21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

On the Automorphism Group of the Binary q-Analog of the Fano Plane

Michael Braun[1], Michael Kiermaier[2], and Anamari Nakić[3] *† ‡

Abstract

An $S_q[t,k,v]$ q-Steiner system is a collection of k-dimensional subspaces of the v-dimensional vector space $\mathbb{F}_q^v$ over the finite field $\mathbb{F}_q$ with q elements, called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly one block. The smallest admissible parameters for which a q-Steiner system could exist is $S_2[2,3,7]$. Up to now the issue whether q-Steiner systems with these parameters exist or not is still unsolved. In this paper we investigate the automorphism group of a putative $S_2[2,3,7]$ q-Steiner system. We conclude that in case of existence the automorphism group is cyclic and of order at most 4.

MSC2010—*51E10, 51E20, 05B05.*

Keywords—*Random network codes, designs over finite fields, q-Steiner systems, automorphism group.*

1. Introduction

Let $\mathbb{F}_q^v$ denote the v-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. A t-(v,k,λ) design over $\mathbb{F}_q$ is a collection of k-dimensional subspaces $\mathscr{B}$ of $\mathbb{F}_q^v$, which are called blocks, such that each t-dimensional subspace of $\mathbb{F}_q^v$ is contained in exactly λ elements of $\mathscr{B}$.

Since in this definition finite sets are replaced by finite vector spaces over finite fields and their orders are replaced by dimensions t-(v,k,λ) designs over $\mathbb{F}_q$ are called q-analogs of combinatorial designs. Thomas [16] introduced the notion of designs over finite fields.

In particular, t-$(v,k,1)$ designs over $\mathbb{F}_q$ are also called q-Steiner systems and will be abbreviated by $S_q[t,k,v]$. It is well-known that $S_q[1,k,v]$ q-Steiner systems exist if k divides v. For this set of parameters the corresponding q-Steiner systems are called trivial. We note that q-Steiner systems have applications for error-correction in networks, under randomized network coding, as shown in [11].

The issue whether $S_q[t,k,v]$ q-Steiner systems do exist for $t > 1$ tantalized many researchers [1, 7, 13, 16, 17] since the early 70s when Cameron [5, 6] extended the notion of designs over finite sets to designs over vector spaces. Recently, the existence of nontrivial q-Steiner systems could be proved [3] by an explicit construction for the parameters $S_2[2,3,13]$.

Nevertheless, there are many open cases to be considered. The existence of the q-analog of the Fano plane, a q-Steiner system with parameters $S_q[2,3,7]$, is still an unsolved issue which has attracted many authors [7, 8, 13, 14, 16, 17].

In this paper we investigate the automorphism group of a putative $S_2[2,3,7]$ q-Steiner system. The goal is to eliminate possible groups of automorphisms and restrict the automorphism group to some few cases.

2. Groups of Automorphisms

Let $G_k(\mathbb{F}_q^v)$ denote the set of k-dimensional subspaces of $\mathbb{F}_q^v$, called the Grassmannian, and let $\mathrm{GL}(\mathbb{F}_q^v)$ denote the general linear group of $\mathbb{F}_q^v$ whose elements are represented by $n \times n$ matrices. The elements α of $\mathrm{GL}(\mathbb{F}_q^v)$ act on the set of subspaces of V by left multiplication $\alpha K := \{\alpha x \mid x \in K\}$.

An element α of $\mathrm{GL}(\mathbb{F}_q^v)$ is called an automorphism of an $S_q[t,k,v]$ q-Steiner system $\mathscr{B}$ if $\mathscr{B} = \alpha\mathscr{B} := \{\alpha K \mid K \in B\}$. The set of all automorphisms $\mathrm{Aut}(\mathscr{B})$ of a q-Steiner system $\mathscr{B}$ forms a group, called the automorphism group of $\mathscr{B}$. Every subgroup of the automorphism group of a q-Steiner system is denoted as a group of automorphisms of the q-Steiner system.

If G is a subgroup of $\mathrm{GL}(\mathbb{F}_q^v)$ the G-orbit on a k-dimensional subspace K is denoted by $G(K) := \{\alpha K \mid \alpha \in G\}$. The G-incidence matrix $\mathbf{A}_{t,k}^G$ is defined to be the matrix whose rows and columns are indexed by the G-orbits on the set of t- and k-dimensional subspaces of $\mathbb{F}_q^v$, respectively. The entry indexed by the orbit $G(T)$ on $G_t(\mathbb{F}_q^v)$ and the orbit $G(K)$ on $G_k(V)$ is defined by

*[1]Faculty of Computer Science, University of Applied Sciences, Darmstadt, Germany, michael.braun@h-da.de

†[3]Lehrstuhl II für Mathematik, Universiät Bayreuth, Germany, michael.kiermaier@uni-bayreuth.de

‡[2]Department of Applied Mathematics, Faculty of Science, University of Zagreb, Croatia, anamari.nakic@fer.hr

$|\{K' \in G(K) \mid T \subseteq K'\}|$.

