On the Existence of $q$-Analogs of Steiner Systems

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

Abstract A $q$-analog of a Steiner system (briefly, $q$-Steiner system), denoted by $S = S_q[t, k, n]$, is a set 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 $S$. 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 known nontrivial $q$-Steiner systems with $t \geq 2$ are constructed. Specifically, $S_2[2, 3, 13]$ $q$-Steiner systems are found by requiring that their automorphism group 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.

Keywords exact cover · Frobenius automorphism group · $q$-analog · Singer subgroup · spread · Steiner system

T. Etzion was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12. P.R.J. Östergård was supported in part by the Academy of Finland, under Grant No. 132122.

Michael Braun
Faculty of Computer Science
University of Applied Sciences Darmstadt
D-64295 Darmstadt, Germany

Tuvi Etzion
Department of Computer Science, Technion
Haifa 32000, Israel

Patric R. J. Östergård
Department of Communications and Networking
Aalto University School of Electrical Engineering
P.O. Box 13000, FI-00076 Aalto, Finland

Alexander Vardy
Department of Electrical and Computer Engineering
University of California San Diego
La Jolla, CA 92093, USA

Alfred Wassermann
Department of Mathematics
University of Bayreuth
D-95440 Bayreuth, Germany
1 Introduction

An \( S(t, k, v) \) Steiner system is a collection of \( k \)-subsets, called blocks, of a \( v \)-set (of points), such that each \( t \)-subset of the \( v \)-set is contained in exactly one block. This paper is devoted to the existence of \( q \)-analogs of Steiner systems, also known as \( q \)-Steiner systems. Throughout this work, we assume that \( q \geq 2 \) is a prime power.

An \( S_q[t, k, n] \) \( q \)-Steiner system is a collection \( S \) of \( k \)-dimensional subspaces of \( \mathbb{F}_q^n \) (\( k \)-subspaces for short) such that each \( t \)-subspace of \( \mathbb{F}_q^n \) is contained in exactly one element of \( S \). Such \( q \)-Steiner systems can be readily constructed for \( t = k \) and \( k = n \) and are called trivial. Moreover, \( S_q[1, k, n] \) \( q \)-Steiner systems are known as spreads and exist if and only if \( k \) divides \( n \) [21, Chap. 24]. No other \( q \)-Steiner systems are known so far.

Indeed, the existence of nontrivial \( S_q[t, k, n] \) \( q \)-Steiner systems with \( t \geq 2 \) has tantalized researchers for decades and has been addressed in various studies including [2, 9, 22, 24, 27, 28]. In particular, much attention has been put on the smallest possible case of \( S_2[2, 3, 7] \). Actually, Metsch [22] conjectured that nontrivial \( q \)-Steiner systems for \( t \geq 2 \) do not exist. Whereas positive results have been missing for \( q \)-Steiner systems, there has been progress on the more general problem of finding \( q \)-analogs of \( t \)-designs, for which it is required that each \( t \)-subspace be contained in \( \lambda \) \( k \)-subspaces [5, 23, 25–28]. Also the corresponding packing and covering problems, with the requirement that each \( t \)-subspace be contained in at most one and at least one \( k \)-subspace, respectively, have been addressed [7–9, 19].

It should be emphasized that one of the main reasons why these issues have received a lot of attention in the recent years are their applications for error-correction in networks, under randomized network coding, as shown in [8, 18].

In the current paper, we carry out a computer-aided search for \( S_2[2, 3, 13] \) \( q \)-Steiner systems after imposing a structure on these via a prescribed group of automorphisms. Indeed, this approach is successful and leads to the discovery of the first known nontrivial \( q \)-Steiner system with \( t \geq 2 \).

The paper is organized as follows. In Section 2 we consider automorphisms of Steiner structures in general and the normalizer of a Singer subgroup of a general linear group in particular. The computational problem that arises in the current work and a solution are presented in Section 3, which is concluded by a discussion of some corollaries of the new result and problems for further research.

2 Automorphisms of \( q \)-Steiner Systems

We consider the action of the group \( G \) of bijective incidence-preserving mappings on the set of subspaces of \( \mathbb{F}_q^n \). We know from the Fundamental Theorem of Projective Geometry [3] that \( G \cong \Gamma L(n, q) \) (the general semilinear group), which in turn is isomorphic to the general linear group \( GL(n, q) \) when \( q \) is a prime.

