Designs, Codes and Cryptography (2023) 91:451–473
https://doi.org/10.1007/s10623-022-01087-3

Constructions of new matroids and designs over $\mathbb{F}_q$

Eimear Byrne[1] · Michela Ceria[2] · Sorina Ionica[3] · Relinde Jurrius[4] · Elif Saçıkara[5]

Received: 23 September 2021 / Revised: 3 June 2022 / Accepted: 30 June 2022 /
Published online: 2 October 2022

Abstract
A perfect matroid design (PMD) is a matroid whose flats of the same rank all have the same size. In this paper we introduce the q-analogue of a PMD and its properties. In order to do so, we first establish a new cryptomorphic definition for q-matroids. We show that q-Steiner systems are examples of q-PMD's and we use this q-matroid structure to construct subspace designs from q-Steiner systems. We apply this construction to the only known q-Steiner system, which has parameters $S(2,3,13;2)$, and hence establish the existence of a new subspace design with parameters 2-(13, 4, 5115; 2).

Keyword Subspace design · q-Matroid · Cryptomorphism · Perfect matroid design

Mathematics Subject Classification 05B35 · 05A30 · 05B05

Communicated by M. Buratti.

✉ Eimear Byrne
ebyrne@ucd.ie

Michela Ceria
michela.ceria@poliba.it

Sorina Ionica
sorina.ionica@u-picardie.fr

Relinde Jurrius
rpmj.jurrius@mindef.nl

Elif Saçıkara
elif.sacikara@math.uzh.ch

[1] School of Mathematics and Statistics, University College Dublin, D4, Dublin, Ireland

[2] Department of Mechanics, Mathematics and Management, Politecnico di Bari, Via Orabona 4, 70125 Bari, Italy

[3] Laboratoire MIS, Université de Picardie Jules Verne, 33 rue Saint Leu, 80000 Amiens, France

[4] Faculty of Military Sciences, Netherlands Defence Academy, Den Helder, Netherlands

[5] Institute of Mathematics, University of Zürich, Zürich, Switzerland

1 Introduction

In combinatorics, we often describe a q-analogue of a concept or theory to be any generalization that replaces finite sets by finite dimensional vector spaces. Two classical topics in combinatorics that have recently been studied as q-analogues are matroids and designs. These objects and some of the connections between them are the main focus of this paper.

A subspace design (also called a q-design, or a design over $\mathbb{F}_q$) is a q-analogue of a design. A t-$(n, k, \lambda; q)$ subspace design is a collection $\mathcal{B}$ of k-dimensional subspaces of an n-dimensional $\mathbb{F}_q$-vector space V with the property that every t-dimensional subspace of V is contained in exactly λ of the members of $\mathcal{B}$. Explicit constructions of subspace designs have proved so far to be more elusive than their classical counterparts. Early papers by Thomas, Suzuki, and Itoh have provided some examples of infinite families of subspace designs [17, 28, 29], while in [6] an approach to the problem using *large sets* is given. A q-analogue of the Assmus–Mattson theorem gives a general construction of subspace designs from coding theory [12]. Further sporadic examples have been found by assuming a prescribed automorphism group of the subspace design [8]. For the special case $\lambda = 1$ we call such a design a q-Steiner system and write $S(t, k, n; q)$. The actual existence of an $S(t, k, n; q)$ Steiner system for $t > 1$, was established for the first time when $S(2, 3, 13; 2)$ designs were discovered by Braun et al. [4]. No other examples have been found to date. The smallest open case is that of the $S(2, 3, 7; q)$ Steiner system, also known as the q-analogue of the Fano plane.

While subspace designs have been intensively studied over the last decade [8], q-analogues of matroids have more recently appeared in the literature [16, 18]. In fact, the q-matroid defined in [18] was a re-discovery of a combinatorial object already studied by Crapo [13]. Classical matroids are a generalisation of several ideas in combinatorics, such as independence in vector spaces and trees in graph theory. One of the important properties of matroids is that there are equivalent, yet seemingly different ways to define them: in terms of their independent sets, flats, circuits, bases, closure operator and rank function. We call these equivalent definitions *cryptomorphisms*. Cryptomorphisms for q-matroids between independent subspaces, the rank function, and bases were established in [18]. In [2] the cryptomorphism via bi-colouring of the subspace lattice is discussed. In [11] several cryptomorphisms were shown to hold, namely those with respect to dependent spaces, circuits, the closure function, hyperplanes, open spaces etc. In this paper we also give a cryptomorphic description of a q-matroid in terms of its flats. In the classical case, there is a link between designs and matroids, given by the so-called *perfect matroid designs* (PMDs). PMDs are matroids for which flats of the same rank have the same cardinality. They were studied by Murty and others in [23] and [22], who showed in particular that Steiner systems are among the few examples of PMDs and, more importantly, that they could be applied to construct new designs. In this paper we obtain q-analogues of some of these results.

First, we extend the theory of q-matroids to include a new cryptomorphism, namely that between flats and the rank function. We apply this cryptomorphism to obtain the first examples of q-PMDs; in particular we show that q-Steiner systems are q-PMDs. Secondly, using the q-matroid structure of the q-Steiner system, we derive new subspace designs. This leads in some cases to designs with parameters not previously known. Interestingly, some of the parameters of the designs we obtain from the putative q-Fano plane coincide with those obtained by Braun et al. [5]. By characterising the group of automorphisms of the designs that we obtained from our q-PMD construction, we show that the subspace designs of [5] cannot be derived from the q-Fano plane via our construction.

This paper is organised as follows. After some preliminary notions in Sect. 2, we prove in Sect. 3 the above-mentioned new cryptomorphism for q-matroids. An overview of the different (but equivalent) ways to define q-matroids is found at the end of this section. In Sect. 4 we prove that q-Steiner systems are examples of the q-analogue of a PMD. We use this to derive new designs from the q-Steiner system, using its q-matroid structure and its flats, independent spaces, and circuits. Finally, we characterize the automorphism groups of these new q-designs in terms of the automorphisms of q-Steiner systems from which they are constructed.

2 Preliminaries

In this section, we bring together certain fundamental definitions on lattices, q-matroids and subspace designs, respectively. Throughout the paper, $\mathbb{F}_q$ will denote the finite field of q elements, n will be a fixed positive integer and E will denote the n-dimensional vector space $\mathbb{F}_q^n$.

2.1 Lattices

Let us first recall preliminaries on lattices. The reader is referred to Stanley [25] or Aigner [1] for further details.

Definition 2.1 Let $(\mathcal{L}, \leq)$ be a partially ordered set. Let $a, b, v \in \mathcal{L}$. We say that v is an **upper bound** of a and b if $a \leq v$ and $b \leq v$ and furthermore, we say that v is a **least upper bound** if $v \leq u$ for any $u \in \mathcal{L}$ that is also an upper bound of a and b. If a least upper bound of a and b exists, then it is unique, is denoted by $a \vee b$ and called the **join** of a and b. We analogously define **a lower bound** and **the greatest lower bound** of a and b and denote the unique greatest lower bound of a and b by $a \wedge b$, which is called the **meet** of a and b. The poset $\mathcal{L}$ is called a **lattice** if each pair of elements has a least upper bound and greatest lower bound and denoted by $(\mathcal{L}, \leq, \vee, \wedge)$.

Of particular relevance to this paper is the subspace lattice $(\mathcal{L}(E), \leq, \vee, \wedge)$, which is the lattice of $\mathbb{F}_q$-subspaces of E, ordered with respect to inclusion and for which the join of a pair of subspaces is their vector space sum and the meet of a pair of subspaces is their intersection. That is, for all subspaces $A, B \subseteq E$ we have:

$$A \leq B \Leftrightarrow A \subseteq B, \quad A \vee B = A + B, \quad A \wedge B = A \cap B.$$

Definition 2.2 Let $(\mathcal{L}, \leq, \vee, \wedge)$ be a lattice and let $a, b \in \mathcal{L}$ with $a \leq b$ but $a \neq b$, we say that b **covers** a if for all $c \in \mathcal{L}$ we have that $a \leq c \leq b$ implies that $c = a$ or $c = b$. A **chain** of length r between two elements $a, b \in \mathcal{L}$ is a sequence of distinct elements $a_0, a_1, \ldots, a_r$ in $\mathcal{L}$ such that $a = a_0 \leq a_1 \leq \cdots \leq a_r = b$. If a_{i+1} covers a_i for all i, we call this a **maximal chain**.

Definition 2.3 Let $(\mathcal{L}, \leq, \vee, \wedge)$ be a finite lattice. We say that $\mathcal{L}$ is a **semimodular lattice** if it has the property that if a covers $a \wedge b$ then $a \vee b$ covers b.

Definition 2.4 A lattice $\mathcal{L}$ is called **geometric** if it is

(1) atomic (every element is a supremum of the elements covering the unique minimal),
(2) semimodular,

(3) without infinite chains.

Definition 2.5 A bijection $\phi : \mathcal{L} \to \mathcal{L}$ on a lattice $(\mathcal{L}, \leq, \vee, \wedge)$ is called an **automorphism** of $\mathcal{L}$ if one of the following equivalent conditions holds for all $a, b \in \mathcal{L}$:

(1) $a \leq b$ iff $\phi(a) \leq \phi(b)$,
(2) $\phi(a \vee b) = \phi(a) \vee \phi(b)$,
(3) $\phi(a \wedge b) = \phi(a) \wedge \phi(b)$.

2.2 *q*-Matroids

The general framework of defining matroid-like structures over modular complemented lattices is treated in [13]. Important examples of complemented modular lattices are the Boolean lattice, resulting in classical matroids, and the subspace lattice, leading to q-matroids.

For background on the theory of matroids we refer the reader to [15] or [24]. For the q-analogue of a matroid we follow the treatment of Jurrius and Pellikaan [18]. The definition of a q-matroid is a straightforward generalisation of the definition of a classical matroid in terms of its rank function. We remark that this definition in fact does not require E to be over a finite field. However, as we are focussed on vector spaces over finite fields, we will assume in our definition that a q-matroid is an object defined with respect to an $\mathbb{F}_q$-vector space.

Definition 2.6 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 $A \subseteq E$, $0 \leq r(A) \leq \dim A$.
(R2) For all subspaces $A \subseteq B \subseteq E$, $r(A) \leq r(B)$.
(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.

We list some examples of q-matroids [18].

Example 2.7 [The uniform q-matroid] Let $M = (E, r)$, where

$$r(A) = \begin{cases} \dim A, & \text{if } \dim A \leq k, \\ k, & \text{if } \dim A > k, \end{cases}$$

for $0 \leq k \leq n$ and a subspace A of E. Then M satisfies axioms (R1)–(R3) and is called the uniform q-matroid. We denote it by $U_{k,n}(\mathbb{F}_q)$.