According to Kramer and Mesner [12] an $S_q[t,k,v]$ q-Steiner system admitting G as a group of automorphisms exists if and only if there is a zero-one column vector $\mathbf{x}$ satisfying

$$\mathbf{A}_{t,k}^{G}\mathbf{x} = \mathbf{1}, \qquad (1)$$

where $\mathbf{1}$ denotes the all-one column vector.

Two q-Steiner systems $\mathscr{B}$ and $\mathscr{B}'$ are called isomorphic with respect to $\mathrm{GL}(\mathbb{F}_q^v)$ if and only if there is an element $\alpha \in \mathrm{GL}(\mathbb{F}_q^v)$ mapping $\mathscr{B}$ onto $\mathscr{B}'$, i.e. $\mathscr{B}' = \alpha\mathscr{B}$. It is well-known [9] that the automorphism groups of isomorphic q-Steiner systems are conjugate. As an immediate consequence for a computer aided search of q-Steiner systems we obtain that it is sufficient to test exactly one representative G of the conjugacy classes of subgroups of the whole subgroup lattice of the general linear group $\mathrm{GL}(\mathbb{F}_q^v)$. Conjugate subgroups G and H yield the same existence results of q-Steiner system admitting G or H as group of automorphisms.

3. Successive Exclusion of Automorphism Groups

We are going to successively exclude possible automorphism groups of the $S_2[2,3,7]$ q-Steiner system which are subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$. Furthermore, by excluding a possible group we immediately exclude all subgroups within the same conjugacy class of subgroups. Since constructing representatives of all conjugacy classes of subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$ exceeds reasonable time limits we successively restrict the set of possible groups of automorphisms.

Cyclic subgroups

We start with the conjugacy classes of cyclic subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$. Using MAGMA [2] immediately produces representatives of the 60 conjugacy classes of subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$. For each of the computed representatives G we solved the Kramer-Mesner system (1) using an implementation of Knuth's dancing links algorithm [10]. For most of the 60 cyclic groups no solution does exist which means that they cannot occur as groups of automorphisms of an $S_2[2,3,7]$ q-Steiner system. The following nontrivial cyclic groups remained as open cases:

$$A = \left\langle \begin{bmatrix} 0&1&0&0&0&0&0\\ 1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1 \end{bmatrix} \right\rangle, |A| = 2$$

$$B = \left\langle \begin{bmatrix} 0&1&0&0&0&0&0\\ 1&1&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{bmatrix} \right\rangle, |B| = 3$$

$$C = \left\langle \begin{bmatrix} 1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&1&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&0&1&1 \end{bmatrix} \right\rangle, |C| = 3$$

$$D = \left\langle \begin{bmatrix} 0&0&0&1&0&0&0\\ 1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&1&0&1\\ 0&0&0&0&0&1&1 \end{bmatrix} \right\rangle, |D| = 4$$

$$E = \left\langle \begin{bmatrix} 0&0&0&1&0&0&0\\ 1&0&0&1&0&0&0\\ 0&1&0&1&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{bmatrix} \right\rangle, |E| = 5$$

$$F = \left\langle \begin{bmatrix} 1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&1&1&0&0&0\\ 0&0&0&0&0&0&1\\ 0&0&0&0&1&0&1\\ 0&0&0&0&0&1&0 \end{bmatrix} \right\rangle, |F| = 7$$

The size of a q-Steiner system with parameters $S_2[2,3,7]$ is given by the *q-packing bound* which is in this case 381 (cf. [15]).

Considering the orbits of E on the set of 3-dimensional subspaces of $\mathbb{F}_2^7$ we obtain one orbit of length one that must be fixed since $381 = 76 \cdot 5 + 1$.

Solving the slightly smaller system of equations showed that no $S_2[2,3,7]$ q-Steiner system does exist admitting E as group of automorphisms.

Considering the orbits of F on the set of 3-dimensional subspaces of $\mathbb{F}_2^7$ we obtain two orbits of length one and all other orbits have full length seven. Obviously the size $381 = 1 \cdot 3 + 7 \cdot 54$ cannot be combined of F-orbits since exactly three orbits of length one are required. Hence, an $S_2[2,3,7]$ q-Steiner system cannot admit F as group of automorphisms.

p-groups

The order of $\mathrm{GL}(\mathbb{F}_2^7)$ is given by $2^{21} \cdot 3^4 \cdot 5^1 \cdot 7^2 \cdot 31^1 \cdot 127^1$. According to Sylow's theorem subgroups of all admissible powers of prime factors of the order of $\mathrm{GL}(\mathbb{F}_2^7)$ do exist. For each prime factor we are now going to find the smallest power for which a group of automorphism of $S_2[2,3,7]$ could exist. We use MAGMA in order to compute the conjugacy classes of p-groups.

