Aalto University

OPEN ACCESS

This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Braun, Michael; Etzion, Tuvi ; Östergård, Patric R. J.; Vardy, Alexander; Wassermann, Alfred

Existence of q-analogs of Steiner systems

Published in:
FORUM OF MATHEMATICS, PI

DOI:
10.1017/fmp.2016.5

Published: 30/08/2016

Document Version
Publisher's PDF, also known as Version of record

Published under the following license:
CC BY

Please cite the original version:
Braun, M., Etzion, T., Östergård, P. R. J., Vardy, A., & Wassermann, A. (2016). Existence of q-analogs of Steiner systems. *FORUM OF MATHEMATICS, PI*, *4*, [e7]. https://doi.org/10.1017/fmp.2016.5

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

Forum of Mathematics, Pi (2016), Vol. 4, e7, 14 pages
doi:10.1017/fmp.2016.5

EXISTENCE OF q-ANALOGS OF STEINER SYSTEMS

MICHAEL BRAUN[1], TUVI ETZION[2], PATRIC R. J. ÖSTERGÅRD[3], ALEXANDER VARDY[4,5] and ALFRED WASSERMANN[6]

[1] Darmstadt University of Applied Sciences, Darmstadt, Germany;
email: michael.braun@h-da.de
[2] Technion, Haifa, Israel;
email: etzion@cs.technion.ac.il
[3] Aalto University, Aalto, Finland;
email: patric.ostergard@aalto.fi
[4] University of California San Diego, La Jolla, California, USA
[5] Nanyang Technological University, Singapore;
email: avardy@ucsd.edu
[6] University of Bayreuth, Bayreuth, Germany;
email: Alfred.Wassermann@uni-bayreuth.de

Received 21 May 2103; accepted 19 July 2016

Abstract

Let $\mathbb{F}_q^n$ be a vector space of dimension n over the finite field $\mathbb{F}_q$. A q-analog of a Steiner system (also known as a *q-Steiner system*), denoted $\mathcal{S}_q(t,k,n)$, is a set $\mathcal{S}$ of k-dimensional subspaces of $\mathbb{F}_q^n$ such that each t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly one element of $\mathcal{S}$. Presently, q-Steiner systems are known only for $t = 1$, and in the trivial cases $t = k$ and $k = n$. In this paper, the first nontrivial q-Steiner systems with $t \geqslant 2$ are constructed. Specifically, several nonisomorphic q-Steiner systems $\mathcal{S}_2(2, 3, 13)$ are found by requiring that their automorphism groups contain the normalizer of a Singer subgroup of GL(13, 2). This approach leads to an instance of the exact cover problem, which turns out to have many solutions.

2010 Mathematics Subject Classification: 51E10 (primary); 05E20 (secondary)

1. Introduction

Let V be a set with n elements. A t-(n, k, λ) combinatorial design (or *t-design*, in brief) is a collection of k-subsets of V, called blocks, such that each t-subset of V is contained in exactly λ blocks. A t-(n, k, λ) design with $t = \lambda = 1$ is

© The Author(s) 2016. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

trivial: it is simply a partition of V into k-subsets, which exists if and only if k divides n. A t-$(n, k, 1)$ design with $t \geqslant 2$ is known as a *Steiner system*, and usually denoted $S(t, k, n)$. Steiner systems are among the most beautiful and well-studied structures in combinatorics. Their history goes back to the work of Plücker [41], Kirkman [31], Cayley [10], and Steiner [45] in the first half of the 19th century. Today, the significance of Steiner systems extends well beyond combinatorics—they have found applications in many areas, including group theory, finite geometry, cryptography, and coding theory [5, 12, 17, 27]. For example, a finite projective plane of order q can be characterized as a Steiner system $S(2, q + 1, q^2 + q + 1)$, with lines as blocks. As another example, the Mathieu groups (which played an important role in the classification of finite simple groups) are most naturally understood as automorphism groups of certain Steiner systems.

It has been known since the celebrated result of Teirlinck [48] that nontrivial t-designs exist for all t. As far as Steiner systems, there are several infinite families with $t \leqslant 3$ as well as numerous sporadic constructions with $t = 4, 5$; see [12, Part II] for more details. A long-standing problem in design theory asks whether nontrivial (meaning $t < k < n$) Steiner systems with $t > 5$ exist. Keevash recently announced a resolution of this problem: his breakthrough paper [29] moreover shows that Steiner systems $S(t, k, n)$ exist for all $t < k$ and all sufficiently large integers n that satisfy the necessary divisibility conditions.

The classical theory of *q-analogs* of mathematical objects and functions has its beginnings in the work of Euler [19, 33]. In 1957, Tits [51] further suggested that combinatorics of sets could be regarded as the limiting case $q \to 1$ of combinatorics of vector spaces over the finite field $\mathbb{F}_q$. Indeed, there is a strong analogy between subsets of a set and subspaces of a vector space, expounded by numerous authors—see [11, 21, 52] and references therein. It is therefore natural to ask which combinatorial structures can be generalized from sets (the $q \to 1$ case) to vector spaces over $\mathbb{F}_q$. For t-designs and Steiner systems, this question was first studied by Cameron [8, 9] and Delsarte [14] in the early 1970s. Specifically, let $\mathbb{F}_q^n$ be a vector space of dimension n over the finite field $\mathbb{F}_q$. Then a t-(n, k, λ) *design over* $\mathbb{F}_q$ is defined in [8, 9, 14] as a collection of k-dimensional subspaces of $\mathbb{F}_q^n$, called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly λ blocks. Such t-designs over $\mathbb{F}_q$ are the q-analogs of conventional designs. By analogy with the $q \to 1$ case, a t-$(n, k, 1)$ design over $\mathbb{F}_q$ is said to be a *q-Steiner system*, and denoted $\mathcal{S}_q(t, k, n)$.