Example 2.8 [Representable q-matroid] Let G be a full-rank $k \times n$ matrix over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. For any subspace $A \subseteq E$ define the rank of A to be $r(A) = \text{rank}_{\mathbb{F}_{q^m}}(GY)$ for any $\mathbb{F}_q$-matrix Y whose columns span A. It can be shown that (E, r) satisfies (R1)–(R3) and hence is a q-matroid.

In classical matroid theory, there are several definitions of a matroid in terms of the axioms of its independent spaces, bases, flats, circuits, etc. These equivalences, which are not immediately apparent, are referred to in the literature as *cryptomorphisms*. In this paper we will establish a new cryptomorphism for q-matroids. First, we define independent spaces, flats, and the closure function in terms of the rank function of a q-matroid.

Definition 2.9 Let (E, r) be a q-matroid. A subspace A of E is called **independent** if

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

We write $\mathcal{I}_r$ to denote the set of independent spaces of the q-matroid (E, r). A subspace that is not independent is called **dependent**. We call C a **circuit** if it is itself a dependent space and every proper subspace of C is independent.

Definition 2.10 Given a q-matroid (E, r), a subspace $F \subseteq E$ is called a **flat** if for all one-dimensional subspaces x such that $x \nsubseteq F$ we have that

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

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

We define the notion of a flat via axioms, without reference to a rank function.

Definition 2.11 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 $x \subseteq E$ a one-dimensional subspace not contained in F, there is a unique $F' \in \mathcal{F}$ covering F such that $x \subseteq F'$.

If $\mathcal{F}$ satisfies (F1)–(F3) then we call its members **flats**. We write $(E, \mathcal{F})$ to denote a vector space E together with a family of flats satisfying the flat axioms.

We will see in Sect. 3 that a space of flats $(E, \mathcal{F})$ completely determines a q-matroid. The following theorem summarizes important results from [18].

Theorem 2.12 *Let (E, r) be a q-matroid and let $A, B \subseteq E$ and let $x, y \subseteq E$ each have dimension one. The following hold.*

1. $r(A + x) \leq r(A) + 1$.
2. *If $r(A+z) = r(A)$ for each one-dimensional space $z \subseteq B$, $z \nsubseteq A$ then $r(A+B) = r(A)$.*
3. *If $r(A + x) = r(A + y) = r(A)$ then $r(A + x + y) = r(A)$.*

An interesting family of matroids, the PMDs were introduced in [22, 23]. For more details in the classical case, we refer the reader to the work of Deza [14]. We consider here a q-analogue of a PMD.

Definition 2.13 A q-**perfect matroid design** (q-PMD) is a q-matroid with the property that any two of its flats of the same rank have the same dimension.

2.3 Subspace designs

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

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

We write $\begin{bmatrix} E \\ k \end{bmatrix}_q$ to denote the set of all k-subspaces of E (the k-Grassmannian of E). Recall the following well-known result.

Lemma 2.14 *Let s, t be positive integers satisfying $0 \leq t \leq s \leq n$. The number of s-spaces of E that contain a fixed t-space is given by $\begin{bmatrix} n-t \\ s-t \end{bmatrix}_q$.*

We recall briefly the definition of a subspace design and well known examples of these combinatorial objects. The interested reader is referred to the survey [8] and the references therein for a comprehensive treatment of designs over finite fields. For more recent results, see also [9, 10].

Definition 2.15 Let $1 \leq t \leq k \leq n$ be integers and let $\lambda \geq 0$ be an integer. A t-$(n, k, \lambda; q)$ **subspace design** is a pair $(E, \mathcal{B})$, where $\mathcal{B}$ is a collection of subspaces of E of dimension k, called blocks, with the property that every subspace of E of dimension t is contained in exactly λ blocks.

Subspace designs are also known as designs over finite fields. A q-**Steiner system** is a t-$(n, k, 1; q)$ subspace design and is said to have parameters $S(t, k, n; q)$. The q-Steiner triple systems are those with parameters $S(2, 3, n; q)$ and are denoted by $STS(n; q)$. The t-$(n, k, \lambda; q)$ subspace designs with $t = 1$ and $\lambda = 1$ are examples of spreads.

Example 2.16 A q-analogue of the Fano plane would be given by an $STS(7; q)$, whose existence is an open question for any q.

For a subspace U of E we define $U^{\perp}:=\{v \in E : \langle u, v\rangle = 0\}$ to be the orthogonal space of U with respect to the scalar product $\langle u, v\rangle = \sum_{i=1}^{n} u_i v_i$. We will use the notions of the supplementary and dual subspace designs [20, 27].

Definition 2.17 Let k, t, λ be positive integers and let $\mathcal{D} = (E, \mathcal{B})$ be a t-$(n, k, \lambda; q)$ design.

(1) The **supplementary design** of $\mathcal{D}$ is the subspace design $\left(E, \begin{bmatrix} E \\ k \end{bmatrix}_q - \mathcal{B}\right)$.

It has parameters t-$\left(n, k, \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q - \lambda; q\right)$.

(2) The **dual design** of $\mathcal{D}$ is given by $(E, \mathcal{B}^{\perp})$, where $\mathcal{B}^{\perp}:=\{U^{\perp} : U \in \mathcal{B}\}$. It has parameters

$$t - \left(n, n-k, \lambda \begin{bmatrix} n-t \\ k \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1}; q\right).$$

The *intersection numbers* $\lambda_{i,j}$ defined in Lemma 2.18 were given in [20] and [27]. These design invariants play an important role in establishing non-existence of a design for a given set of parameters.

Lemma 2.18 *Let k, t, λ be positive integers and let $\mathcal{D}$ be a t-$(n, k, \lambda; q)$ design. Let I, J be i, j dimensional subspaces of $\mathbb{F}_q^n$ satisfying $i + j \leq t$ and $I \cap J = \{0\}$. Then the number*

$$\lambda_{i,j}:=|\{U \in \mathcal{B} : I \subseteq U,\ J \cap U = \{0\}\}|,$$

where $\mathcal{B}$ is the set of blocks of $\mathcal{D}$, depends only on i and j, and is given by the formula

$$\lambda_{i,j} = q^{j(k-i)} \lambda \begin{bmatrix} n-i-j \\ k-i \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1}.$$

By Lemma 2.18, the existence of a t-$(n, k, \lambda; q)$ design implies the *integrality conditions*, namely that $\lambda_i = \lambda_{i,0}$ are positive integers for $0 \leq i \leq t$.

Definition 2.19 A parameter set t-$(n, k, \lambda; q)$ is called **admissible** if it satisfies the integrality conditions and is called **realisable** if a t-$(n, k, \lambda; q)$ design exists.

It is well-known and follows directly from the integrality conditions that an $STS(n; q)$ is admissible if and only if $n \equiv 1$ or $3 \mod 6$. More generally, it was observed in [10] that a $\mathcal{S}(2, k, n; q)$ Steiner system exists only if $n \equiv 1, k \mod k(k-1)$.

Finally, for a given subspace design $(E, \mathcal{B})$, an automorphism ϕ of $\mathcal{L}(E)$ is called an **automorphism of the design** if $\phi(\mathcal{B}) = \mathcal{B}$. We will denote the automorphism group of the design $\mathcal{D} = (E, \mathcal{B})$ by $\mathrm{Aut}(\mathcal{D})$ or by $\mathrm{Aut}(E, \mathcal{B})$. The automorphism group of a subspace design is equal to the automorphism group of its supplementary design and is in $1-1$ correspondence with that of the dual design. Automorphism groups have been leveraged to construct new subspace designs using the Kramer–Mesner method [21]. If the number of orbits of the automorphism group is small enough, then the corresponding diophantine system of equations can be solved in a feasible amount of time on a personal computer [3, 5]. It is known that the binary q-Fano plane has automorphism group of order at most 2 [7, 19], so this method cannot be applied in this case.

3 A cryptomorphism of *q*-matroids

In this section we provide a new cryptomorphic definition of a q-matroid, in terms of its flats. The proofs of this cryptomorphism largely follow the classical case. We include the details for expository purposes. Recall that a flat of a q-matroid (E, r) is a subspace F such that for all one-dimensional spaces $x \nsubseteq F$ we have that $r(F + x) > r(F)$. We remark that the results of this section hold for q-matroids defined with respect to finite dimensional vector spaces over arbitrary fields.

Definition 3.1 Let F_1 and F_2 be flats of a q-matroid. We say that F_1 **covers** F_2 if $F_2 \subseteq F_1$ and there is no other flat F' such that $F_2 \subseteq F' \subseteq F_1$.

Before establishing a cryptomorphism between the q-matroids (E, r) and $(E, \mathcal{F})$, we prove some preliminary results.

Lemma 3.2 *Let (E, r) be a q-matroid with rank function r. Let $A \subseteq B$ be subspaces of E and let x be a one-dimensional subspace of E. If $r(B+x) = r(B)+1$ then $r(A+x) = r(A)+1$.*

Proof Suppose that $r(B + x) = r(B) + 1$. Since $A \subseteq B$, we have $(A + x) + B = B + x$ and $A \subseteq (A + x) \cap B$. Therefore, by (R2) and applying (R3) to $A + x$ and B we get:

$$\begin{aligned} r(A + x) + r(B) &\geq r((A + x) + B) + r((A + x) \cap B) \\ &\geq r(B + x) + r(A) = r(B) + 1 + r(A), \end{aligned}$$

and so $r(A + x) \geq r(A) + 1$. By Theorem 2.12, $r(A + x) \leq r(A) + 1$ and so we get the equality $r(A + x) = r(A) + 1$. □

Lemma 3.3 *If F_1, F_2 are two flats of a q-matroid (E, r), then $F_1 \cap F_2$ is also a flat.*

Proof Let $F{:=}F_1 \cap F_2$ and take a one-dimensional space $x \nsubseteq F$; therefore x is not a subspace of F_1 or F_2; say, without loss of generality, that $x \nsubseteq F_1$. By Theorem 2.12, $r(F_1 + x) = r(F_1) + 1$ and by Lemma 3.2, $r(F + x) = r(F) + 1 > r(F)$, which implies that F is flat of (E, r). □

Definition 3.4 Let $\mathcal{F}$ be a collection of subspaces of E and let $A \subseteq E$ be a subspace. We define the subspace

$$C_{\mathcal{F}}(A) := \bigcap \{F \in \mathcal{F} : A \subseteq F\}.$$

Lemma 3.5 *Let $\mathcal{F}$ be a collection of subspaces of E satisfying the axioms* (F1)–(F3). *Let $A \subseteq E$ be a subspace. Then $C_{\mathcal{F}}(A)$ is the unique flat in $\mathcal{F}$ such that the following hold.*

(1) $A \subseteq C_{\mathcal{F}}(A)$.
(2) *If $A \subseteq F \in \mathcal{F}$, then $C_{\mathcal{F}}(A) \subseteq F$.*

Moreover, if $A \subseteq B \subseteq E$, then $C_{\mathcal{F}}(A) \subseteq C_{\mathcal{F}}(B)$.