The action of \( G \cong \Gamma L(n, q) \) on single subspaces extends in the obvious way to sets of subspaces, and thereby to \( q \)-Steiner systems. Given a set \( S \) of subspaces of \( \mathbb{F}_q^n \) and a group element \( g \in G \), we denote the image of \( S \) under the action of \( g \) by \( S^g \). We say that two sets of subspaces \( S_1 \) and \( S_2 \) are isomorphic if there exists an element \( g \in G \) such that \( S_2 = S_1^g \). An element \( g \in G \) for which \( S^g = S \) is called an automorphism of \( S \). The automorphisms of a set \( S \) of subspaces form a group under composition, called the (full) automorphism group and denoted \( \text{Aut}(S) \).
subgroup of Aut(S) is called a group of automorphisms. As G acts transitively on the set of k-subspaces for any fixed k, the automorphism group of a nontrivial q-Steiner system is necessarily a proper subgroup of G.

Throughout the rest of this work, we assume that q is prime, whereby $G \cong \text{GL}(n,q)$. A standard technique for finding combinatorial objects is to prescribe a group of automorphisms and search for corresponding objects. For surveys of the theory and applications in design theory, where this approach has been very successful along the years, the reader is referred to [10, Sect. 6.3] and [15, Sect. 9.2]. By prescribing a group of automorphisms, the construction problem is simplified, but choosing the right groups can be a challenge. We shall now discuss certain apposite subgroups of $\text{GL}(n,q)$.

Vectors in $\mathbb{F}_q^n$ can be interpreted as elements of the field $\mathbb{F}_{q^n}$. Let $\alpha$ be a primitive element in $\mathbb{F}_{q^n}$. A Singer cycle of $\text{GL}(n,q)$ is an element of order $q^n - 1$. Such elements always exist, and correspond to multiplication by $\alpha$ in the multiplicative group $\mathbb{F}_{q^n}^* = \{\alpha^0, \alpha^1, \ldots, \alpha^{q^n-2}\}$ of $\mathbb{F}_{q^n}$. The group generated by a Singer cycle is called a Singer subgroup and its $q^n - 1$ elements correspond to multiplication by $\alpha^i$, $0 \leq i \leq q^n - 2$ in $\mathbb{F}_{q^n}^*$.

Another subgroup of $\text{GL}(n,q)$ is obtained via the Frobenius automorphism group of $\mathbb{F}_{q^n}$, which is cyclic of order n and maps $\alpha^i$ to $(\alpha^i)^q$ in $\mathbb{F}_{q^n}^*$, where $0 \leq i \leq n - 1$ specifies an element in the group. The normalizer of a subgroup $H \leq G$ is defined as $N_G(H) = \{g \in G : gHg^{-1} = H\}$. The following well-known result can be found in, for example, [13, pp. 187, 188].

**Theorem 1** The normalizer of a Singer subgroup of $\text{GL}(n,q)$ has order $n(q^n - 1)$ and is isomorphic to the semidirect product of the Singer subgroup and the Frobenius automorphism group of $\mathbb{F}_{q^n}$.

The following theorem follows from a more general result by Kantor [14] and is stated explicitly in [6].

**Theorem 2** Let $n$ be a prime. Then, except when $n = q = 2$, the normalizer of a Singer subgroup is a maximal subgroup of $\text{GL}(n,q)$.

A Singer subgroup and the normalizer of a Singer subgroup have earlier been successful choices when prescribing automorphisms for various types of $q$-analog structures [5,8]. The following lemma for the case $q = 2$, $t = 2$ is useful in the sequel.

**Lemma 1** A collection $S$ of k-subspaces of $\mathbb{F}_2^n$ is an $S_2[2,k,n]$ q-Steiner system if and only if each pair of distinct non-zero vectors from $\mathbb{F}_2^n$ occurs in exactly one element of $S$.