Remark. We observe that q-analogs of designs and Steiner systems are not only of interest in their own right, but also arise naturally in other areas,

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

such as network coding. In conventional coding theory, a code is a collection of elements of $\mathcal{A}^n$ (where $\mathcal{A}$ is a fixed set, called the alphabet) that are well separated according to some metric, for example, the Hamming distance. Such codes, however, are not appropriate for error correction in networks. In random network coding [24, 54], a source of information injects into the network several (say, k) vectors lying in some ambient space $\mathbb{F}_q^n$. A network is simply a directed acyclic graph; each node in the network performs a (random) linear operation on the vectors incident on its incoming edges, propagating the result on its outgoing edges. Clearly, the only information that is preserved and propagated through the network in this manner is the vector space spanned by the source vectors. The appropriate code in this case is a collection of subspaces of $\mathbb{F}_q^n$ that are well separated according to a metric defined on the Grassmannian $\mathrm{Gr}(k, \mathbb{F}_q^n)$. Consequently, a q-Steiner system $\mathcal{S}_q(t, k, n)$ can be thought of as an *optimal code* for error correction in networks. For more details on this, see [17, 34]. □

Following the work of Cameron [8, 9] and Delsarte [14], the first examples of nontrivial t-designs over $\mathbb{F}_q$ were found by Thomas [49] in 1987. Today, owing to the efforts of many authors [7, 20, 30, 40, 42, 46, 47, 50], numerous such examples are known.

However, the situation is very different for q-Steiner systems. They are known to exist in the trivial cases $t = k$ or $k = n$, and in the case where $t = 1$ and k divides n. In the latter case, q-Steiner systems coincide with the classical notion of *spreads* in projective geometry [38, Ch. 24]. Some 40 years ago, Beutelspacher [6] asked whether nontrivial q-Steiner systems with $t \geqslant 2$ exist, and this question has tantalized mathematicians ever since. The problem has been studied by numerous authors [3, 18, 39, 44, 49, 50], without much progress toward constructing such q-Steiner systems. In particular, Thomas [50] showed in 1996 that certain kinds of $\mathcal{S}_2(2, 3, 7)$ q-Steiner systems (the smallest possible example) cannot exist. Three years later, Metsch [39] conjectured that nontrivial q-Steiner systems with $t \geqslant 2$ do not exist in general. In contrast to this conjecture, our main result is the following theorem.

THEOREM 1. *There exist nontrivial q-Steiner systems with $t \geqslant 2$.*

In fact, we have discovered over 500 nonisomorphic $\mathcal{S}_2(2, 3, 13)$ q-Steiner systems. For more on this, see Section 3; however, let us briefly outline our general approach here. We begin by imposing a carefully chosen *additional structure* on a putative $\mathcal{S}_2(2,3,13)$ q-Steiner system $\mathcal{S}$. Specifically, we construct a group $A \leqslant \mathrm{GL}(13,2)$ as the semidirect product of the Galois group $\mathrm{Gal}(\mathbb{F}_{2^{13}}/\mathbb{F}_2)$ and a Singer subgroup C_α of $\mathrm{GL}(13, 2)$, and then insist that the automorphism group $\mathrm{Aut}(\mathcal{S})$ contains A. Next, we make use of the well-known Kramer–Mesner

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

method, and consider the Kramer–Mesner incidence structure between the orbits of 2-subspaces of $\mathbb{F}_2^{13}$ and the orbits of 3-subspaces of $\mathbb{F}_2^{13}$ under the action of A. Given the corresponding Kramer–Mesner matrix $\mathbf{M}^A$ with 105 rows and 30 705 columns, we reformulate the search for $\mathcal{S}$ as an instance of the exact cover problem, which we solve using the dancing links algorithm of Knuth [32].

As corollaries to the existence of $\mathcal{S}_2(2,3,13)$, we obtain a number of related results. Starting with $\mathcal{S}_2(2,3,13)$, we use [18, Theorem 3.2] to construct a Steiner system $S(3, 8, 8192)$. Steiner systems with these parameters were not known previously [12]. An $\mathcal{S}_2(2,3,13)$ q-Steiner system also leads to new diameter-perfect codes in the Grassmann graph [3, 44]. Finally, as explained earlier, q-Steiner systems produce optimal codes for error correction in networks [17, 34]. Thus we find that the maximum number of codewords in a subspace code over $\mathbb{F}_2^{13}$ of constant dimension $k = 3$ and minimum subspace distance $d = 4$ is 1 597 245.

The rest of this paper is organized as follows. In Section 2, we consider automorphisms of q-Steiner systems, and introduce the normalizer of a Singer subgroup, which is the group of automorphisms we choose to impose on $\mathcal{S}_2(2, 3, 13)$. In Section 3, we briefly outline the Kramer–Mesner method, and describe the computer search we have carried out based upon the results of Section 2. We give an explicit set of 15 orbit representatives for the 1 597 245 subspaces of one $\mathcal{S}_2(2, 3, 13)$ q-Steiner system, thereby proving Theorem 1. We also present several negative results that establish nonexistence of q-Steiner systems of certain kinds, extending the work of [16, 18, 35, 50]. We elaborate upon the connection to difference sets in Section 4, and compile a number of related results. In Section 5, we conclude with a brief discussion of open problems, and formulate a specific conjecture regarding the existence of an infinite family of q-Steiner systems.

2. Automorphisms of q-Steiner systems

Let G be the group of bijective incidence-preserving mappings from the set of subspaces of $\mathbb{F}_q^n$ onto itself. We know from the fundamental theorem of projective geometry [4, Ch. 3] that G is the general semilinear group $\Gamma\mathrm{L}(n, q)$. This group is isomorphic to the semidirect product of the general linear group $\mathrm{GL}(n, q)$ and the Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, where p is the characteristic of $\mathbb{F}_q$. Unless stated otherwise, we will henceforth assume that q is prime, in which case G reduces to the general linear group $\mathrm{GL}(n, q)$. Basic familiarity with the main properties of $\mathrm{GL}(n, q)$ is assumed; an in-depth treatment of $\mathrm{GL}(n, q)$ can be found, for example, in [25].