Proof (1) and (2) follow immediately from the definition of $C_{\mathcal{F}}(A)$, which is clearly uniquely determined because if there were two flats satisfying these properties, their intersection would violate (2). If $B \subseteq F$ for some flat F then $A \subseteq F$ and so clearly, $C_{\mathcal{F}}(A) \subseteq C_{\mathcal{F}}(B)$. □

In the instance that $\mathcal{F}$ is the set of flats of a q-matroid (E, r), then from Lemma 3.3, $C_{\mathcal{F}}(A)$ is itself a flat, which we denote by F_A. In particular, F_A is the unique minimal flat of $\mathcal{F}_r$ that contains A.

Lemma 3.6 *Let (E, r) be a q-matroid, let G be a subspace of E and let x be a one-dimensional subspace such that $r(G) = r(G + x)$. Then $x \subseteq F_G$.*

Proof Suppose, towards a contradiction, that $x \nsubseteq F_G$. We apply (R3) to F_G and $G + x$:

$$r(F_G + G + x) + r(F_G \cap (G + x)) \leq r(F_G) + r(G + x).$$

Now since $G \subseteq F_G$ but $x \nsubseteq F_G$, the above inequality can be stated as

$$r(F_G + x) + r(G) \leq r(F_G) + r(G).$$

However, as F_G is a flat, $r(F_G + x) = r(F_G) + 1$, which gives the required contradiction. □

Lemma 3.7 *Let (E, r) be a q-matroid and let $G \subseteq E$. Then $r(G) = r(F_G)$.*

Proof Consider the collection of subspaces

$$\mathcal{H} := \{y \subseteq E : \dim(y) = 1, r(G + y) = r(G)\}.$$

Let U be the vector space sum of the elements of $\mathcal{H}$. By applying Theorem 2.12 Part 2, we have that $r(U) = r(G)$. Moreover, $U \subseteq F_G$ by Lemma 3.6.

Suppose $r(G) < r(F_G)$. If $U = F_G$ then we would arrive at the contradiction $r(U) = r(F_G) > r(G)$, so assume otherwise. Then there exists a one-dimensional subspace $x \subseteq F_G$, $x \nsubseteq U$. Since $x \notin \mathcal{H}$ and $G \subseteq U$, by (R2) we have

$$r(U) = r(G) < r(G + x) \leq r(U + x).$$

On the other hand, Lemma 3.6 tells us that for a one-dimensional subspace $x' \subseteq E$, $x' \nsubseteq F_G$ we have

$$r(U) = r(G) < r(G + x') \leq r(U + x').$$

Therefore U is itself a flat and $G \subseteq U \subsetneq F_G$, contradicting the minimality of F_G. We deduce that $r(G) = r(F_G)$. □

Proposition 3.8 *The flats of a q-matroid satisfy the flat axioms* (F1)–(F3) *of Definition* 2.11.

Proof Let (E, r) be a q-matroid with rank function r. By definition, the set of flats $\mathcal{F}_r$ of (E, r) is characterised by:

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

The condition (F1) holds vacuously, while (F2) comes from Lemma 3.3.

To prove (F3), let $F \subseteq E$ and $x \subseteq E$ with $\dim(x) = 1$ and $x \nsubseteq F$. We will show that there is a unique F' covering F and containing x. Suppose, towards a contradiction, that x is not contained in any flat covering F. Let $G = F + x$ and consider F_G, the minimal flat containing G. By our assumption, there must be a flat F' such that $F \subsetneq F' \subsetneq F_G$. Without loss of generality, we may assume that F' is a cover of F. Clearly $x \nsubseteq F'$. Let y be a one-dimensional space $y \subseteq F'$, $y \nsubseteq F$. Now, $x, y \nsubseteq F$ and $y \subseteq F_G$. Let $H = F + y$. We claim that $x \subseteq F_H$, in which case we would arrive at the contradiction $x \subseteq F_H \subseteq F'$ and $x \nsubseteq F'$. Since $G = F + x$, $H = F + y$, $x, y \nsubseteq F$ and F is a flat, we have $r(G) = r(H) = r(F) + 1$. By Lemma 3.7, $r(G) = r(F_G)$ and since $y \subseteq F_G$ we also have $r(G) = r(G + y) = r(F_G)$. Now,

$$r(H + x) = r(F + x + y) = r(G + y) = r(G) = r(F) + 1 = r(H).$$

Hence by Lemma 3.6, $x \subseteq F_H$. We deduce that x is contained in a cover of F. As regards uniqueness, suppose we have two different covers $F_1 \neq F_2$ of F containing x and let $L := F_1 \cap F_2$. By the flat axiom (F2), L is a flat and since $x, F \subseteq F_1, F_2$ then $x, F \subseteq L$. On the other hand, $F \neq L$ since $x \nsubseteq F$, so $F \subsetneq L$. Since $F_1 \neq F_2$, L cannot be equal to both of them; say $L \neq F_2$, so $F \subsetneq L \subsetneq F_2$, which contradicts the fact that F_2 covers L. □

Our aim is to prove the converse of Proposition 3.8: that is, if we have a collection of flats $\mathcal{F}$ that satisfies the axioms (F1)–(F3), it is the collection of flats of a q-matroid. The next lemma will be used frequently in our proofs.

Lemma 3.9 *Let $\mathcal{F}$ be a collection of flats. Let $F \in \mathcal{F}$ and let $x \subseteq E$ be a one-dimensional subspace. Then the minimal member of $\mathcal{F}$ containing $F + x$ is either equal to F or it covers F.*

Proof If $x \subseteq F$, then $F + x = F$ so the minimal member of $\mathcal{F}$ containing $F + x$ is F itself. If $x \nsubseteq F$, then by (F3) there is a unique $F' \in \mathcal{F}$ that covers F and contains x. Since F' covers F and contains both F and x, it is clearly the minimal member of $\mathcal{F}$ containing $F + x$. □

Next we show that the members of $\mathcal{F}$ form a semimodular lattice. (The flats of a q-matroid form in fact a geometric lattice, as was noted in Theorem 1 of [2].)

Theorem 3.10 *Let $\mathcal{F}$ be a collection of flats. Then its members form a semimodular lattice under inclusion, where for any two $F_1, F_2 \in \mathcal{F}$ 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 $C_{\mathcal{F}}(F_1 + F_2)$.*

Proof The members of $\mathcal{F}$ clearly form a poset with respect to inclusion. We prove that the definitions of meet and join as $F_1 \wedge F_2 := F_1 \cap F_2$ and $F_1 \vee F_2 := C_{\mathcal{F}}(F_1 + F_2)$ are well defined.

Let us consider the meet. From (F2) $F_1 \wedge F_2$ is in $\mathcal{F}$ and the fact that it is the greatest lower bound of F_1 and F_2 follows from the definition of intersection. As regards the join, $C_{\mathcal{F}}(F_1 + F_2)$ is in $\mathcal{F}$ by Lemma 3.5 and, more precisely, is the unique minimal member of $\mathcal{F}$ containing $F_1 + F_2$. We remark that, since we have a lattice, there is a maximal member of $\mathcal{F}$, which is E, and a minimal one, that is $\cap\{F \in \mathcal{F}\}$, which is also the minimal member of $\mathcal{F}$ containing the zero space.

In order to prove that the lattice is semimodular, we have to prove that if $F_1 \wedge F_2$ is covered by F_1, then F_2 is covered by $F_1 \vee F_2$. So let $F_1 \cap F_2 \in \mathcal{F}$ be covered by F_1. Then for all one-dimensional subspaces $x \subseteq F_1$ but $x \nsubseteq F_2$ we have that the minimal member of $\mathcal{F}$ containing $(F_1 \cap F_2) + x$ is F_1 by Lemma 3.9. Since $F_2 + x \subseteq F_2 + F_1$, we have that the minimal $H \in \mathcal{F}$ containing $F_2 + x$ satisfies $H \leq F_2 \vee F_1$. On the other hand, because $(F_1 \cap F_2) + x \subseteq F_2 + x$, we have that $F_1 \leq H$. Now we have that both $F_1, F_2 \leq H$ so H must contain the least upper bound of the two, that is, $H \geq F_1 \vee F_2$. We conclude that $H = F_1 \vee F_2$, which means $F_1 \vee F_2$ covers F_2 by Lemma 3.9. This proves that the lattice of a collection of flats $\mathcal{F}$ is semimodular. □

Since the lattice of a collection of flats is semimodular, we can deduce the following corollary (see [25, Prop. 3.3.2], [26, Prop. 3.7] or [1, Prop. 2.1].)

Corollary 3.11 *The lattice of a collection of flats $\mathcal{F}$ satisfies the Jordan–Dedekind property, that is: all maximal chains between two fixed elements of the lattice have the same finite length.*

In what follows, we will need the following lemma.

Lemma 3.12 *Let A be a subspace of E and let $\mathcal{F}$ be a collection of subspaces of E. Let $x \subseteq A$ have dimension one and let $F \subseteq A$ be an element of $\mathcal{F}$. Let F' be the minimal element of $\mathcal{F}$ containing $x + F$. If $A \subseteq F'$ then $F' = C_{\mathcal{F}}(A)$.*

Proof If $A \subseteq F' \in \mathcal{F}$, we have $C_{\mathcal{F}}(A) \subseteq F'$ by definition. Then since $F + x \subseteq A$ we have $F + x \subseteq C_{\mathcal{F}}(A) \subseteq F'$. Since F' is the the minimal flat containing F and x, $F' \subseteq C_{\mathcal{F}}(A)$, implying their equality. □

For each $A \subseteq E$, let $r_{\mathcal{F}}(A)$ denote the length of a maximal chain of flats from $C_{\mathcal{F}}(\{0\})$ to $C_{\mathcal{F}}(A)$. By Corollary 3.11, all such maximal chains have the same length, so $r_{\mathcal{F}}$ is well defined as a function on $\mathcal{L}(E)$. We are now ready to prove our main theorem.

Theorem 3.13 *Let E be a finite dimensional space. If $\mathcal{F}$ is a family of subspaces of E that satisfies the flat axioms* (F1)–(F3) *and for each $A \subseteq E$, then $(E, r_{\mathcal{F}})$ is a q-matroid and its family of flats is $\mathcal{F}$. Conversely, for a given q-matroid (E, r), $\mathcal{F}_r$ satisfies the conditions* (F1)–(F3) *and $r = r_{\mathcal{F}_r}$.*

Proof Let (E, r) be a q-matroid. We have seen in Proposition 3.8 that $\mathcal{F}_r$ satisfies (F1)–(F3).

Let now $(E, \mathcal{F})$ be a family of flats. Write F_0 to denote $C_{\mathcal{F}}(\{0\})$. We will show that $r_{\mathcal{F}}$ satisfies (R1)–(R3), that is, that $(E, r_{\mathcal{F}})$ is a q-matroid.

