussion after [9, Theorem 64].

The family of subspaces $\mathcal{C}_\mathcal{I}$ does not satisfy the axiom (C3): for a counter example, take $C_1 = \langle 1100 \rangle$, $C_2 = \langle 0011 \rangle$ and $X = \langle 1001 \rangle^\perp$. Then $(C_1 + C_2) \cap X = \langle 1111 \rangle$ and this does not contain a member of $\mathcal{C}_\mathcal{I}$. This shows that (C3) is a stronger axiom than $\overline{\text{(C3)}}$.

12. Open Spaces and Flats

In this section, we discuss the axiomatic definition of open spaces and prove the cryptomorphism between open spaces and flats. We follow the same approach as in the previous section and call $\mathcal{O}^*$ the family of **co-open spaces** of a q-matroid.

Theorem 85. *Let $\mathcal{O}^*$ and $\mathcal{F}$ be two families of subspaces of E such that $\mathcal{O}^* = \mathcal{F}^\perp$. Then $(E, \mathcal{F})$ is a collection of flats if and only if $(E, \mathcal{O}^*)$ is a collection of open spaces.*

Proof. Suppose $(E, \mathcal{F})$ is a collection of flats, so that it satisfies the flat axioms. Since $\mathcal{O}^* = \mathcal{F}^\perp$, we get that $\mathcal{O}^*$ satisfies the open space axioms by taking orthogonal complements in all the flat axioms. Since $(\mathcal{F}^\perp)^\perp = \mathcal{F}$, we get the other implication by taking orthogonal complements again. □

The fact that a collection of co-open spaces determines q-matroid is the content of the following corollary.

Corollary 86. *Let $(E, \mathcal{O}^*)$ be a collection of open spaces and let $(E, \mathcal{F})$ be a collection of flats. Suppose that $\mathcal{O}^* = \mathcal{F}^\perp$. Then both $(E, \mathcal{O}^*)$ and $(E, \mathcal{F})$ each determine the same q-matroid (E, r) such that $\mathcal{O}^*$ is the collection of co-open spaces of (E, r) and $\mathcal{F}$ is the collection of flats of (E, r).*

Proof. By Theorem 48, $(E, \mathcal{F})$ is a q-matroid whose family of flats is equal to $\mathcal{F}$. The result now follows since $\mathcal{O}^* = \mathcal{F}^\perp$. □

As with cocircuits and circuits, co-open spaces are open spaces of the dual q-matroid.

Proposition 87. *The flats of a q-matroid $M = (E, r)$ are the orthogonal spaces of the open spaces of the dual q-matroid M^*.*

Proof. In [4], it was proved that the lattice of flats is semimodular with the meet of two flats F_1, F_2 defined to be $F_1 \wedge F_2 := F_1 \cap F_2$ and the join $F_1 \vee F_2$ is defined to be the minimal flat containing $F_1 + F_2$, which is $\mathrm{cl}_r(F_1 + F_2)$. The maximal flats of M are the hyperplanes.
Dualizing to co-open sets, we have an *anti-isomorphism* and we have a semimodular lattice of open spaces, where, if $O_1, O_2 \in \mathcal{O}$, $O_1 \wedge O_2 = O_1 + O_2$, while their meet is the maximal subspace contained in their intersection. Since the orthogonal complements of hyperplanes are cocircuits, it follows that every co-open space is the sum of cocircuits. By Proposition 81, cocircuits are circuits in M^*, hence sums of cocircuits are sums of circuits in M^* and these are by definition open spaces. □

From this proposition it follows directly that the open spaces of a q-matroid are a collection of open spaces.

Corollary 88. *Let $(E, \mathcal{O}^*)$ be a collection of co-open spaces of a q-matroid M. Then $(E, \mathcal{O})$ is the collection of open spaces of M^*.*

Remark 89. Consider the following open *set* axioms for classical matroids, for a collection $\mathcal{O}$ of subsets of some ground set S of finite cardinality n.

(O1) The empty set is a member of $\mathcal{O}$.
(O2) If $O_1, O_2 \in \mathcal{O}$, then $O_1 \cup O_2 \in \mathcal{O}$.
(O3) For each $O \in \mathcal{O}$ and each subset $X \subset S$ of cardinality $n-1$ such that $O \nsubseteq X$, there exists a unique set $O' \in \mathcal{O}$, such that $O' \subseteq X \cap O$ and O' is covered by O in $\mathcal{O}$.
($\overline{\text{O3}}$) For each $O \in \mathcal{O}$, if $O_1, \ldots, O_k \in \mathcal{O}$ are all the sets in $\mathcal{O}$ covered by O in $\mathcal{O}$, then $\bigcap_{i=1}^k O_i = \varnothing$.