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

The action of $\mathrm{GL}(n,q)$ on subspaces of $\mathbb{F}_q^n$ extends in the obvious way to sets of subspaces, and thereby to q-Steiner systems. Given a set $\mathcal{S}$ of subspaces of $\mathbb{F}_q^n$ and a group element $g \in \mathrm{GL}(n,q)$, we denote the image of $\mathcal{S}$ under the action of g by $\mathcal{S}^g$. We say that two sets of subspaces $\mathcal{S}_1$ and $\mathcal{S}_2$ are *isomorphic* if there exists an element $g \in \mathrm{GL}(n,q)$ such that $\mathcal{S}_2 = \mathcal{S}_1^g$. An element $g \in \mathrm{GL}(n,q)$ for which $\mathcal{S}^g = \mathcal{S}$ is called an *automorphism* of $\mathcal{S}$. The automorphisms of a set $\mathcal{S}$ of subspaces form a group under composition, called the *automorphism group* and denoted $\mathrm{Aut}(\mathcal{S})$. A subgroup of $\mathrm{Aut}(\mathcal{S})$ is called a *group of automorphisms*. We note that, since $\mathrm{GL}(n,q)$ acts transitively on the set of k-subspaces of $\mathbb{F}_q^n$ for any fixed k, the automorphism group of a nontrivial q-Steiner system is necessarily a proper subgroup of $\mathrm{GL}(n,q)$.

A well-known approach to constructing combinatorial objects is to prescribe a certain group of automorphisms A and then search only for those objects whose automorphism group contains A. For an overview of the theory and applications of this method to combinatorial designs, the reader is referred to [27, Section 9.2]. Prescribing a group of automorphisms simplifies the construction problem, sometimes rendering intractable problems tractable, but choosing the right groups can be a challenge. We shall now discuss certain apposite subgroups of $\mathrm{GL}(n,q)$.

A *Singer cycle* of $\mathrm{GL}(n,q)$ is an element of order $q^n - 1$. Singer cycles can be constructed, for example, by identifying vectors in $\mathbb{F}_q^n$ with elements of the finite field $\mathbb{F}_{q^n}$. Since multiplication by a primitive element $\alpha \in \mathbb{F}_{q^n}$ is a linear operation, it corresponds to a Singer cycle in $\mathrm{GL}(n,q)$. In fact, there is a one-to-one correspondence between Singer cycles in $\mathrm{GL}(n,q)$ and primitive elements in $\mathbb{F}_{q^n}$. Given a primitive element $\alpha \in \mathbb{F}_{q^n}$, the subgroup of $\mathrm{GL}(n,q)$ generated by the corresponding Singer cycle is cyclic of order $q^n - 1$, and its elements correspond to multiplication by α^i for $i = 0, 1, \ldots, q^n - 2$. We denote such groups by C_α and call them the *Singer subgroups* of $\mathrm{GL}(n,q)$.

Another group of importance to us is generated by the *Frobenius automorphism* $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, defined by $\phi(\beta) = \beta^q$ for all $\beta \in \mathbb{F}_{q^n}$. The Frobenius automorphism ϕ is the canonical generator of the *Galois group* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, which is cyclic of order n.

The *normalizer of a subgroup* $H \leqslant G$ is the set of elements of G that commute with H as a whole. That is, $N_G(H) = \{g \in G : gH = Hg\}$. The following well-known result can be found, for example, in [25, pages 187–188].

THEOREM 2. *Let A_α be the normalizer of a Singer subgroup C_α in $\mathrm{GL}(n,q)$. Then A_α has order $n(q^n - 1)$ and is isomorphic to the semidirect product of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ and C_α.*

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

The following theorem follows from a more general result by Kantor [26]. It is stated explicitly in [15].

THEOREM 3. *Let n be an odd prime. Then the normalizer of a Singer subgroup is a maximal subgroup of* $\mathrm{GL}(n, q)$.

In Section 3, we will search for q-Steiner systems $\mathcal{S}$ whose automorphism group $\mathrm{Aut}(\mathcal{S})$ contains the normalizer of a Singer subgroup. We observe that Singer subgroups and normalizers of Singer subgroups have been used when prescribing automorphisms for various types of q-analog structures in [7, 17].

We already noted that $\mathrm{Aut}(\mathcal{S}) < \mathrm{GL}(n, q)$ for nontrivial designs over $\mathbb{F}_q$. Thus for odd primes n, it follows from Theorem 3 that if $\mathrm{Aut}(\mathcal{S})$ contains A_α, then A_α is the full automorphism group of $\mathcal{S}$. In turn, the fact that $\mathrm{Aut}(\mathcal{S}) = A_\alpha$ makes it possible to say much more. In particular, we will show that distinct nontrivial designs whose automorphism group contains A_α are necessarily nonisomorphic. We point out that similar results have been already established in various contexts—for example, see [37] and [43, Theorem 4.1]. Nevertheless, we provide a self-contained proof. First, we need the following lemma.

LEMMA 4. *The normalizer of a Singer subgroup is self-normalizing in* $\mathrm{GL}(n, q)$. *That is,* $A_\alpha = N_{\mathrm{GL}(n,q)}(A_\alpha)$.