**Proof** This follows from the definition of a q-Steiner system and the fact that any two of of the three non-zero vectors in a 2-subspace, $\mathbf{u}$ and $\mathbf{v}$, defines the third one, $\mathbf{u} + \mathbf{v}$. $\Box$

We shall now connect an $S_2[2,k,n]$ with a Singer subgroup as a group of automorphisms to a difference family. A $(v,k,\lambda)$ difference family over an additive
group $G$ is a collection $B_1, B_2, \ldots, B_m$ of $k$-subsets of $G$ such that every nonidentity element of $G$ occurs $\lambda$ times in the multiset $\{a - b : a, b \in B_i, \ a \neq b, 1 \leq i \leq m\}$.

For a set $X = \{x_1, x_2, \ldots, x_m\}$ of powers of a primitive element $\alpha$, such as the non-zero elements of a subspace, we define $\text{inv}(X) := \{x_i - x_j : i \neq j\}$.

**Lemma 2** If two sets $X, Y$ of powers of $\alpha \in \mathbb{F}_2^n$ are in the same orbit under the Singer cycle, then $\text{inv}(X) = \text{inv}(Y)$.

**Theorem 3** If there exists an $\mathbb{S}_2[2, k, n]$ $q$-Steiner system with the Singer subgroup 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** We show that a transformation between the involved structures via the mapping between vectors in $\mathbb{F}_2^n$ and powers of a primitive element $\alpha$ in the multiplicative group $\mathbb{F}_2^\ast$ ($\cong \mathbb{Z}_{2^n-1}$) gives the desired result.

Consider an $\mathbb{S}_2[2, k, n]$ $q$-Steiner system $S$ with a Singer subgroup as a group of automorphisms, and carry out the above mentioned transformation to the nonzero vectors in the orbit representatives of the $k$-dimensional elements of $S$. In this manner, $(2^k - 1)$-subsets of $\mathbb{F}_2^n$ are obtained and, by extracting the power $i$ of each element $\alpha^i$, $(2^k - 1)$-subsets of $\mathbb{Z}_{2^n-1}$.

Now consider an arbitrary nonidentity element $a \in \mathbb{Z}_{2^n-1}$. This element can be obtained as a difference in exactly $2^n - 1$ ways: $(a + i) - i$ for $0 \leq i \leq 2^n - 2$. By Lemma 1 each pair $\{a + i, i\}$ occurs in exactly one element of $S$ and by Lemma 2 such a pair occurs in an orbit representative. Consequently, the difference $a$ occurs once in exactly one of the $(2^k - 1)$-subsets of $\mathbb{Z}_{2^n-1}$.

The implication in Theorem 3 also works in the opposite direction if one restricts the difference families considered to those that are mapped to subspaces with the transformation used. Indeed, theoretical results needed in the current work can be adopted from the context of difference families, developed and discussed in, for example, [1] and [4, Chap. VII].

A generator of the Frobenius automorphism group corresponds to a *multiplier* in the framework of difference families. We cannot get arbitrary multipliers as only elements of $\text{GL}(n, 2)$ are considered. For elements of the Frobenius automorphism group of $\mathbb{F}_{q^n}$ we do know that $a + b = c$ implies that $a^{q^i} + b^{q^i} = (a + b)^{q^i} = c^{q^i}$.

**3 Computer Search and Results**

The problem of finding a $q$-analog of a $t$-design can be formulated in terms of a system of linear Diophantine equations. Let $M$ be a 0-1 matrix with rows and columns corresponding to the $t$-subspaces and the $k$-subspaces of $\mathbb{F}_q^n$, respectively. We assume that $k > t$ and let the 1s in $M$ denote inclusion. By definition, a solution to $Mx = [\lambda, \lambda, \ldots, \lambda]^T$ is then a $q$-analog of a $t$-design. The problem of finding solutions for these large systems is commonly out of computational feasibility for interesting parameters, but the problem of finding $q$-analogues of a $t$-design with a prescribed group $A$ can also be handled within this framework.

With prescribed automorphisms, the entries of the matrix $M^A$, where rows and columns correspond to $A$-orbits instead of single subspaces, may be larger than 1.
This technique—which is analogous to a standard technique in design theory that is called the Kramer–Mesner method after its developers—is described in detail in [5].