(R1): For a subspace A, $r_{\mathcal{F}}(A) \geq 0$ since $C_{\mathcal{F}}(A)$ is contained in any chain from F_0 to $C_{\mathcal{F}}(A)$. If $A \subseteq F_0$ then $F_0 = C_{\mathcal{F}}(A)$ and $r_{\mathcal{F}}(A) = 0 \leq \dim(A)$, so the result clearly holds. If F_0 does not contain A, then there is a one-dimensional space $x_0 \subseteq A$, $x_0 \nsubseteq F_0$. Let $G_0 = F_0 + x_0$ and define F_1 to be the minimal flat containing F_0 and x_0. F_1 clearly has dimension at least 1 and is a cover of F_0. Indeed if there is a flat H such that $F_0 \subsetneq H \subsetneq F_1$, H contains F_0 properly (otherwise $H = F_0$) and $x_0 \nsubseteq H$ (otherwise $H = F_1$). If it contains any element of $F_0 + x_0$ that is not in F_0 it would contain x_0 itself as a subspace. If $A \subseteq F_1$, then by Lemma 3.12 we have $F_1 = C_{\mathcal{F}}(A)$ and the required maximal chain is $F_0 \subsetneq C_{\mathcal{F}}(A)$. If $A \nsubseteq F_1$ then choose $x_1 \subseteq A$ but $x_1 \nsubseteq F_1$ and define F_2 to be the unique cover of $G_1 = F_1 + x_1$; clearly $\dim(F_2) \geq 2$. We continue in this way, choosing at each step a one-dimensional subspace $x_i \subseteq A$, $x_i \nsubseteq F_i$ and construct the unique flat F_{i+1} covering $G_i = F_i + x_i$, until we arrive at a flat F_k that contains A. By Lemma 3.12, we have $F_k = F_A$, yielding the maximal chain of flats $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = C_{\mathcal{F}}(A)$. Since $\dim(F_i) \geq i$ for each i, it follows that $r_{\mathcal{F}}(A) = k \leq \dim(A)$.

(R2): Let $A \subseteq B$; we prove $r_{\mathcal{F}}(A) \leq r_{\mathcal{F}}(B)$. By Lemma 3.5 Part 2, $C_{\mathcal{F}}(A) \subseteq C_{\mathcal{F}}(B)$, therefore a maximal chain of flats $F_0 \subseteq F_1 \subseteq \cdots \subseteq C_{\mathcal{F}}(A)$ is contained in $C_{\mathcal{F}}(B)$.

(R3): Let $A, B \subseteq E$ be subspaces and consider a maximal chain of flats $F_0 \subseteq \cdots \subseteq C_{\mathcal{F}}(A \cap B)$. If $C_{\mathcal{F}}(A \cap B) \neq C_{\mathcal{F}}(A)$ then choose a one-dimensional space $x_1 \subseteq A, x_1 \nsubseteq C_{\mathcal{F}}(A \cap B)$ and continue extending the chain, by setting $G_1 = C_{\mathcal{F}}(A \cap B) + x_1$ and taking $F_1 = C_{\mathcal{F}}(G_1)$ and then repeating this procedure, each time choosing $x_i \subseteq A, x_i \nsubseteq F_{i-1}$, where F_i is the cover of $G_i = F_{i-1} + x_i$ for each i. This sequence is clearly finite (in fact has length at most $\dim(A) - \dim(C_{\mathcal{F}}(A \cap B))$, and by Lemma 3.12, there exists some k such that $F_k = C_{\mathcal{F}}(A)$. Once we have a maximal chain terminating at $C_{\mathcal{F}}(A)$, if $B \nsubseteq C_{\mathcal{F}}(A)$, we repeat the same procedure, constructing a maximal chain terminating at $C_{\mathcal{F}}(A + B)$. In the same way, from $F_0 \subseteq \cdots \subseteq C_{\mathcal{F}}(A \cap B)$, we construct a maximal chain terminating at $C_{\mathcal{F}}(B)$, which can be extended to a maximal chain terminating at $C_{\mathcal{F}}(A + B)$. For any $y \subseteq C_{\mathcal{F}}(B)$, by (F2), the minimal flat containing $C_{\mathcal{F}}(A \cap B) + y$ is contained in the minimal flat containing $C_{\mathcal{F}}(A) + y$. Repeating this procedure gives us that every flat in the chain from $C_{\mathcal{F}}(A \cap B)$ to $C_{\mathcal{F}}(B)$ is contained in exactly one flat in the chain from $C_{\mathcal{F}}(A)$ to $C_{\mathcal{F}}(A + B)$, and any flat in the latter chain contains at least one flat of the former chain. In other words, there is a surjection between flats in the chain from $C_{\mathcal{F}}(A \cap B)$ to $C_{\mathcal{F}}(B)$ and the flats in the chain from $C_{\mathcal{F}}(A)$ to $C_{\mathcal{F}}(A + B)$. Therefore, the length of a maximal chain from $C_{\mathcal{F}}(A \cap B)$ to $C_{\mathcal{F}}(B)$ is longer than or equal to the length of a maximal chain from $C_{\mathcal{F}}(A)$ to $C_{\mathcal{F}}(A + B)$. This yields

$$r_{\mathcal{F}}(A + B) - r_{\mathcal{F}}(A) \leq r_{\mathcal{F}}(B) - r_{\mathcal{F}}(A \cap B),$$

and this proves (R3).

The only thing that remains to be proved is that rank and flats defined as above compose correctly, namely $\mathcal{F} \to r \to \mathcal{F}'$ implies $\mathcal{F} = \mathcal{F}'$, and $r \to \mathcal{F} \to r'$ implies $r = r'$. Given a family $\mathcal{F}$ of flats satisfying (F1)-(F3), define $r(A)$ to be the length of a maximal chain $F_0 \subseteq \cdots \subseteq C_{\mathcal{F}}(A)$. Then let $\mathcal{F}' = \mathcal{F}_r = \{F \subseteq E : r(F + x) > r(F), \forall x \nsubseteq F, \dim(x) = 1\}$. We want to show that $\mathcal{F} = \mathcal{F}'$. Let $F \in \mathcal{F}$, which means that $F = C_{\mathcal{F}}(F)$ is the endpoint of a maximal chain. Equivalently, for any one-dimensional subspace $x \subseteq E, x \nsubseteq F$, we have that a maximal chain for $F + x$ has to terminate at a flat that properly contains F and so $r(F + x) > r(F)$. Thus $F \in \mathcal{F}'$.

Conversely, if r is a rank function satisfying (R1)–(R3), let $\mathcal{F} = \mathcal{F}_r$. Then let $r_{\mathcal{F}}(A)$ be the length of a maximal chain $F_0 \subseteq \cdots \subseteq C_{\mathcal{F}}(A)$. We want to show that $r = r_{\mathcal{F}}$. This follows from the same reasoning as above: each element $F \in \mathcal{F}$ is the endpoint of a maximal chain and hence is strictly contained in the unique cover of $x + F$ for any $x \nsubseteq F$. □

4 *q*-PMD's and subspace designs

As an application of the cryptomorphism between the rank and flat axioms proved in Sect. 3, we obtain the first example of q-PMD that has a classical analogue, namely the q-Steiner systems. Furthermore, we generalize a result of Murty et al. [22] and show that from the flats, independent subspaces and circuits of our q-PMD we derive subspace designs. While only the $STS(13, 2)$ parameters are known to be realisable to date, we have used it in our construction to obtain subspace designs for parameters that were not previously known to be realisable. Finally, we focus on the automorphism groups of the subspace designs that are considered in this section.

4.1 *q*-Steiner systems are *q*-PMDs

We start by showing that a q-Steiner system gives a q-matroid, and we classify its family of flats. The construction given here uses the flat axioms, whereas in [22] the hyperplane axioms are used.

Proposition 4.1 *Let $\mathcal{S}$ be a q-Steiner system and let $\mathcal{B}$ denote its blocks. We define the family*

$$\mathcal{F} := \left\{ \bigcap_{B \in S} B : S \subseteq \mathcal{B} \right\}.$$

Let F be a subspace of E. Then $F \in \mathcal{F}$ if and only if one of the following holds:

(1) $F = E$,
(2) $F \in \mathcal{B}$,
(3) $\dim(F) \leq t - 1$.

Proof By definition, $\mathcal{F}$ is the collection of all intersections of the blocks in $\mathcal{B}$, so clearly $E \in \mathcal{F}$ (taking the empty intersection) and every block is contained in $\mathcal{F}$. Let us consider the case for which that F is the intersection of at least two blocks. Clearly, $\dim(F) \leq t - 1$, because every t-space is in precisely one block by the Steiner subspace design property. Let $\dim(F) = i$. By Lemma 2.18, there are exactly $\lambda_i = \begin{bmatrix} n-i \\ k-i \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1}$ blocks that contain F, so that F is contained in the intersection I of these blocks. We claim that $F = I$. If not, then there exists a 1-dimensional space $x \subseteq I$, $x \nsubseteq F$ such that the $(i + 1)$-dimensional space $x + F$ is contained in I and so, in particular, $x + F$ is contained in some λ_i blocks. However, again by Lemma 2.18 there are exactly $\lambda_{i+1} = \begin{bmatrix} n-i-1 \\ k-i-1 \end{bmatrix}_q \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q^{-1}$ blocks that contain $x + F$, which leads to a contradiction since $\lambda_{i+1} < \lambda_i$. We conclude that every space of dimension at most $t - 1$ is contained in $\mathcal{F}$. □

Theorem 4.2 *Let $\mathcal{S}$ be a q-Steiner system and let $\mathcal{B}$ denote its blocks. Let $\mathcal{F}$ be defined as in Proposition 4.1. Then $(E, \mathcal{F})$ defines a q-matroid given by its flats.*

Proof By the cryptomorphic definition of a q-matroid in Theorem 3.13, it would be enough to show that $\mathcal{F}$ satisfies the axioms (F1), (F2) and (F3). We have that (F1) holds by Proposition 4.1. By the definition of $\mathcal{F}$, we see that (F2) also holds. To prove (F3), let $F \in \mathcal{F}$ and let $x \subseteq E$ be a one-dimensional subspace such that $x \nsubseteq F$. If $\dim(F) = k$ then the unique cover of F in $\mathcal{F}$ that contains x is the whole space $E \in \mathcal{F}$, since no block contains a $(k + 1)$-dimensional space. Now suppose that $\dim(F) = t - 1$. Then $\dim(x + F) = t$ so that there exists a unique block, which is contained in $\mathcal{F}$, that covers F and contains x. Finally, suppose that $\dim(F) \leq t - 2$. Then $\dim(F + x) \leq t - 1$, so that by Proposition 4.1 $x + F \in \mathcal{F}$, which is clearly the unique cover of F that contains x. □

The q-matroid $(E, \mathcal{F})$ determined by a q-Steiner system as described in Theorem 4.2 is referred to as the q-matroid *induced* by the q-Steiner system.