Proof. Let $g \in N_{\mathrm{GL}(n,q)}(A_\alpha)$. Then we have $g^{-1}C_\alpha g \leqslant g^{-1}A_\alpha g = A_\alpha$. The conjugate of a Singer subgroup is also a Singer subgroup. On the other hand, it is known [13, Proposition 2.5] that A_α contains a *unique* Singer subgroup. In conjunction with $g^{-1}C_\alpha g \leqslant A_\alpha$, this implies that $g^{-1}C_\alpha g = C_\alpha$. This, in turn, implies that $g \in A_\alpha$, and therefore $N_{\mathrm{GL}(n,q)}(A_\alpha) = A_\alpha$. □

THEOREM 5. *Suppose that $n \geqslant 3$ and q are primes, and let A_α be the normalizer of a Singer subgroup in* $\mathrm{GL}(n, q)$. *Then two distinct nontrivial q-Steiner systems $\mathcal{S}_q(t, k, n)$ admitting A_α as a group of automorphisms are nonisomorphic.*

Proof. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be two distinct $\mathcal{S}_q(t, k, n)$ q-Steiner systems, both admitting A_α as a group of automorphisms. Then

$$\mathrm{Aut}(\mathcal{S}_1) = \mathrm{Aut}(\mathcal{S}_2) = A_\alpha \tag{1}$$

by Theorem 3. Now assume to the contrary that $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic, that is $\mathcal{S}_1^g = \mathcal{S}_2$ for some $g \in \mathrm{GL}(n, q)$. Let $a \in A_\alpha$. Then it follows from (1) that

$$\mathcal{S}_2^{g^{-1}ag} = \mathcal{S}_1^{ag} = \mathcal{S}_1^g = \mathcal{S}_2 \tag{2}$$

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

and therefore $g^{-1}ag \in \mathrm{Aut}(\mathcal{S}_2) = A_\alpha$. Since (2) holds for all $a \in A_\alpha$, we conclude that g must belong to the normalizer of A_α, which is A_α itself by Lemma 4. But for $g \in A_\alpha$, we have $\mathcal{S}_1^g = \mathcal{S}_1$ by (1). Hence $\mathcal{S}_2 = \mathcal{S}_1$, a contradiction. □

We next show how to classify the subspaces of $\mathbb{F}_q^n$ into orbits under the action of various groups. Fix a primitive element α of $\mathbb{F}_{q^n}$, and write a k-subspace X of $\mathbb{F}_q^n$ as $X = \{\mathbf{0}, \alpha^{x_1}, \alpha^{x_2}, \ldots, \alpha^{x_m}\}$, where $m = q^k - 1$ and $x_1, x_2, \ldots, x_m \in \mathbb{Z}/(q^n-1)$. For $x \in \mathbb{Z}/(q^n-1)$, let $\rho(x)$ be the minimal cyclotomic representative for x, that is $\rho(x) = \min\{xq^i \mod (q^n - 1) : 0 \leqslant i \leqslant n-1\}$. We define:

$$\begin{aligned} \mathrm{inv}_F(X) &\stackrel{\text{def}}{=} \{\rho(x_i) : 1 \leqslant i \leqslant m\}, \\ \mathrm{inv}_S(X) &\stackrel{\text{def}}{=} \{x_i - x_j : 1 \leqslant i, j \leqslant m \text{ with } i \neq j\}, \\ \mathrm{inv}_N(X) &\stackrel{\text{def}}{=} \{\rho(x_i - x_j) : 1 \leqslant i, j \leqslant m \text{ with } i \neq j\}. \end{aligned} \tag{3}$$

The notation in (3) stems from invariance under the action of the various groups of interest (to us), as explained in the following lemma.

LEMMA 6.

(1) *If two k-subspaces X, Y of $\mathbb{F}_q^n$ are in the same orbit under the action of the Galois group* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *then* $\mathrm{inv}_F(X) = \mathrm{inv}_F(Y)$.

(2) *If two k-subspaces X, Y of $\mathbb{F}_q^n$ are in the same orbit under the action of the Singer subgroup C_α then* $\mathrm{inv}_S(X) = \mathrm{inv}_S(Y)$.

(3) *If two k-subspaces X, Y of $\mathbb{F}_q^n$ are in the same orbit under the action of the normalizer A_α of the Singer subgroup C_α then* $\mathrm{inv}_N(X) = \mathrm{inv}_N(Y)$.

Proof. Let $X = \{\mathbf{0}, \alpha^{x_1}, \alpha^{x_2}, \ldots, \alpha^{x_m}\}$ be a k-subspace of $\mathbb{F}_q^n$, with $x_1, x_2, \ldots, x_m$ in $\mathbb{Z}/(q^n-1)$. The action of the generator of C_α on X increases $x_1, x_2, \ldots, x_m$ by one modulo $q^n - 1$, thereby preserving the differences between them. The action of the Frobenius automorphism ϕ on X multiplies each x_i by q modulo $q^n - 1$, thereby leaving it in the same cyclotomic coset. □

3. Kramer–Mesner computer search

Constructing t-designs over $\mathbb{F}_q$ is equivalent to solving certain systems of linear Diophantine equations. Let $\mathbf{M}$ be a $\{0, 1\}$ matrix with rows and columns indexed by the t-subspaces and the k-subspaces of $\mathbb{F}_q^n$, respectively; there is a 1 in row X and column Y of $\mathbf{M}$ if and only if t-subspace X is contained

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

in k-subspace Y. With this definition, a t-(n, k, λ) design over $\mathbb{F}_q$ is precisely a $\{0, 1\}$ solution to

$$\mathbf{M}\, x = (\lambda, \lambda, \ldots, \lambda)^T. \tag{4}$$

Unfortunately, for most parameters of interest, finding solutions to the resulting large systems of equations is outside the realm of computational feasibility.

However, if we impose a prescribed group of automorphisms A on a putative solution, thereby reducing the size of the problem, the situation can still be described in terms of a system of linear equations. In this case, the rows and columns of the matrix $\mathbf{M}^A$ correspond to A-orbits of t-subspaces and k-subspaces; the entries of $\mathbf{M}^A$ are nonnegative integers, possibly greater than 1. This is analogous to a well-known technique in design theory that is called the Kramer–Mesner method after its developers [36]. For more details on applications of the Kramer–Mesner method in the context of designs over $\mathbb{F}_q$, see [7].