The direct q-analogue of the axioms (O1)-(O3) given above are given by the open spaces axioms of Definition 11, while the axioms (O1), (O2) and ($\overline{\text{O3}}$) are the usual classical open space axioms. In fact, as we now show, the open set axioms (O1), (O2), (O3), are equivalent to (O1), (O2), ($\overline{\text{O3}}$).
Let M be a matroid with ground set S of size n and let $\mathcal{O}$ be a collection of subsets of S.
(O3) $\Rightarrow$ ($\overline{\text{O3}}$): Assume that (O3) holds. Let $O \in \mathcal{O}$ and let $O_1, \ldots, O_k$ be all the open sets covered by O in $\mathcal{O}$. Suppose that $\bigcap_{i=1}^k O_i$ is non-empty and so contains some element h. Let $X' = S \setminus \{h\}$. By (O3), there exists a unique open set $O' \subseteq X' \cap O = O \setminus \{h\}$ that is covered by O in $\mathcal{O}$. By construction, this set O' does not contain h, which contradicts the assumption that h is contained in the intersection of all such sets.
($\overline{\text{O3}}$) $\Rightarrow$ (O3): Now assume that ($\overline{\text{O3}}$) holds. Let $O \in \mathcal{O}$ and let X be a subset of S of cardinality $n-1$ such that $O \nsubseteq X$. Then $S = X \cup \{h\}$ for some $h \in S$. Now suppose, towards a contradiction, that there is no subset of $X \cap O$ that is covered by O in $\mathcal{O}$. Then in particular, there no such set contained in X, so all sets covered by O in $\mathcal{O}$ contain h. However, this contradicts ($\overline{\text{O3}}$), which we have assumed by hypothesis. We deduce that (O3) holds.

A direct q-analogue of ($\overline{\text{O3}}$) is given by the following for a collection $\mathcal{O}$ of subspaces of E.

($\overline{\text{O3}}$) For each $O \in \mathcal{O}$, if $O_1, \ldots, O_k \in \mathcal{O}$ are all the subspaces in $\mathcal{O}$ covered by O in $\mathcal{O}$, then $\bigcap_{i=1}^k O_i = \{0\}$.

However, even though (O3) and ($\overline{\text{O3}}$) are equivalent in the classical case, this cannot be said of their q-analogues, as the following example shows.

Example 90. We give an easy counterexample, coming from the q-matroid M_6^*, namely the dual of M_6 from Example 23. By dualizing the flats in Table 1, we see that the open spaces of the q-matroid M_6^* are $0, \mathbb{F}_2^6$ and the orthogonal complements of $G_1, \dots, G_9$, namely $G_1^\perp, \dots, G_9^\perp$.

It can be easily observed that the set $L_{O'} = \{\{0\}, G_1^\perp, \dots, G_8^\perp, \mathbb{F}_2^6\}$, which is the set of open spaces of M_6 excluding $G_9^\perp$, satisfies (O1), (O2), and ($\overline{\text{O3}}$), as we now show. Clearly, $\{0\} \in L_{O'}$. Since the $G_1^\perp, \dots, G_8^\perp$ all have trivial pairwise intersections, their pairwise vector-space sums are all equal to $\mathbb{F}_2^6$ and clearly the sum of any member $L_{O'}$ with $\{0\}$ or $\mathbb{F}_2^6$ is contained in $L_{O'}$ so that (O2) holds. Also ($\overline{\text{O3}}$) holds; the only nontrivial case to consider is that involving the open spaces covered by $\mathbb{F}_2^6$, which are $G_1^\perp, \dots, G_8^\perp$ and have trivial intersection. We will now show that $L_{O'}$ does not satisfy (O3). Let $O = \mathbb{F}_2^6$ and let $X := G_9^\perp + \langle (1,0,0,1,0,0), (1,0,0,0,0,1) \rangle$. Then X has codimension 1 in $\mathbb{F}_2^6$ and clearly $X \cap O = X$. The only space in $L_{O'}$ in X that is not covered by O is the zero space and in particular, it is not true that there is a unique open space covered by O in $X \cap O = X$. Therefore (O3) fails for the collection $L_{O'}$.