In Theorem 3.13 it was shown that a collection of subspaces $\mathcal{F}$ of E satisfying (F1)–(F3) determines a q-matroid (E, r) for which $r(A) + 1$ is the length of a maximal chain of flats contained in $F_{A,} A \subseteq E$. We will now determine explicit values of the rank function of the q-matroid induced by a q-Steiner system as described in Theorem 4.2.

Proposition 4.3 *Let $M = (E, \mathcal{F})$ be the q-matroid for which $\mathcal{F}$ is the set of intersections of the blocks of an $S(t, k, n; q)$ Steiner system $(E, \mathcal{B})$. Then M is a q-PMD with rank function defined by*

$$r(A) = \begin{cases} \dim(A) & \textit{if } \dim(A) \leq t, \\ t & \textit{if } \dim(A) > t \textit{ and } A \textit{ is contained in a block of } \mathcal{B}, \\ t+1 & \textit{if } \dim(A) > t \textit{ and } A \textit{ is not contained in a block of } \mathcal{B}. \end{cases}$$

Proof Let $A \subseteq E$ be a subspace. Then $r(A) + 1$ is the length of a maximal chain of flats contained in $F_A = C_{\mathcal{F}}(A)$. If $\dim A \leq t - 1$ then A is a flat, as are all its subspaces. So a maximal chain of flats contained in $F_A = A$ has length $\dim A + 1$, hence $r(A) = \dim A$. If $\dim A = t$ then A is contained in a unique block, and this block is equal to F_A. A maximal chain of flats has the form $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{t-1} \subseteq F_A$, where $\dim F_i = i$. This chain has length $t + 1$ hence $r(A) = t = \dim A$.

If $\dim A > t$ and A is contained in a block, then F_A is a block and we apply the same reasoning as before to find $r(A) = t$. If $\dim A > t$ and A is not contained in a block, then $F_A = E$ and a maximal chain of flats is $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{t-1} \subseteq B \subseteq E$ where B is a block. This gives $r(A) = t + 1$.

To establish the q-PMD property, we show that flats of the same rank have the same dimension. Clearly this property is satisfied by flats of dimension at most t. Let F be a flat of dimension at least $t + 1$ and rank t. Then F is contained in a unique block and hence, being an intersection of blocks by definition, is itself a block and has dimension k. If F has rank $t + 1$, then it is not contained in a block, and hence must be E. □

4.2 Subspace designs from *q*-PMD's

Let M be a q-matroid induced by a q-Steiner system. We will now give a classification of its flats, independent subspaces and circuits and show that these yield new subspace designs by the idea given in [22] for the classical case. However, while the constructions are a direct generalisation to the q-analogue, the counting arguments for the parameters in these constructions are considerably more involved than in the classical case.

Flats

We have classified the flats of a q-matroid induced by a q-Steiner system in Proposition 4.1. By considering all flats of a given rank, we thus get the following designs:

(1) For rank $t + 1$ we have only one block, $\mathbb{F}_q^n$. This is an n-$(n, n, 1)$ design.
(2) For rank t, we get the original q-Steiner system.
(3) For rank less than t we get a trivial design.

Independent spaces

Proposition 4.4 *Let M be the q-PMD induced by a q-Steiner system with blocks $\mathcal{B}$. Let I be a subspace of E. Then I is independent if:*

(1) $\dim I \leq t$,

(2) $\dim I = t+1$ *and* I *is not contained in a block of* $\mathcal{B}$*.*

Proof This follows directly from the fact that I is independent if and only if $r(I) = \dim I$ and the definition of the rank function of M in Proposition 4.3. □

We want to know if all independent spaces of a fixed dimension ℓ of a given q-PMD form the blocks of a q-design. There are two trivial cases:

(1) If $\ell \leq t$ then the blocks are all spaces of dimension ℓ. This is a trivial design.
(2) If $\ell > t+1$ then there are no independent spaces. This is the empty design.

So, the only interesting case to study is that of the independent spaces of dimension $t+1$. These comprise the $(t+1)$-spaces none of which is contained in a block of $\mathcal{B}$.

Theorem 4.5 *Let* M *be the* q*-PMD induced by a* q*-Steiner system with parameters* $S(t,k,n;q)$ *and blocks* $\mathcal{B}$*. The independent spaces of dimension* $t+1$ *of* M *form a* t*-*$(n, t+1, \lambda_{\mathcal{I}})$ *design with* $\lambda_{\mathcal{I}} = (q^{n-t} - q^{k-t})/(q-1)$*.*

Proof Let $\mathcal{I}$ be the set of independent spaces of dimension $t+1$ of M. We claim that, for a given t-space A, the number of blocks $I \in \mathcal{I}$ containing it is independent of the choice of A, and thus equal to $\lambda_{\mathcal{I}}$.

Let A be a t-space and let $\lambda(A)$ denote the number of $(t+1)$-spaces of $\mathcal{I}$ that contain A. A is contained in a unique block $B \in \mathcal{B}$ of the q-Steiner system. We extend A to a $(t+1)$-space I that is not contained in any block of $\mathcal{B}$, that is, we extend A to $I \in \mathcal{I}$. We do this by taking a 1-dimensional vector space x not in B and letting $I = A + x$. The number of 1-spaces not in B is equal to the total number of 1-spaces minus the number of one-dimensional spaces in B:

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_q - \begin{bmatrix} k \\ 1 \end{bmatrix}_q = \frac{q^n - 1}{q-1} - \frac{q^k - 1}{q-1} = q^k \begin{bmatrix} n-k \\ 1 \end{bmatrix}_q.$$

However, another one-dimensional space y that is in I but not in A gives that $A + x = A + y$. The number of one-dimensional spaces in I but not in A is equal to

$$\begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} t \\ 1 \end{bmatrix}_q = \frac{q^{t+1} - 1}{q-1} - \frac{q^t - 1}{q-1} = q^t.$$

This means that the number of ways we can extend A to $I \in \mathcal{I}$ is the quotient of the two values calculated above:

$$\lambda(A) = q^{k-t} \begin{bmatrix} n-k \\ 1 \end{bmatrix}_q = \frac{q^{n-t} - q^{k-t}}{q-1} = \lambda_{\mathcal{I}},$$

which is independent of the choice of A of dimension t. □

Example 4.6 For the q-PMD arising from the $S(2,3,13;2)$ Steiner system we have $b_{\mathcal{I}} = 3267963270$ and $\lambda_{\mathcal{I}} = 2046$. For the q-PMD arising from the putative q-Fano plane $STS(7;2)$, we have $b_{\mathcal{I}} = 11430$ and $\lambda_{\mathcal{I}} = 30$.

Remark 4.7 For $k = t+1$ the construction from Theorem 4.5 gives the supplementary design of the q-Steiner system.

Circuits

Proposition 4.8 *Let M be a q-PMD induced by a q-Steiner system $S(t, k, n; q)$ with blocks $\mathcal{B}$. Let C be a subspace of M. Then C is a circuit if and only if:*

(1) $\dim C = t + 1$ *and C is contained in a block of $\mathcal{B}$,*
(2) $\dim C = t + 2$ *and all $(t + 1)$-subspaces of C are contained in none of the blocks of $\mathcal{B}$.*

Proof A circuit is a space such that all its codimension 1 subspaces are independent. All spaces of dimension at most t are independent, so a circuit will have dimension at least $t+1$. Also, since the rank of M is $t+1$, a circuit has dimension at most $t+2$. The result now follows from the definition of a circuit and the above Proposition 4.4 that classifies the independent spaces of M. □

We now show that all the $(t + 1)$-circuits form a design and that all the $(t + 2)$-circuits form a design.

Theorem 4.9 *Let M be a q-PMD induced by a q-Steiner system $S(t, k, n; q)$ with blocks $\mathcal{B}$. Let $\mathcal{C}_{t+1}$ be the collection of all circuits of M of dimension $(t + 1)$. Then $\mathcal{C}_{t+1}$ are the blocks of a t-$(n, t + 1, \lambda_{\mathcal{C}_{t+1}})$ design where*

$$\lambda_{\mathcal{C}_{t+1}} = \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q .$$

Proof Let A be a t-space contained in a unique block B_A in the q-Steiner system. There are $\begin{bmatrix} k-t \\ t+1-t \end{bmatrix}_q = \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q$ $(t + 1)$-dimensional subspaces of B_A that contain A, from Lemma 2.14. Every such $(t+1)$-space is a circuit by definition. If C is a circuit not contained in B_A, then by Proposition 4.8 C is contained in another block $B \in \mathcal{B}$. Therefore, if $A \subseteq C$, then A is contained in two distinct blocks B_A and B, contradicting the Steiner system property. Hence the number of blocks that contain A is $\lambda(A) = \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q$, which is independent of our choice of A of dimension t. □

Remark 4.10 In fact by Proposition 4.8, Theorems 4.9 and 4.5 are equivalent. The circuits of dimension $t + 1$ are precisely the set $(t + 1)$-spaces each of which is contained in some block of the q-Steiner system. Therefore this set of circuits is the complement of the set of $(t+1)$-spaces for which none of its members is contained in a block of the Steiner system. It follows that the q-designs of Theorems 4.5 and 4.9 are supplementary designs with respect to each other.

Theorem 4.11 *Let M be a q-PMD induced by a q-Steiner system $S(t, k, n; q)$ with blocks $\mathcal{B}$. Let $\mathcal{C}_{t+2}$ be the collection of all circuits of M of dimension $(t + 2)$. Then $\mathcal{C}_{t+2}$ are the blocks of a t-$(n, t + 2, \lambda_{\mathcal{C}_{t+2}})$ design where*

$$\lambda_{\mathcal{C}_{t+2}} = q^{k-t} \begin{bmatrix} n-k \\ 1 \end{bmatrix}_q \left(\begin{bmatrix} n-t-1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q \right) \frac{1}{q+1} .$$

Proof Let $\mathcal{C}_{t+2}$ be the set of circuits of dimension $t + 2$ of M. We argue that every t-space is contained in the same number $\lambda_{\mathcal{C}_{t+2}}$ of members of $\mathcal{C}_{t+2}$. We do this by calculating for a given t-space A the number of blocks $C \in \mathcal{C}_{t+2}$ it is contained in. It turns out this number is independent of the choice of A, and thus equal to $\lambda_{\mathcal{C}_{t+2}}$.

Define

$$N(A):=|\{(I,C):A\subseteq I\subseteq C, I\in\mathcal{I}, \dim I=t+1, C\in\mathcal{C}_{t+2}\}|.$$

The number of $(t+1)$-dimensional independent spaces I containing A is exactly the number $\lambda_{\mathcal{I}}$ calculated in Theorem 4.5, which is $(q^{n-t}-q^{k-t})/(q-1)$. Now let I be an independent space of dimension $t+1$ that contains the t-space A. Then I is a $(t+1)$-space that is not contained in a block of $\mathcal{B}$. We will count the number of $(t+2)$-dimensional spaces C such that $I\subseteq C\in\mathcal{C}_{t+2}$. Such a subspace C contains I as a subspace of codimension 1 and meets any block of $\mathcal{B}$ in a space of dimension at most t, by Proposition 4.8. Define $\mathcal{B}_I:=\{B\in\mathcal{B}:\dim(B\cap I)=t\}$. Clearly, the complement of $\mathcal{C}_{t+2}$ in the set of all $(t+2)$-dimensional spaces containing I is the set of $(t+2)$-dimensional subspaces of E that contain I and meet some block of $\mathcal{B}_I$ in a $(t+1)$-dimensional space.