There are several group-theoretic algorithms that, given a prescribed group A acting on a set of finite structures, compute the orbits under A and produce the corresponding Kramer–Mesner matrix. For more details, see [7, 43]. In our case, the Kramer–Mesner matrix $\mathbf{M}^A$, where A is the normalizer of a Singer subgroup, can be also computed directly using the invariants in Lemma 6.

In order to find a solution to (4) for a given Kramer–Mesner matrix $\mathbf{M}^A$, we observe that when $\lambda = 1$, the system of equations in (4) reduces to an instance of the *exact cover* problem [32]. That is, we wish to find a set $\mathcal{S}$ of columns of $\mathbf{M}^A$ such that for each row of $\mathbf{M}^A$, there is exactly one column of $\mathcal{S}$ containing 1 in this row. The exact cover problem can be solved efficiently using the dancing links algorithm of Knuth. For more on this, see [28, 32].

We now specialize the above to the case of the q-Steiner system $\mathcal{S}_2(2, 3, 13)$. At first, the matrix $\mathbf{M}$ in (4) has $\begin{bmatrix}13\\2\end{bmatrix} = 11\,180\,715$ rows and $\begin{bmatrix}13\\3\end{bmatrix} = 3\,269\,560\,515$ columns, where $\begin{bmatrix}n\\k\end{bmatrix}$ is the q-binomial coefficient with $q = 2$. We need to find an exact cover of the rows of $\mathbf{M}$ consisting of some

$$|\mathcal{S}_2(2, 3, 13)| = \begin{bmatrix}13\\2\end{bmatrix} \Big/ \begin{bmatrix}3\\2\end{bmatrix} = 1\,597\,245$$

columns. However, the resulting instance of the exact cover problem is well beyond the domain of feasibility of existing algorithms. Instead, we prescribe the normalizer A_α of a Singer subgroup of $\mathrm{GL}(13, 2)$ as a group of automorphisms. Specifically, we have used the Singer subgroup generated by the primitive element $\alpha \in \mathbb{F}_{2^{13}}$ which is a root of the polynomial $x^{13} + x^{12} + x^{10} + x^9 + 1$. We note that the specific choice of the primitive element is unimportant, in the sense that the set of Singer subgroups (and, thereby, also the set of their normalizers) forms a conjugacy class of subgroups of $\mathrm{GL}(n, q)$. By Theorem 2, we have $|A_\alpha| = 13(2^{13} - 1) = 106\,483$. The orbits of 2-subspaces and 3-subspaces under

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

the action of A_α are all full length, resulting in a Kramer–Mesner matrix $\mathbf{M}^{A_\alpha}$ with $\begin{bmatrix}13\\2\end{bmatrix}/106\,483 = 105$ rows and $\begin{bmatrix}13\\3\end{bmatrix}/106\,483 = 30\,705$ columns. Since all the orbits have full length $|A_\alpha|$, we need to find an exact cover consisting of $|\mathcal{S}_2(2,3,13)|/|A_\alpha| = 15$ columns of $\mathbf{M}^{A_\alpha}$. One such set of columns corresponds to the 15 subspaces of $\mathbb{F}_2^{13}$ listed below:

$$\begin{gathered}\{0,1,1249,5040,7258,7978,8105\},\ \{0,7,1857,6681,7259,7381,7908\},\\ \{0,9,1144,1945,6771,7714,8102\},\ \{0,11,209,1941,2926,3565,6579\},\\ \{0,12,2181,2519,3696,6673,6965\},\ \{0,13,4821,5178,7823,8052,8110\},\\ \{0,17,291,1199,5132,6266,8057\},\ \{0,20,1075,3939,3996,4776,7313\},\\ \{0,21,2900,4226,4915,6087,8008\},\ \{0,27,1190,3572,4989,5199,6710\},\\ \{0,30,141,682,2024,6256,6406\},\ \{0,31,814,1161,1243,4434,6254\},\\ \{0,37,258,2093,4703,5396,6469\},\ \{0,115,949,1272,1580,4539,4873\},\\ \{0,119,490,5941,6670,6812,7312\}.\end{gathered} \tag{5}$$

Each 3-subspace $\{\mathbf{0},\alpha^{x_1},\alpha^{x_2},\ldots,\alpha^{x_7}\}$ is specified in (5) in terms of the exponents $\{x_1, x_2, \ldots, x_7\}$ of its nonzero elements. The A_α-orbits of the 15 subspaces in (5) form a q-Steiner system $\mathcal{S}_2(2,3,13)$, thereby proving Theorem 1.

The first solution to the exact cover problem instantiated by the Kramer–Mesner matrix $\mathbf{M}^{A_\alpha}$ was found in about two hours on a personal computer. After about a month, we have found 512 distinct solutions. By Theorem 5, these solutions give rise to 512 nonisomorphic $\mathcal{S}_2(2,3,13)$ q-Steiner systems. We note, however, that classifying *all* the solutions to the exact cover instance specified by $\mathbf{M}^{A_\alpha}$ does not appear to be computationally feasible.

Inspired by the positive results for $\mathcal{S}_2(2,3,13)$, we have searched extensively for other q-Steiner systems, with various parameters, while imposing certain groups of automorphisms. We were able to resolve definitively the seven cases listed below. Unfortunately, in all these cases the outcome was negative. Our results show that q-Steiner systems with the following parameters and automorphisms do not exist:

$$\begin{aligned}\mathcal{S}_2(2,3,7),&\ \text{Galois group } \mathrm{Gal}(\mathbb{F}_{2^7}/\mathbb{F}_2)\ \text{(order 7)}\\ \mathcal{S}_2(3,4,8),&\ \text{Singer subgroup (order 255)}\\ \mathcal{S}_2(2,4,10),&\ \text{normalizer of Singer subgroup (order 10\,230)}\\ \mathcal{S}_2(2,4,13),&\ \text{normalizer of Singer subgroup (order 106\,483)}\\ \mathcal{S}_2(3,4,10),&\ \text{normalizer of Singer subgroup (order 10\,230)}\\ \mathcal{S}_3(2,3,7),&\ \text{Singer subgroup (order 2\,186)}\\ \mathcal{S}_5(2,3,7),&\ \text{normalizer of Singer subgroup (order 546\,868).}\end{aligned} \tag{6}$$

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

This extends upon the previous work on nonexistence of q-Steiner systems [16, 18, 35, 50]. E.g., it was shown in [35] that a q-Steiner system $\mathcal{S}_2(2, 3, 7)$ admitting a Singer subgroup as a group of automorphisms does not exist.