For the case of \( \lambda = 1 \), that is, for \( S_q[t,k,n] \) \( q \)-Steiner systems, the system of linear Diophantine equations can be reduced to an instance of the exact cover problem [17]. For algorithms and software for solving instances of the exact cover problem, see [16,17].

For \( S_q[2,3,13] \) \( q \)-Steiner systems we get a matrix \( M \) with 11 180 715 rows and 3 269 560 515 columns. Since an \( S_q[2,3,13] \) \( q \)-Steiner system consists of 1 597 245 3-subspaces, a solution vector has to contain that many 1s. It is apparent that it is not feasible to attack the corresponding instance in a direct way with existing algorithms. However, by prescribing a group along the discussion in the previous section, one can reduce the size of the instance.

By prescribing the normalizer of a Singer subgroup of \( \text{GL}(13,2) \) as a group \( A \) of automorphisms, we arrive at an instance of the exact cover problem represented by the \( A \)-incidence matrix \( M^A \) with 105 rows and 30 705 columns of which 25 572 columns have admissible entries less than 2. Since \( n = 13 \) is a prime, all orbits represented by the columns of \( M^A \) have trivial stabilizers in \( A \) and hence full length \( |A| = 106 483 \). Consequently, we want to find 1 597 245/106 483 = 15 columns in \( M^A \) such that each row is covered exactly by one column.

In our implementation, we considered the primitive element \( \alpha \in \mathbb{F}_q^\ast \) that is a root of the primitive polynomial \( x^{13} + x^4 + x^3 + x + 1 \). A computer search then found several solutions for this instance of the exact cover problem, one of which is as follows (the powers of \( \alpha \) of the nonzero elements in the 3-subspaces are listed):

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

On a contemporary personal computer, we found the first solution after a couple of hours. We let the program run for more than a month and during this period 401 solutions were found. However, it does not seem feasible to find all solutions of this type since estimates indicate a total run time far outside what is currently feasible, beyond one million years.

By Theorem 2, we know that the prescribed group is the (full) automorphism group of the \( q \)-Steiner systems in this case. Otherwise, if the full automorphism group would be \( \text{GL}(n,2) \), all \( k \)-subspaces would be contained in one single orbit and the \( q \)-Steiner system would be trivial.

The fact that the group is a maximal subgroup of \( \text{GL}(13,2) \) makes it possible to say much more. Actually, one can prove that the systems obtained are pairwise nonisomorphic. The following theorem and its proof are analogous to those in [20, Lemma 2.1].
**Lemma 3** Let $A \leq \text{GL}(n, q) = G$ be the automorphism group of two $\mathcal{S}_q[t, k, n]$ $q$-Steiner systems $\mathcal{S}_1$ and $\mathcal{S}_2$. Then an element in $G$ that maps the $k$-subspaces of $\mathcal{S}_1$ onto those of $\mathcal{S}_2$ lies in the normalizer $N_G(A)$.

**Proof** Let $S_2^g = S_2$ for some $g \in G$, and consider an arbitrary $a \in \text{Aut}(\mathcal{S}_1)$. Since $S_2^g^{-1}ag = S_2^g = S_2$, we have that $g^{-1}ag \in \text{Aut}(\mathcal{S}_2) = \text{Aut}(\mathcal{S}_1) = A$. By definition, $g \in N_G(A)$.

**Theorem 4** Let $n$ be a prime, and let $A \leq \text{GL}(n, q) = G$ be the normalizer of a Singer subgroup. Then two distinct nontrivial $\mathcal{S}_q[t, k, n]$ $q$-Steiner systems $\mathcal{S}_1$ and $\mathcal{S}_2$ with automorphism group $A$ are nonisomorphic.

**Proof** Nontrivial $q$-Steiner systems must obviously have $n \geq 3$. Assume that $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic. Then, by Lemma 3, $S_2^g = S_2$ for some $g \in N_G(A)$. As $A$ is the normalizer of a Singer subgroup and $n$ is a prime, we know by Theorem 2 that the only overgroups of $A$—and possible values of $N_G(A)$—are $A$ and $G$. But any normal subgroup of $G$ is either a subgroup of the center $Z(\text{GL}(n, q))$ or an overgroup of $\text{SL}(n, q)$ and $q - 1 = |Z(\text{GL}(n, q))| < |A| < |\text{SL}(n, q)|$ when $n \geq 3$. Hence $N_G(A) = A$, and $g \in A = \text{Aut}(\mathcal{S}_1)$ implies that $S_2^g = S_1$, which gives $\mathcal{S}_1 = \mathcal{S}_2$ and a contradiction.