Now fix some $B\in\mathcal{B}_I$. Let

$$\mathcal{S}(B,I):=\{D\subseteq E:\dim(D)=t+2, I\subseteq D, \dim(B\cap D)=t+1\}$$

and let

$$\mathcal{T}(B,I):=\{X\subseteq B:\dim(X)=t+1, I\cap B\subseteq X\}.$$

We now claim that the following are well defined mutually inverse bijections:

$$\varphi:\mathcal{S}(B,I)\longrightarrow\mathcal{T}(B,I):D\mapsto D\cap B,\quad \phi:\mathcal{T}(B,I)\longrightarrow\mathcal{S}(B,I):X\mapsto X+I.$$

Let $D\in\mathcal{S}(B,I)$ and let $X=D\cap B$. Then $I\cap B\subseteq X$ as $I\subseteq D$ and clearly $\dim(X)=t+1$. Therefore $X\in\mathcal{T}(B,I)$ and φ is well-defined. Conversely, let $X\in\mathcal{T}(B,I)$ and define $D=X+I$. Note first that as $\dim(I\cap B)=t$, $I\cap X=I\cap B$ has codimension 1 in X. We have $\dim(D)=\dim(X+I)=\dim(X)+\dim(I)-\dim(X\cap I)=t+1+t+1-t=t+2$. Clearly, $I\subseteq D$ and $\dim(D\cap B)=\dim(D)+\dim(B)-\dim(D+B)=t+2+k-\dim(I+B)=t+2+k-k-1=t+1$. Therefore, ϕ is well-defined. Let $X\in\mathcal{T}(B,I)$ and let $D\in\mathcal{S}(B,I)$. Then, as $I\cap B\subseteq X\subseteq B$,

$$\begin{aligned}\varphi\circ\phi(X)&=\varphi(X+I)=(X+I)\cap B=(X\cap B)+(I\cap B)=X,\\ \phi\circ\varphi(D)&=\phi(D\cap B)=(D\cap B)+I=D,\end{aligned}$$

where the last equality follows from the fact that I has codimension 1 in D and $I\nsubseteq B$. It follows that there is a 1-1 correspondence between the members of $\mathcal{S}(B,I)$ and $\mathcal{T}(B,I)$. Therefore, $|\mathcal{S}(B,I)|=|\mathcal{T}(B,I)|=\begin{bmatrix}k-t\\1\end{bmatrix}_q$, since this counts the number of $(t+1)$-dimensional subspaces of B that contain $I\cap B$. We claim now that the $\mathcal{S}(B,I)$ are disjoint. Let $B_1,B_2\in\mathcal{B}_I$ and let $D\in\mathcal{S}(B_1,I)\cap\mathcal{S}(B_2,I)$. Then B_1 and B_2 both each meet D in spaces of dimension $t+1$, say $A_1=B_1\cap D$ and $A_2=B_2\cap D$. Then $A_1\cap A_2=B_1\cap B_2\cap D$ has dimension t, being an intersection of two spaces of codimension 1 in D. This contradicts the fact that every t-dimensional subspace of E is contained in a unique block. Therefore,

$$\left|\bigcup_{B\in\mathcal{B}_I}\mathcal{S}(I,B)\right|=\sum_{B\in\mathcal{B}_I}|\mathcal{S}(I,B)|=|\mathcal{B}_I|\begin{bmatrix}k-t\\1\end{bmatrix}_q=\begin{bmatrix}t+1\\1\end{bmatrix}_q\begin{bmatrix}k-t\\1\end{bmatrix}_q.$$

The number of $(t+2)$-dimensional subspaces C that contain I and do not meet any block $B\in\mathcal{B}_I$ in a space of dimension $t+1$ is thus

$$\begin{bmatrix}n-t-1\\1\end{bmatrix}_q-\begin{bmatrix}t+1\\1\end{bmatrix}_q\begin{bmatrix}k-t\\1\end{bmatrix}_q.$$

By Theorem 4.5, there are exactly $q^{k-t}\begin{bmatrix} n-k \\ 1 \end{bmatrix}_q$ different $(t+1)$-dimensional independent spaces that contain A. It follows that

$$N(A) = q^{k-t}\begin{bmatrix} n-k \\ 1 \end{bmatrix}_q \left(\begin{bmatrix} n-t-1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q \right),$$

which is independent of our choice of A of dimension t. Now for a fixed circuit $C \in \mathcal{C}_{t+2}$ containing A there are

$$\begin{bmatrix} (t+2)-t \\ (t+1)-t \end{bmatrix}_q = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = \frac{q^2-1}{q-1} = q+1$$

independent $(t+1)$-spaces containing A and contained in C. So we have

$$N(A) = (q+1)|\{C \in \mathcal{C}_{t+2} : A \subseteq C\}| = (q+1)\lambda(A).$$

We conclude that

$$\lambda_{\mathcal{C}_{t+2}} = \lambda(A) = q^{k-t}\begin{bmatrix} n-k \\ 1 \end{bmatrix}_q \left(\begin{bmatrix} n-t-1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} t+1 \\ 1 \end{bmatrix}_q \begin{bmatrix} k-t \\ 1 \end{bmatrix}_q \right) \frac{1}{q+1}.$$

□

Remark 4.12 For the putative q-analogue of the Fano plane, the dual of the construction in Theorem 4.11 was described in [20, Theorem 4.1]. This Theorem states that the existence of a 2-$(7, 3, 1; q)$ design [i.e., a $S(2, 3, 7; q)$ Steiner system] implies the existence of a 2-$(7, 3, q^4; q)$ design and is proved by showing that the dual spaces of some subspaces described by the authors as 'of type 4_0' form a 2-$(7, 3, q^4; q)$ design. Spaces of type 4_0 are 4-spaces that do not contain any block of the original design. Indeed, taking $k = 3$ and $t = 2$ in Proposition 4.8 shows that the spaces of type 4_0 are exactly the 4-circuits of the q-PMD induced by the $S(2, 3, 7; q)$ Steiner system. They form a 2-$(7, 4, q^6 + q^4; q)$ design by Theorem 4.11 and the corresponding dual design would have parameters 2-$(7, 3, q^4; q)$ by Definition 2.17.

The admissibility of design parameters (see Lemma 2.18) plays an important role on the question of existence of subspace designs. In the following corollary we give admissibility conditions on the parameters of the design presented in Theorem 4.11 arising from an $STS(n, q)$. In order to arrive at *normalised* parameters in all cases [i.e. those for which $2k \le n$ and $2\lambda \le \lambda_{\max}$, where $\lambda_{\max}$ is the maximum possible value corresponding to an admissible parameter set t-$(n, k, \lambda_{\max})$], we also calculate the parameters of the supplementary and dual subspace designs.

Corollary 4.13 *If a q-Steiner triple system $STS(n; q)$ exists, then there exist* 2-$(n, k, \lambda; q)$ *designs with the following parameters.*

(1) $k = 4,\ \lambda = q^4 \dfrac{(q^{n-3}-1)(q^{n-6}-1)}{(q^2-1)(q-1)}$,

(2) $k = 4,\ \lambda = \dfrac{(q^{n-3}-1)(q^4-1)}{(q^2-1)(q-1)}$,

(3) $k = n-4,\ \lambda = \begin{bmatrix} n-3 \\ 3 \end{bmatrix}_q$,

(4) $k = n-4$, $\lambda = q^4 \begin{bmatrix} n-3 \\ 4 \end{bmatrix}_q$.

In this case, the design with the parameters of (2) *is the supplementary design of the design with parameters* (1), *the design of* (3) *is the dual design of the design with parameters* (2), *and the design of* (4) *is the dual of the design with parameters* (1). *Moreover, the parameters of the designs listed above are admissible if and only if* $n \equiv 0, 1, 3, 4 \mod 6$.

Proof As a special case of Theorem 4.11, if an STS$(n; q)$ exists then a 2-$(n, 4, \lambda; q)$ design $\mathcal{D}$ exists for

$$\begin{aligned}\lambda &= q \begin{bmatrix} n-3 \\ 1 \end{bmatrix}_q \left(\begin{bmatrix} n-3 \\ 1 \end{bmatrix}_q - \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \right) \frac{1}{q+1} \\ &= q^4 \frac{(q^{n-3}-1)(q^{n-6}-1)}{(q^2-1)(q-1)}.\end{aligned}$$

It is straightforward to verify that the supplementary design $\mathcal{D}'$ of $\mathcal{D}$ has parameters as given in (2), that the dual design of $\mathcal{D}'$ has parameters as given in (3), and that the dual design of $\mathcal{D}$ has parameters as given in (4). Clearly, the parameters of (1)–(3) are admissible or not admissible simultaneously. Therefore we need only check for admissibility of one parameter set. To this end we only consider the parameters in (3). Note that these parameters are admissible if and only if $\lambda_2 = \lambda$, λ_1 and λ_0 (the number of blocks of the design) are all non negative integers. From Lemma the 2.18, the intersection number λ_1 corresponding to the parameters 2-$\left(n, n-4, \lambda = \begin{bmatrix} n-3 \\ 3 \end{bmatrix}_q ; q\right)$ of (3) is

$$\lambda_1 = \begin{bmatrix} n-3 \\ 3 \end{bmatrix}_q \begin{bmatrix} n-1 \\ 4 \end{bmatrix}_q \begin{bmatrix} n-2 \\ 4 \end{bmatrix}_q^{-1} = \frac{q^{n-1}-1}{q^3-1} \frac{q^{n-3}-1}{q^2-1} \frac{q^{n-4}-1}{q-1}.$$

If $n \equiv 0, 1, 3, 4 \mod 6$ such that $n > 6$, we see that λ, λ_1 are positive integers and hence the parameters of (3) are admissible. Conversely, assume that the parameters of (3) are admissible. Then in particular λ_1 is an integer, which holds if and only if either

$$\begin{cases} \sum_{i=0}^{2r-2} q^i \sum_{j=0}^{2r-4} q^j \sum_{t=0}^{r-3} q^{2t} \equiv 0 \mod q^2+q+1 \text{ and } n = 2r \text{ for some } r \in \mathbb{Z}, \\ \sum_{i=0}^{2r-1} q^i \sum_{j=0}^{r-1} q^{2j} \sum_{t=0}^{2r-4} q^t \equiv 0 \mod q^2+q+1 \text{ and } n = 2r+1 \text{ for some } r \in \mathbb{Z}. \end{cases}$$