4. Related results

Obviously, an $\mathcal{S}_2(2, 3, 13)$ q-Steiner system gives rise to an $S(2, 7, 8191)$ Steiner system: simply represent each subspace of $\mathbb{F}_2^{13}$ by the characteristic vector of the set of its nonzero elements. We observe that Steiner systems with these parameters were already known [2, Table 3.3]. Notably, however, it follows from [18, Theorem 3.2] that $\mathcal{S}_2(2, 3, 13)$ also gives rise to an $S(3, 8, 8192)$ Steiner system. No $S(3, 2^k, 2^n)$ Steiner systems with $2^k \geqslant 8$ were previously known [12, 18]. The $S(3, 8, 8192)$ Steiner system can be used in various constructions (for example, those of [5, 12, 23]) to produce new $S(3, 8, v)$ Steiner systems for many other values of v.

Following [17, 34], we let $\mathcal{A}_q(n, d, k)$ denote the size of the largest subspace code in $\mathbb{F}_q^n$ of constant dimension k and minimum subspace distance d. Then the existence of $\mathcal{S}_2(2, 3, 13)$ implies that $\mathcal{A}_2(13, 4, 3) = 1\,597\,245$ (the upper bound $\mathcal{A}_2(13, 4, 3) \leqslant 1\,597\,245$ follows from [17, Theorem 1]).

The new $\mathcal{S}_2(2, 3, 13)$ q-Steiner systems found in Section 3 also produce new diameter-perfect codes in the corresponding Grassmann graph. Precious few examples of such codes are known. For more on the connection between q-Steiner systems and diameter-perfect codes in a Grassmann graph, see [3, 44].

In the remainder of this section, we expound upon the connection between q-Steiner systems and difference families. Recall from [1] that a (v, k, λ) *difference family* over an additive group G of order v is a collection $B_1, B_2, \ldots, B_s$ of k-subsets of G such that every nonidentity element of G occurs exactly λ times in the multiset $\{a - b : a, b \in B_i,\ a \neq b,\ 1 \leqslant i \leqslant s\}$.

THEOREM 7. *Let k and n be coprime, and suppose there exists an $\mathcal{S}_2(2, k, n)$ q-Steiner system admitting a Singer subgroup C_α as a group of automorphisms. Then there exists a $(2^n - 1, 2^k - 1, 1)$ difference family over the group $\mathbb{Z}/(2^n-1)$.*

Proof. Fix a primitive element α of $\mathbb{F}_{2^n}$, and let φ be an isomorphism from the multiplicative group of $\mathbb{F}_{2^n}$ to $\mathbb{Z}/(2^n-1)$ defined by $\varphi(\alpha^i) = i$. We extend φ to subspaces $X = \{\mathbf{0}, \alpha^{x_1}, \alpha^{x_2}, \ldots, \alpha^{x_m}\}$ of $\mathbb{F}_2^n$ in the obvious way, by defining

$$\varphi(X) \stackrel{\text{def}}{=} \{x_1, x_2, \ldots, x_m\} \subseteq \mathbb{Z}/(2^n-1).$$

Now let $\mathcal{S}$ be an $\mathcal{S}_2(2, k, n)$ q-Steiner system admitting C_α as a group of automorphisms. Partition the subspaces of $\mathcal{S}$ into orbits under the action of C_α.

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

Since k and n are coprime, $2^k - 1$ and $2^n - 1$ are also coprime, which implies that all the orbits have full length $|C_\alpha| = 2^n - 1$. It follows that the number of orbits is given by

$$s = \frac{|\mathcal{S}_2(2,k,n)|}{|C_\alpha|} = \frac{2^{n-1}-1}{(2^k-1)(2^{k-1}-1)}.$$

We choose (arbitrarily) one subspace from each orbit. Let $X_1, X_2, \ldots, X_s$ be the resulting set of orbit representatives. We claim that $\varphi(X_1), \varphi(X_2), \ldots, \varphi(X_s)$ is a $(2^n-1, 2^k-1, 1)$ difference family over $\mathbb{Z}/(2^n-1)$.

Indeed, consider an arbitrary nonzero element $a \in \mathbb{Z}/(2^n-1)$. Observe that a can be obtained as a difference of two group elements in exactly $2^n - 1$ ways: $(a+i)-i$ for $i = 0,1,\ldots,2^n-2$. To each such pair $\{a+i, i\}$, there corresponds a 2-subspace $\{\mathbf{0}, \alpha^i, \alpha^{a+i}, \alpha^i+\alpha^{a+i}\}$, and to each such 2-subspace, there corresponds a unique k-subspace of $\mathcal{S}$. All such k-subspaces of $\mathcal{S}$ are in the same orbit under the action of C_α, and every k-subspace in this orbit contains $\{\mathbf{0}, \alpha^j, \alpha^{a+j}, \alpha^j+\alpha^{a+j}\}$ for some j. It follows that a occurs at least once as a difference of two elements of $\varphi(X)$, where X is the representative of the corresponding orbit. But the total number of differences in the set $\{a-b \ : \ a,b \in \varphi(X_i), a \neq b, \ 1 \leqslant i \leqslant s\}$ is given by $s(2^k-1)(2^k-2) = 2^n - 2$, which completes the proof. □

We observe that, in fact, the following more general result is true: if k and n are coprime, then an $\mathcal{S}_q(2,k,n)$ q-Steiner system that admits a Singer subgroup as a group of automorphisms gives rise to a $((q^n-1)/(q-1), \ (q^k-1)/(q-1), \ 1)$ difference family over $\mathbb{Z}/((q^n-1)/(q-1))$. We omit the proof, which is similar to the proof of Theorem 7.