13. Spanning and Non-spanning Spaces

In this short section, we discuss spanning and non-spanning spaces. We follow the same approach as the previous two sections. Therefore we prove the duality between independent and spanning spaces between and dependent and non-spanning spaces.

Proposition 91. *The orthogonal complements of the independent spaces of M are the spanning spaces of M^*.*

Proof. By definition, an independent space I has $r(I) = \dim(I)$. Applying the dual rank function to $I^\perp$ and E gives that

$$\begin{aligned} r^*(I^\perp) &= \dim(I^\perp) - r(E) + r(I) \\ &= \dim(E) - \dim(I) - r(E) + \dim(I) \\ &= \dim(E) - r(E) \\ &= r^*(E) \end{aligned}$$

and this is exactly saying that $I^\perp$ is a spanning space of M^*. □

In a similar fashion as the previous two sections, we can now prove that $\mathcal{S}^* = \mathcal{I}^\perp$ is a collection of spanning spaces, and in combination with the proposition above we arrive at the following.

Corollary 92. *Let $(E, \mathcal{S})$ be a collection of spanning spaces and let $(E, \mathcal{I})$ be a collection of independent spaces. Suppose that $\mathcal{S}^\perp = \mathcal{I}$. Then both $(E, \mathcal{S})$ and $(E, \mathcal{I})$ each determine the same q-matroid (E, r) such that $\mathcal{S}$ is the collection of spanning spaces of (E, r) and $\mathcal{I}$ is the collection of independent spaces of (E, r).*

We can repeat the very same reasoning for non-spanning spaces. In particular, spanning sets should be substituted by non-spanning spaces and independent spaces should be replaced by dependent spaces. We get then the following.

Proposition 93. *The orthogonal complements of the dependent spaces of M are the non-spanning spaces of M^*.*

Proof. Let $\mathcal{N}^*$ be the non-spanning spaces of M^*. Then $\text{opp}(\mathcal{N}^*) = \mathcal{S}^*$ are the spanning spaces of M^*. By Proposition 91, these are the orthogonal complements of the independent spaces of M. The result now follows because $\mathcal{I} = \text{opp}(\mathcal{D})$. See also Figure 2. □

Corollary 94. *Let $(E, \mathcal{N})$ be a collection of non-spanning spaces and let $(E, \mathcal{D})$ be a collection of dependent spaces. Suppose that $\mathcal{N}^\perp = \mathcal{D}$. Then both $(E, \mathcal{N})$ and $(E, \mathcal{D})$ each determine the same q-matroid (E, r) such that $\mathcal{N}$ is the collection of non-spanning spaces of (E, r) and $\mathcal{D}$ is the collection of dependent spaces of (E, r).*

14. Acknowledgements

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).
The authors are grateful to Heide Gluesing-Luerssen and the anonymous reviewers for their comments on earlier versions of the paper, that lead to various improvements.

References

[1] G. Bollen, H. Crapo, and R. Jurrius. The Tutte q-Polynomial. https://arxiv.org/abs/1707.03459, 2017.
[2] T. Britz, A. Mammoliti, and K. Shiromoto. Wei-type duality theorems for rank-metric codes. *Designs, Codes, and Cryptography*, 88:1503–1519, 2020.
[3] T. Brylawski. Appendix of matroid cryptosystems. In *Theory of Matroids*, volume 26 of *Encyclopedia of Mathematics and its Application*, pages 389–496. Cambridge University Press, 1986.
[4] E. Byrne, M. Ceria, S. Ionica, R. Jurrius, and E. Saçıkara. Constructions of new matroids and designs over $\mathbb{F}_q$, https://arXiv.org/abs/2005.03369v3. 2021.
[5] H. Crapo. *On the theory of combinatorial independence*. PhD thesis, M.I.T., 1964.
[6] S. R. Ghorpade and T. Johnsen. A polymatroid approach to generalized weights of rank metric codes. *Designs, Codes and Cryptography*, 88(12):2531–2546, 2020.
[7] G. Gordon and J. McNulty. *Matroids, a Geometric Introduction*. Cambridge University Press, 2012.
[8] E. Gorla, R. Jurrius, H. H. López, and A. Ravagnani. Rank-metric codes and q-polymatroids. *Journal of Algebraic Combinatorics*, 52:1–19, 2020.
[9] R. Jurrius and R. Pellikaan. Defining the q-analogue of a matroid. *Electronic Journal of Combinatorics*, 25(3):P3.2, 2018.
[10] R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.
[11] G. Nicoletti and W. N. Axiom systems. In *Theory of Matroids*, volume 26 of *Encyclopedia of Mathematics and its Application*, pages 389–496. Cambridge University Press, 1986.
[12] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non Desarguesiane. *Annali di Matematica Pura ed Applicata*, 64:1–76, 1964.
[13] K. Shiromoto. Codes with the rank metric and matroids. *Designs, Codes and Cryptography*, 87(8):1765–1776, 2019.