For $n = 2r$, if $\sum_{i=0}^{2r-2} q^i$ is divisible by q^2+q+1, then $2r-1 \equiv 0 \mod 3$, which implies $n \equiv 1 \mod 3$. Then since $n \equiv 1 \mod 3$ and $n \equiv 0 \mod 2$ we obtain $n \equiv 4 \mod 6$. If $\sum_{j=0}^{2r-4} q^j$ is divisible by q^2+q+1, then $2r-3 \equiv 0 \mod 3$, which implies $n = 2r \equiv 0 \mod 3$. Both $n \equiv 0 \mod 3$ and $n \equiv 0 \mod 2$ implies $n \equiv 0 \mod 6$. For $n = 2r+1$, if $\sum_{i=0}^{2r-1} q^i$ is divisible by q^2+q+1 then $2r-2 \equiv 0 \mod 3$, which implies $n = 2r+1 \equiv 0 \mod 3$. Both $n \equiv 1 \mod 2$ and $n \equiv 0 \mod 3$ implies $n \equiv 3 \mod 6$. And finally, if $\sum_{t=0}^{2r-4} q^t$ is divisible by q^2+2+1 then $2r-3 \equiv 0 \mod 3$, which implies $n = 2r+1 \equiv 1 \mod 3$. Both $n \equiv 1 \mod 2$ and $n \equiv 1 \mod 3$ implies $n \equiv 1 \mod 6$. On the other hand, when $n \equiv 2 \mod 6$, that is $n = 6m+2$ for some $m \in \mathbb{Z}$, then

$$\lambda_1 = \frac{q^{6m+1}-1}{q^3-1} \frac{q^{6m-1}-1}{q^2-1} \frac{q^{6m-2}-1}{q-1}.$$

Table 1 Parameters of the new designs in Corollary 4.13 from an $STS(13; 2)$

$q = 2$	2-(13, 4, 692912; 2)
	2-(13, 4, 5115; 2)
	2-(13, 9, 6347715; 2)
	2-(13, 9, 859903792; 2)

Hence, $\lambda_1 \in \mathbb{Z}$ if and only if $\sum_{i=0}^{6m} q^i \sum_{j=0}^{6m-2} q^j \sum_{t=0}^{3m-2} q^{2t}$ is divisible by $q^2 + q + 1$. Since $\sum_{i=0}^{6m} q^i \sum_{j=0}^{6m-2} q^j \equiv q + 1 \mod q^2 + q + 1$ and $\gcd(q + 1, q^2 + q + 1) = 1$, $\lambda_1 \in \mathbb{Z}$ if and only if $\sum_{t=0}^{3m-2} q^{2t}$ is divisible by $q^2 + q + 1$, which yields a contradiction. Similarly, when $n \equiv 5 \mod 6$, i.e. $n = 6m + 5$ for some $m \in \mathbb{Z}$ we have

$$\lambda_1 = \frac{q^{6m+4} - 1}{q^3 - 1} \frac{q^{6m+2} - 1}{q^2 - 1} \frac{q^{6m+1} - 1}{q - 1}.$$

Note that $\lambda_1 \in \mathbb{Z}$ if and only if $\sum_{t=0}^{3m+1} q^{2t} \sum_{i=0}^{6m+1} q^i \sum_{j=0}^{6m} q^j \equiv 0 \mod q^2 + q + 1$. Since $\sum_{i=0}^{6m+1} q^i \sum_{j=0}^{6m} q^j \equiv q + 1 \mod q^2 + q + 1$, and $\gcd(q + 1, q^2 + q + 1) = 1$, $\lambda_1 \in \mathbb{Z}$ if and only if $\sum_{t=0}^{3m+1} q^{2t}$ is divisible by $q^2 + q + 1$, which yields a contradiction. □

Table 1 shows the parameters that we obtain from the Steiner system $STS(13; q)$ and Corollary 4.13. In particular, the normalized form of these parameters is 2-(13, 4, 5115; 2). Of course the other two parameter sets are immediately implied by this one. Table 2 summarizes the parameters of subspace designs whose existence would be implied by the existence of the q-Fano plane.

Remark 4.14 In the literature, the only known Steiner triple systems found are those with parameters $STS(13; 2)$. The existence of such $STS(13; 2)$ Steiner triple systems implies, via Corollary 4.13, the existence of new subspace designs with parameters as shown in Table 1.

Moreover, for $q = 2, 3$ and $n = 7$, Corollary 4.13 shows that the existence of the q-Fano plane implies the existence of 2-(7, 3, 15; 2) and 2-(7, 3, 40; 3) designs (see also Table 2). Designs with these parameters have actually been found [3]. However, for $q \geq 4$, there is no information on the existence of designs with parameters 2-$\left(7, 3, \frac{q^4-1}{q-1}; q\right)$, which would arise from the q-Fano plano over $\mathbb{F}_q$.

Remark 4.15 Let n, k, t be positive integers satisfying $n \geq k \geq t + 1$ and suppose that the parameters $S(t, k, n; q)$ are admissible. One may ask the question as to whether this implies that the parameters

(1) t-$\left(n, t + 1, \begin{bmatrix} k - t \\ 1 \end{bmatrix}_q\right)$ (Theorem 4.9),

(2) t-$\left(n, t + 2, q^{k-t} \begin{bmatrix} n - k \\ 1 \end{bmatrix}_q \left(\begin{bmatrix} n - t - 1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} k - t \\ 1 \end{bmatrix}_q \begin{bmatrix} t + 1 \\ 1 \end{bmatrix}_q\right) \frac{1}{q + 1}\right)$ (Theorem 4.11),

Table 2 Parameters of the designs of Corollary 4.13 from a putative $STS(7;q)$

$q=2$	2-(7, 4, 80; 2)	
	2-(7, 4, 75; 2)	
	2-(7, 3, 15; 2)	[3], [8, Table 1]
	2-(7, 3, 16; 2)	
$q=3$	2-(7, 4, 810; 3)	
	2-(7, 4, 400; 3)	
	2-(7, 3, 40; 3)	[3], [8, Table 2]
	2-(7, 3, 81; 3)	
$q=4$	2-(7, 4, 4352; 4)	
	2-(7, 4, 1445; 4)	
	2-(7, 3, 85; 4)	
	2-(7, 3, 256; 4)	
$q=5$	2-(7, 4, 16250; 5)	
	2-(7, 4, 4056; 5)	
	2-(7, 3, 156; 5)	
	2-(7, 3, 625; 5)	

are admissible. In the case that $t=2$, from [10] we have that a $\mathcal{S}(2,k,n;q)$ Steiner system exists only if $n \equiv 1, k \mod k(k-1)$.

We have found by a computer check that for the case $t=2$, if $q \leq 11$, for $3 \leq k \leq 20$, and $n \in \{1+ik(k-1), k+ik(k-1) : 1 \leq i \leq 40\}$ then the parameters of (2) are admissible. Similarly, for the cases $t=3,4$, $q \in \{2,3,4,5,7,8,9,11,13\}$; $k \in \{t+2,\ldots,15\}$, $n \in \{k+3,\ldots,300\}$, we have found that the parameters of (2) are admissible whenever the $\mathcal{S}(2,k,n;q)$ parameters are admissible, while the converse does not hold.

While the experimental evidence appears to suggest that the admissibility of the parameters of an $\mathcal{S}(2,k,n;q)$ Steiner system implies the admissibility of the circuit designs constructed in this paper, calculations to prove this are rather formidable. We give a proof for the case $t=2$ regarding the $(t+1)$-dimensional circuit designs.

Proposition 4.16 *Let n,k be positive integers satisfying $n \geq k \geq 3$. If the parameters $S(2,k,n;q)$ are admissible then the parameters 2-$\left(n, 3, \begin{bmatrix} k-2 \\ 1 \end{bmatrix}_q\right)$ are admissible.*

Proof Suppose that the parameters $S(t,k,n;q)$ are admissible, so that $n \equiv 1, k \mod k(k-1)$. The parameters 2-$\left(n, 3, \begin{bmatrix} k-2 \\ 1 \end{bmatrix}_q\right)$ are admissible if and only if, for $i=0,1$ we have:

$$B_i{:=}{:=}\begin{bmatrix} k-2 \\ 1 \end{bmatrix}_q \begin{bmatrix} n-i \\ 3-i \end{bmatrix}_q \begin{bmatrix} n-2 \\ 1 \end{bmatrix}_q^{-1} = \frac{q^{k-2}-1}{q-1} \prod_{j=i}^{1} \frac{q^{n-j}-1}{q^{3-j}-1} \in \mathbb{Z}.$$

If $n-1$ is even then q^2-1 divides $q^{n-1}-1$. On the other hand, since $k-1$ divides $n-1$, if $n-1$ is odd then $k-2$ is even and so q^2-1 divides $q^{k-2}-1$. Clearly, in either case B_1 is a positive integer. Now consider

$$B_0 = \frac{q^{k-2}-1}{q-1} \frac{q^n-1}{q^3-1} \frac{q^{n-1}-1}{q^2-1} = \frac{q^n-1}{q^3-1} B_1.$$

If $k \equiv 0 \mod 3$ and $k \equiv 1 \mod 2$ then $(q^3-1)(q^2-1)|(q^k-1)(q^{k-1}-1)$, which divides $(q^n-1)(q^{n-1}-1)$ by the admissibility of $S(t,k,n;q)$. Therefore, $B_0 \in \mathbb{Z}$. If $k \equiv 0 \mod 3$ and $k \equiv 0 \mod 2$ then $(q^3-1)(q^2-1)|(q^n-1)(q^{k-2}-1)$ and so again B_0 must be an integer. If $k \equiv 2 \mod 3$ then $(q^3-1)|(q^{k-2}-1)$ and clearly $(q-1)(q^2-1)|(q^n-1)(q^{n-1}-1)$, so that $B_0 \in \mathbb{Z}$. Finally, suppose now that $k \equiv 1 \mod 3$, so that $n \equiv 1 \mod 3$. If $k \equiv 0 \mod 2$ then $(q^3-1)(q^2-1)|(q^{n-1}-1)(q^{k-2}-1)$ and so $B_0 \in \mathbb{Z}$. If $k \equiv 1 \mod 2$ we can consider the parameters of the supplementary design (i.e. the design of Theorem 4.5), which are admissible if and only if

$$C_0 = \frac{q^{n-k}-1}{q-1}\frac{q^n-1}{q^3-1}\frac{q^{n-1}-1}{q^2-1} \quad \text{and} \quad C_1 = \frac{q^{n-k}-1}{q-1}\frac{q^{n-1}-1}{q^2-1}$$

are both positive integers. We have $n-k \equiv 0 \mod 3$, so that $C_0 \in \mathbb{Z}$ and $n-k \equiv 0 \mod 2$, so that $C_1 \in \mathbb{Z}$. It follows that the parameters of the supplementary design are admissible in the final case $k \equiv 1 \mod 3$ and $k \equiv 1 \mod 2$. □

4.3 The automorphism group of designs from *q*-PMDs

For the subspace designs constructed in Theorems 4.5, 4.9, and 4.11, we show that their automorphism groups are isomorphic to the automorphism group of the original Steiner system. Since the designs in Theorems 4.5 and 4.9 are supplementary to each other and moreover the constructions of the circuits in Theorem 4.11 are obtained by the independent spaces in Theorem 4.5, we only consider the automorphism groups of the designs in Theorems 4.5 and 4.11, respectively.