In order to obtain an (8191,7,1) difference family from the 15 sets in (5), first adjoin to each such set $\{x_1, x_2, \ldots, x_7\}$ the sets $\{2^i x_1, 2^i x_2, \ldots, 2^i x_7\}$ modulo 8191, for $i = 1, 2, \ldots, 12$ (thereby accounting for the action of the Galois group). It is easy to verify that the resulting $15 \cdot 13 = 195$ sets indeed form an (8191,7,1) difference family over $\mathbb{Z}/(8191)$. We note that (8191, 7, 1) difference families over $\mathbb{Z}/(8191)$ were already known. They were obtained by Greig [22] using a modification of a construction method due to Wilson [53].

5. Discussion and open problems

There is no good reason to believe that many q-Steiner systems, other than $\mathcal{S}_2(2,3,13)$, would not exist. In particular, we conjecture as follows.

CONJECTURE 8. *If $n \geqslant 13$ is a prime such that $n \equiv 1 \pmod 6$ then there exists a q-Steiner system $\mathcal{S}_2(2,3,n)$.*

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

The apparent large number of isomorphism classes of $\mathcal{S}_2(2, 3, 13)$ q-Steiner systems suggests that an $\mathcal{S}_2(3, 4, 14)$ q-Steiner system might exist. A more general open question is whether nontrivial q-Steiner systems $\mathcal{S}_q(t, k, n)$ exist for parameters other than $q = 2$, $t = 2$, and $k = 3$.

In fact, in light of our results, the main question is no longer whether q-Steiner systems exist but rather how they can be found. Not only should computer-aided searches be carried out, but one should also consider algebraic and combinatorial constructions of either specific q-Steiner systems or even infinite families of q-Steiner systems (for example, in the framework of difference sets).

Acknowledgements

The research of Tuvi Etzion was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12. The research of Patric Östergård was supported in part by the Academy of Finland under Grant No. 132122. The research of Alexander Vardy was supported in part by the United States National Science Foundation under Grants CCF-1116820 and CCF-1405119. The authors are grateful to the organizers of the conference TRENDS IN CODING THEORY, held in Ascona, Switzerland, between October 28, 2012, and November 2, 2012. The final pieces of this work were put together at this conference. The COST Action IC1104, titled *'Random Network Coding and Designs over* GF(q)*'*, provided some of the impetus for gathering four of the authors together in Ascona. The authors also thank Don Knuth for making available his dancing links software. Last but not least, we are grateful to Eimear Byrne, who checked our results and found a crucial typo in an earlier version of this paper.

Supplementary materials

Supplementary materials are available at http://dx.doi.org/10.1017/fmp.2016.5

References

[1] R. J. R. Abel and M. Buratti, 'Difference families', in *Handbook of Combinatorial Designs*, 2nd edn, (eds. C. J. Colbourn and J. H. Dinitz) (Chapman & Hall/CRC, Boca Raton, 2007), 392–410.

[2] R. J. R. Abel and M. Greig, 'BIBDs with small block size', in *Handbook of Combinatorial Designs*, 2nd edn, (eds. C. J. Colbourn and J. H. Dinitz) (Chapman & Hall/CRC, Boca Raton, 2007), 72–79.

[3] R. Ahlswede, H. K. Aydinian and L. H. Khachatrian, 'On perfect codes and related concepts', *Des. Codes Cryptogr.* **22** (2001), 221–237.

[4] R. Baer, *Linear Algebra and Projective Geometry* (Academic Press, New York, 1952).

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, 2nd edn, Vol. I. (Cambridge University Press, Cambridge, 1999).
[6] A. Beutelspacher, 'Parallelismen in unendlichen projektiven Raumen endlicher Dimension', *Geom. Dedicata* **7** (1978), 499–506.
[7] M. Braun, A. Kerber and R. Laue, 'Systematic construction of q-analogs of designs', *Des. Codes Cryptogr.* **34** (2005), 55–70.
[8] P. Cameron, 'Generalisation of Fisher's inequality to fields with more than one element', in *Combinatorics*, (eds. T. P. McDonough and V. C. Mavron), London Math. Soc. Lecture Note, 13 (Cambridge University Press, Cambridge, 1974), 9–13.
[9] P. Cameron, 'Locally symmetric designs', *Geom. Dedicata* **3** (1974), 65–76.
[10] A. Cayley, 'On the triadic arrangements of seven and fifteen things', *Philos. Mag.* **37** (1850), 50–53.
[11] H. Cohn, 'Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients', *Amer. Math. Monthly* **111** (2004), 487–495.
[12] C. J. Colbourn and J. H. Dinitz (Eds.), *Handbook of Combinatorial Designs*, 2nd edn, (Chapman & Hall/CRC, Boca Raton, 2007).
[13] A. Cossidente and M. J. de Resmini, 'Remarks on Singer cyclic groups and their normalizers', *Des. Codes Cryptogr.* **32** (2004), 97–102.
[14] P. Delsarte, 'Association schemes and t-designs in regular semilattices', *J. Combin. Theory Ser.* A **20** (1976), 230–243.
[15] R. H. Dye, 'Maximal subgroups of symplectic groups stabilizing spreads II', *J. Lond. Math. Soc.* **40**(2) (1989), 215–226.
[16] T. Etzion, 'Covering of subspaces by subspaces', *Des. Codes Cryptogr.* **72** (2014), 405–421.
[17] T. Etzion and A. Vardy, 'Error-correcting codes in projective space', *IEEE Trans. Inform. Theory* **57** (2011), 1165–1173.
[18] T. Etzion and A. Vardy, 'On q-analogs for Steiner systems and covering designs', *Adv. Math. Commun.* **5** (2011), 161–176.
[19] L. Euler, 'Consideratio quarumdam serierum quae singularibus proprietatibus sunt praeditae', *Novi Comment. Acad. Sci. Petropolitanae* **3**(1750–1751) 10–12. 86–108; *Opera Omnia, Ser. I*, vol. 14, B. G. Teubner, Leipzig, 1925, pp. 516–541.
[20] A. Fazeli, S. Lovett and A. Vardy, 'Nontrivial t-designs over finite fields exist for all t', *J. Combin. Theory Ser. A* **127** (2014), 149–160.
[21] J. R. Goldman and G.-C. Rota, 'On the foundations of combinatorial theory IV: finite vector spaces and Eulerian generating functions', *Stud. Appl. Math.* **49** (1970), 239–258.
[22] M. Greig, 'Some balanced incomplete block design constructions', *Congr. Numer.* **77** (1990), 121–134.
[23] H. Hanani, 'A class of three-designs', *J. Combin. Theory Ser.* A **26** (1979), 1–19.
[24] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi and B. Leong, 'A random linear network coding approach to multicast', *IEEE Trans. Inform. Theory* **52** (2006), 4413–4430.
[25] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).
[26] W. M. Kantor, 'Linear groups containing a Singer cycle', *J. Algebra* **62** (1980), 232–234.
[27] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs* (Springer, Berlin, 2006).
[28] P. Kaski and O. Pottonen, 'Libexact user guide, Version 1.0', HIIT Technical Reports 2008-1, Helsinki Institute for Information Technology, 2008.
[29] P. Keevash, 'The existence of designs', Preprint 2014, arXiv:1401.3665.
[30] M. Kiermaier and R. Laue, 'Derived and residual subspace designs', *Adv. Math. Commun.* **9** (2015), 105–115.