Obviously, there are other groups than the group considered here for which $\mathcal{S}_2[2, 3, 13]$ $q$-Steiner systems might exist. Inspired by the positive results, further attempts were made to find other $q$-Steiner systems, considering various parameters and groups. The following nonexistence results were obtained in this manner (extending work in [8, 19]):

- $\mathcal{S}_2[2, 3, 7]$: Frobenius automorphism group, order 7
- $\mathcal{S}_2[3, 4, 8]$: Singer subgroup, order 255
- $\mathcal{S}_2[2, 4, 10]$: Normalizer of Singer subgroup, order 10230
- $\mathcal{S}_2[2, 4, 13]$: Normalizer of Singer subgroup, order 106483
- $\mathcal{S}_2[3, 4, 10]$: Normalizer of Singer subgroup, order 10230
- $\mathcal{S}_3[3, 3, 7]$: Singer subgroup, order 2186
- $\mathcal{S}_5[2, 3, 7]$: Normalizer of Singer subgroup, order 546868

To get an $(8191, 7, 1)$ difference family from (1), the 15 sets should be developed by, for each set $\{s_1, s_2, \ldots, s_7\}$, constructing the sets $\{2^is_1, 2^is_2, \ldots, 2^is_7\}$ modulo 8191 for $0 \leq i \leq 12$. This gives $15 \cdot 13 = 195$ sets in total. It is already known that an $(8191, 7, 1)$ difference family exists; such a difference family is obtained in [11] using a construction developed by Wilson [29].

We get an $S(2, 7, 8191)$ Steiner system by developing each of the 195 sets of our $(8191, 7, 1)$ difference family by, for each set $\{s_1, s_2, \ldots, s_7\}$, constructing the sets $\{s_1 + i, s_2 + i, \ldots, s_7 + i\}$ modulo 8191 for $0 \leq i \leq 8190$; cf. [1, Remarks 16.5].

An $S(2, 7, 8191)$ Steiner system can also be obtained as a derived design of an $S(3, 8, 8192)$ Steiner system, which exists by the following theorem [9].

**Theorem 5** If there exists an $\mathcal{S}_2[2, k, n]$ $q$-Steiner system, then there exists an $S(3, 2^k, 2^n)$ Steiner system.
Such an $S(3, 8, 8192)$ Steiner system can further be applied to various constructions, such as those in [12], to get $S(3, 8, n)$ Steiner systems also for other values of $n$.

We give one further application of $q$-Steiner systems: it is proved in [2] that $q$-Steiner systems are diameter perfect codes.

There is no reason to believe that $q$-Steiner systems would not exist for any other parameters than those mentioned in the current work. We conjecture that $S_q[2, 3, n]$-Steiner systems exist at least whenever $n \equiv 1 \pmod{6}$ and $n \geq 13$ is a prime.

As a matter of fact, the main question is no longer whether further $q$-Steiner systems exist but how these can be found. Not only should computational attempts be carried out, but one should also consider the possibility of algebraic and combinatorial constructions of particular systems and recursively of infinite families (for example, in the framework of difference families).

The large number of isomorphism classes of $S_q[2, 3, 13]$ $q$-analog Steiner systems indicates that an $S_q[3, 4, 14]$ might exist. A general open question is whether non-trivial $S_q[t, k, n]$ $q$-analog Steiner systems exist for other parameters than $q = 2$, $t = 2$, and $k = 3$.

Acknowledgements The authors are grateful to Elisa Gorla, Joachim Rosenthal, and Amin Shokrollahi for organizing the conference “Trends in Coding Theory” in Ascona, Switzerland between October 28 and November 2, 2012, where the final pieces of the current work were put together. The authors also thank Prof. Donald Knuth for making available his dancing links software, which finally produced the very first solution.

References