Theorem 4.17 *Let $\mathcal{S}$ be an $S(t,k,n;q)$ q-Steiner system. Then*

(1) *The automorphism group of the subspace design obtained in Theorem 4.5 from $\mathcal{S}$ is isomorphic to the automorphism group of $\mathcal{S}$.*
(2) *The automorphism group of the subspace design obtained in Theorem 4.11 from $\mathcal{S}$ is isomorphic to the automorphism group of $\mathcal{S}$.*

Proof Let $\mathcal{B}$ denote the blocks of $\mathcal{S}$. Let $\mathcal{I}_{t+1}$ be the set of independent spaces of dimension $t+1$ and let $\mathcal{C}_{t+2}$ be the set of circuits of dimension $t+2$ of the q-PMD arising from $\mathcal{S}$.

(1) No member of $\mathcal{I}_{t+1}$ is contained in a block of $\mathcal{B}$. Let ϕ be an automorphism of $\mathcal{S}$. Given an independent space $I \in \mathcal{I}_{t+1}$, we claim that the image $\phi(I)$ is also an independent space. Since $\phi \in \mathrm{Aut}(\mathcal{L}(E))$, then $\dim \phi(I) = t+1$. Moreover, $\phi(I)$ cannot be contained in a block B of $\mathcal{B}$, because otherwise $I \subseteq \phi^{-1}(B) \in \mathcal{B}$, which is a contradiction. Therefore, $\phi(\mathcal{I}_{t+1}) = \mathcal{I}_{t+1}$ and so $\phi \in \mathrm{Aut}(\mathrm{E}, \mathcal{I}_{t+1})$.

Conversely, let ϕ be an automorphism of the subspace design with blocks $\mathcal{I}_{t+1}$. We will show that $\phi(B) \in \mathcal{B}$ for all $B \in \mathcal{B}$. Let $B \in \mathcal{B}$ and let A be a t-dimensional subspace of B such that $\phi(A) \neq A$. Note that if no such space exists, then $\phi(B) = B$, hence $\phi(B)$ is a block. We will denote by $B_A = B$ the unique block containing A and by $B_{\phi(A)}$ the unique block in $\mathcal{B}$ containing $\phi(A)$. Now assume that $\phi(B_A)$ is not a block, which in particular implies that there exists a one-dimensional subspace $x \subseteq \phi(B_A)$, $x \nsubseteq B_{\phi(A)}$. By considering the independent space construction in Theorem 4.5, we claim that the set $I_A = \phi(A) + x$ is independent, since it has dimension $t+1$ and is not contained in a block. Indeed, if it were contained in a block $B' \neq B_{\phi(A)}$, then $\phi(A)$ would be contained in two different blocks and this would contradict the fact that $\mathcal{S}$ is a Steiner system. Finally, note that since $\mathcal{I}_{t+1}$ is the set of blocks of a subspace design, there are λ_I independent spaces $I_1, \ldots, I_{\lambda_I}$ each of

which contains A. It follows that for each i, $\phi(A) \subseteq \phi(I_i)$ and since each $I_i \not\subseteq B_A$, we have $\phi(I_i) \not\subseteq \phi(B_A)$. Since $I_A \subseteq \phi(B_A)$, it follows that I_A is different from each of the subspaces I_i. However, in that case $\phi(A)$ is contained in $\lambda_I + 1$ independent subspaces in $\mathcal{I}_{t+1}$, yielding a contradiction. It follows that $\phi(B) \in \mathcal{B}$ for each $B \in \mathcal{B}$ and so the result follows.
(2) Let ϕ be an automorphism of $\mathcal{S}$. Let $C \in \mathcal{C}_{t+2}$. If $\phi(C)$ is not a circuit of dimension $t+2$, there exists a $(t+1)$-dimensional subspace $I' \subseteq \phi(C)$ that is contained in a block B of $\mathcal{B}$. Then $\phi^{-1}(I')$ is a $(t+1)$-subspace of C such that $\phi^{-1}(I') \subseteq \phi^{-1}(B)$. This contradicts the fact that C is a circuit of dimension $t+2$. It follows that ϕ is an automorphism of $(E, \mathcal{C}_{t+2})$.

Conversely, let $\phi \in \mathrm{Aut}(E, \mathcal{C}_{t+2})$. We claim that ϕ is also an automorphism of $(E, \mathcal{I}_{t+1})$. Let $I \in \mathcal{I}_{t+1}$ and let $C \in \mathcal{C}_{t+2}$ such that $I \subseteq C$. Then $\phi(C) \in \mathcal{C}_{t+2}$ and so is a circuit of dimension $t+2$ that contains the $(t+1)$-dimensional space $\phi(I)$. It follows that $\phi(I)$ is independent and so $\phi(I) \in \mathcal{I}_{t+1}$. It now follows from 1 that ϕ is an automorphism of $\mathcal{S}$. □

Remark 4.18 Subspace designs with parameters 2-(7, 3, 15; 2) and 2-(7, 3, 40; 3) were found by computer search in [5], applying the Kramer–Mesner method and under the assumption that their automorphism groups contain a Singer cycle. In Table 1, we see that subspace designs with the same parameters appear, with such designs arising from an $STS(7; 2)$ q-Steiner triple system. However, the designs of [5] could not be constructed by the methods of this paper, as then their automorphism groups would be isomorphic to that of the q-Fano plane, which has automorphism group of order at most 2 [7, 19].

Acknowledgements The authors are indebted to Ferdinand Ihringer for pointing out a counting error in Theorem 4.11 in an earlier version of this paper, as well as to Ragnar Freij-Hollanti for his remarks on Proposition 4.1 and Theorem 4.2. The authors wish to thank the anonymous referees for their helpful comments. This paper is the product of 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). Elif Saçıkara is supported by the Swiss National Science Foundation Grant No. 188430.

Funding Open Access funding provided by the IReL Consortium.

References

1. Aigner M.: Combinatorial Theory. Springer, New York (1979).
2. Bollen G., Crapo H., Jurrius R.: The Tutte q-Polynomial (2017). arxiv:1707.03459.
3. Braun M.: Some new designs over finite fields. Bayreuth. Math. Schr. **74**, 58 (2005).
4. Braun M., Etzion T., Östergård P.R.J., Vardy A., Wassermann A.: Existence of q-analogs of Steiner systems. Forum Math. Pi **4**, e7 (2016). https://doi.org/10.1017/fmp.2016.5.
5. Braun M., Kerber A., Laue R.: Systematic construction of q-analogs of t-(v, k, λ)-designs. Des. Codes Cryptogr. **34**(1), 55–70 (2005).
6. Braun M., Kiermaier M., Kohnert A., Reinhard L.: Large sets of subspace designs. J. Comb. Theory A **147**, 155–185 (2017).

7. Braun M., Kiermaier M., Nakiç A.: On the automorphism group of a binary q-analog of the Fano plane. Eur. J. Comb. **51**, 443–457 (2016).
8. Braun M., Kiermaier M., Wassermann A.: q-Analogs of designs: subspace designs. In: Network Coding and Subspace Designs, pp. 171–211. Springer, Cham (2018).
9. Buratti M., Nakić A.: Designs over finite fields by difference methods. Finite Fields Their Appl. **57**, 128–138 (2019). https://doi.org/10.1016/j.ffa.2019.02.006.
10. Buratti M., Nakič A., Wassermann A.: Graph decompositions in projective geometries. J. Comb. Des. **29**(3), 141–174 (2020).
11. Byrne E., Ceria M., Jurrius R.: Constructions of new q-cryptomorphisms. J. Comb. Theory B **153**, 149–194 (2022).
12. Byrne E., Ravagnani A.: An Assmus–Mattson theorem for rank metric codes. SIAM J. Discret. Math. **33**(3), 1242–1260 (2019).
13. Crapo H.H.: On the theory of combinatorial independence. PhD Thesis, Massachusetts Institute of Technology, Department of Mathematics (1964).
14. Deza M.: Perfect matroid designs. In: Matroid Applications, vol. 40, pp. 54–72. Cambridge University Press, Cambridge (1992).
15. Gordon G., McNulty J.: Matroids, a Geometric Introduction. Cambridge University Press, Cambridge (2012).
16. Gorla E., Jurrius R., López H.H., Ravagnani A.: Rank-metric codes and q-polymatroids. J. Algebr. Comb. **52**, 1–19 (2020).
17. Itoh T.: A new family of 2-designs over $GF(q)$ admitting $SL_m(q^\ell)$. Geom. Dedicata **69**(3), 261–286 (1998).
18. Jurrius R., Pellikaan R.: Defining the q-analogue of a matroid. Electron. J. Comb. **25**(3), P3.2 (2018).
19. Kiermaier M., Kurz S., Wassermann A.: The order of the automorphism group of a binary q-analog of the Fano plane is at most two. Des. Codes Cryptogr. **86**(2), 239–250 (2018).
20. Kiermaier M., Pavčević M.O.: Intersection numbers for subspace designs. J. Comb. Des. **23**(11), 463–480 (2015).
21. Kramer E.S., Mesner D.M.: t-Designs on hypergraphs. Discret. Math. **15**(3), 263–296 (1976).
22. Murty U., Young H., Edmonds J.: Equicardinal matroids and matroid designs. In: Proceedings of the 2nd Chapel Hill Conference on Combinatorial Mathematics, Chapel Hill, pp. 498–547 (1970).
23. Murty U.S.R.: Equicardinal matroids and finite geometries. In: Combinatorial Structures and Their Applications, pp. 289–293. Gordon and Breach, New York (1970).
24. Oxley J.: Matroid Theory, 2nd edn Oxford University Press, Oxford (2011).
25. Stanley R.: Enumerative Combinatorics, vol. 1. Cambridge University Press, Cambridge (1997).
26. Stanley R.: An introduction to hyperplane arrangements. In: Geometric Combinatorics. IAS/Park City Mathematical Series, vol. 13, pp. 389–496. American Mathematical Society, Providence (2007).
27. Suzuki H.: On the inequalities of t-designs over a finite field. Eur. J. Comb. **11**(6), 601–607 (1990).
28. Suzuki H.: 2-Designs over $GF(q)$. Graphs Comb. **8**(4), 381–389 (1992).
29. Thomas S.: Designs over finite fields. Geom. Dedicata **24**(2), 237–242 (1987).