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5

[31] T. P. Kirkman, 'On a problem in combinations', *Cambridge Dublin Math. J.* **II** (1847), 191–204.
[32] D. E. Knuth, 'Dancing links', in *Millennial Perspectives in Computer Science* (eds. J. Davies, B. Roscoe and J. Woodcock) (Palgrave Macmillan, Basingstoke, 2000), 187–214.
[33] E. Koelink and W. van Assche, 'Leonhard Euler and a q-analogue of the logarithm', *Proc. Amer. Math. Soc.* **137** (2009), 1663–1676.
[34] R. Koetter and F. R. Kschischang, 'Coding for errors and erasures in random network coding', *IEEE Trans. Inform. Theory* **54** (2008), 3579–3591.
[35] A. Kohnert and S. Kurz, 'Construction of large constant dimension codes with a prescribed minimum distance', in *Mathematical Methods in Computer Science*, (eds. J. Calmet, W. Geiselmann and J. Müller-Quade) Lecture Notes in Computer Science, 5393 (Springer, Berlin, 2008), 31–42.
[36] E. Kramer and D. Mesner, 't-designs on hypergraphs', *Discrete Math.* **15** (1976), 263–296.
[37] R. Laue, 'Eine konstruktive Version des Lemmas von Burnside', *Bayreuther Math. Schr.* **28** (1989), 111–125.
[38] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd edn (Cambridge University Press, Cambridge, 2001).
[39] K. Metsch, 'Bose-Burton type theorems for finite projective, affine and polar spaces', in *Surveys in Combinatorics* (eds. J. D. Lamb and D. A. Preece) London Math. Soc. Lecture Note, 267 (Cambridge University Press, Cambridge, 1999), 137–166.
[40] M. Miyakawa, A. Munemasa and S. Yoshiara, 'On a class of small 2-designs over GF(q)', *J. Combin. Des.* **3** (1995), 61–77.
[41] J. Plücker, *System der analytischen Geometrie: auf neue Betrachtungsweisen gegründet, und insbesondere eine ausführliche Theorie der Curven dritter Ordnung enthaltend*, (Duncker und Humblot, Berlin, 1835).
[42] D. K. Ray-Chaudhuri and N. M. Singhi, 'q-analogues of t-designs and their existence', *Linear Algebra Appl.* **114/115** (1989), 57–68.
[43] B. Schmalz, 'The t-designs with prescribed automorphism group, new simple 6-designs', *J. Combin. Des.* **1** (1993), 125–170.
[44] M. Schwartz and T. Etzion, 'Codes and anticodes in the Grassmann graph', *J. Combin. Theory Ser.* A **97** (2002), 27–42.
[45] J. Steiner, 'Combinatorische Aufgabe', *J. reine angew. Math.* **45** (1853), 181–182.
[46] H. Suzuki, '2-designs over GF(2^m)', *Graphs Combin.* **6** (1990), 293–296.
[47] H. Suzuki, '2-designs over GF(q)', *Graphs Combin.* **8** (1992), 381–389.
[48] L. Teirlinck, 'Non-trivial t-designs without repeated blocks exist for all t', *Discrete Math.* **65** (1987), 301–311.
[49] S. Thomas, 'Designs over finite fields', *Geom. Dedicata* **21** (1987), 237–242.
[50] S. Thomas, 'Designs and partial geometries over finite fields', *Geom. Dedicata* **63** (1996), 247–253.
[51] J. Tits, 'Sur les analogues algébriques des groupes semi-simples complexes', in *Colloque d'Algébre Supèrieure, tenu á Bruxelles du 19 au 22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick* (Louvain, Paris, Librairie Gauthier-Villars, 1957), 261–289.
[52] J. Wang, 'Quotient sets and subset-subspace analogy', *Adv. Appl. Math.* **23** (1999), 333–339.
[53] R. M. Wilson, 'Cyclotomy and difference families in elementary abelian groups', *J. Number Theory* **4** (1972), 17–47.
[54] R. W. Yeung, *Information Theory and Network Coding* (Springer, Berlin, 2008).

Downloaded from https://www.cambridge.org/core. Aalto University, on 04 Apr 2017 at 09:10:48, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fmp.2016.5