Appendix A. A summary of relations

In this section we summarize all known relations between various notions associated to q-matroids. Some follow directly from a cryptomorphism, others are either direct or proven elsewhere.

(1) **Independent spaces in terms of**
   (a) Bases: all bases and all their subspaces;
   (b) Rank: subspaces of E whose rank equals the dimension;
   (c) Circuits: all proper subspaces;
   (d) Closure: subspaces I of E whose codimension-1 subspaces have the same closure as I;
   (e) Spanning spaces: orthogonal complements of spanning spaces of the dual q-matroid;
   (f) Dependent spaces: all spaces that are not dependent;
   (g) Bi-colouring: all coverings downwards from the subspace are red.

(2) **Rank function in terms of**
   (a) Independent spaces: maximal dimension of independent subspaces of the given space

(b) Closure: maximal dimension of all subspaces whose closure equals the closure of the given space;
(c) Bi-colourings: number of red coverings in a chain from $\{0\}$ to the given subspace.

(3) **Circuits in terms of**
(a) Independent spaces: spaces that are not independent and whose proper subspaces are all independent;
(b) Dependent spaces: minimal dependent spaces;
(c) Hyperplanes: orthogonal complements of hyperplanes of the dual q-matroid.

(4) **Bases in terms of**
(a) Independent spaces: maximal independent spaces;
(b) Rank: minimal spaces B such that $r(B) = r(M)$;
(c) Bi-colouring: all coverings downwards from the subspace are red and all coverings upwards from the subspace are green.

(5) **Spanning spaces in terms of**
(a) Independent spaces: orthogonal complement of independent spaces of the dual q-matroid;
(b) Rank: subspaces S such that $r(S) = r(M)$;
(c) Bi-colouring: all coverings upward from the subspace green.

(6) **Dependent spaces in terms of**
(a) Independent spaces: all spaces that are not independent;
(b) Rank: subspaces D such that $r(D) > \dim D$;
(c) Circuits: all subspaces containing a circuit;
(d) Non-spanning spaces: orthogonal complements of non-spanning spaces of the dual q-matroid.

(7) **Hyperplanes in terms of**
(a) Rank: maximal spaces with $r(H) = r(M)$;
(b) Bases: maximal space with respect to not containing a basis;
(c) Circuits: orthogonal complements of circuits of the dual q-matroid;
(d) Flats: maximal proper flats.

(8) **Non-spanning spaces in terms of**
(a) Spanning spaces: all spaces that are not spanning spaces;
(b) Dependent spaces: orthogonal complements of dependent spaces of the dual q-matroid.

(9) **Closure in terms of**
(a) Flats: intersection of all flats containing the given space.
(b) Bi-colouring: maximal subspace of $\mathcal{L}(E)$ that can be reached from the given subspace going upwards using only green coverings.

(10) **Flats in terms of**
(a) Closure: a space equal to its own closure;
(b) Rank: spaces whose rank increases by one by adding any 1-dimensional space not already in the given space;
(c) Hyperplanes: intersections of hyperplanes;
(d) Open Spaces: orthogonal complements of open spaces in the dual q-matroid;
(e) Bi-colouring: all coverings upwards from the subspace are red.

(11) **Open spaces in terms of**
(a) Circuits: sums of circuits;
(b) Flats: orthogonal complements of flats in the dual q-matroid.

(12) **Bi-colourings in terms of**
(a) Rank: green if the rank does not increase, red otherwise.

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

Faculty of Military Science, Netherlands Defence Academy, The Netherlands
Email address: rpmj.jurrius@mindef.nl