All subgroups of order 5, 7, 31, and 127 which are cyclic due to the prime order were already investigated with the result that they cannot occur as groups of automorphisms of $S_2[2,3,7]$. Hence, all these factors cannot occur in the order of the automorphism group.

There are four conjugacy classes of order 3^2 for which the Kramer-Mesner system (1) has no solutions. Finally, only the two mentioned groups B and C of order 3 could occur as subgroups of the automorphism group.

For the order 2^3 there exist 867 conjugacy classes of subgroups. Only 37 contain conjugates of A and D as subgroups of order 2 and 4. The Kramer-Mesner system (1) has again no solutions for each representative of the remaining 37 conjugacy classes. Hence at most 2^2 could occur as a power of 2 in the cardinality of the automorphism group. Checking the value 2^2 we get eight conjugacy classes of subgroups of this order where seven could again be eliminated by solving the Kramer-Mesner system (1). Only the mentioned group D remained as possible subgroup of the automorphism group of $S_2[2,3,7]$.

Summarizing, we obtain that the automorphism group of $S_2[2,3,7]$ has at most the cardinality $2^2 \cdot 3 = 12$.

Subgroups of order 6 and 12

Since the orders 2, 3, and 4 are already considered we construct conjugacy classes of subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$ of order 6 and of order 12 with MAGMA: There are 96 conjugacy classes of order 12 and twelve conjugacy classes of order 6. Solving the Kramer-Mesner system (1) again eliminates all these groups of order 12 and of order 6.

4. Conclusion

By successive elimination we determined that the possible automorphism group G of $S_2[2,3,7]$ (up to conjugation of subgroups with respect to $\mathrm{GL}(\mathbb{F}_2^7)$) is cyclic, has order at most 4, and satisfies $G \in \{\{1\}, A, B, C, D\}$.

5. Acknowledgements

The authors are grateful to the organizers of the conference "Conference on Random Network Codes and Designs over GF(q)" held at the Department of Mathematics of Ghent University, Belgium, from September 18–20, 2013, where the first steps towards the present paper were initiated. This conference was organized in the framework of the COST action IC1104, titled "Random Network Coding and Designs over GF(q)".

References

[1] A. Beutelspacher. Parallelismen in unendlichen projektiven Räumen endlicher Dimension. *Geometriae Dedicata*, 7:499–506, 1978.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System. I. The User Language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann. On the Existence of q-Analogs of Steiner Systems. *submitted*.

[4] M. Braun, A. Kerber, and R. Laue. Systematic Construction of q-Analogs of Designs. *Designs, Codes and Cryptography*, 34(1):55–70, 2005.

[5] P. Cameron. Generalisation of Fisher's Inequality to Fields with more than One Element. In T. P. McDonough and V. C. Mavron, editors, *Combinatorics, Proceedings of British Combinatorial Conference 1973*, volume 13 of *London Mathematical Society Lecture Notes*, pages 9–13. Cambridge University Press, 1974.

[6] P. Cameron. Locally Symmetric Designs. *Geometriae Dedicata*, 3:56–76, 1974.

[7] T. Etzion and A. Vardy. On q-Analogs of Steiner Systems and Covering Designs. *Advances in the Mathematics of Communications, Special Issue on ALCOMA'10 — Algebraic Combinatorics and Applications, April 11-18, 2010, Thurnau, Germany*, 5(2):161–176, 2011.

[8] O. Heden and P. A. Sissokho. On the Existence of a $(2,3)$-Spread in $V(7,2)$. arXiv:1101.5336, 2011.

[9] A. Kerber. *Applied Finite Group Actions*. Springer-Verlag, 1999.

[10] D. E. Knuth. Dancing links. In J. Davies, B. Roscoe, and J. Woodcock, editors, *Millennial Perspectives in*

Computer Science, pages 187–214. Palgrave Macmillan, Basingstoke, 2000.

[11] R. Koetter and F. R. Kschischang. *Coding for Errors and Erasures in Random Network Coding*. IEEE Trans. Inform. Theory 54, 35793591, 2008.

[12] E. Kramer and D. Mesner. t-Designs on Hypergraphs. *Discrete Mathematics*, 15(3):263–296, 1976.

[13] K. Metsch. Bose-Burton Type Theorems for Finite Projective, Affine and Polar Spaces. In Lamb and Preece, editors, *Surveys in Combinatorics, Lecture Notes Series*, volume 267. London Mathematical Society, 1999.

[14] M. Miyakawa, A. Munemasa, and S. Yoshiara. On a Class of Small 2-Designs over $GF(q)$. *Journal of Combinatorial Designs*, 3:61–77, 1995.

[15] M. Schwartz and T. Etzion. Codes and Anticodes in the Grassman Graph. *Journal of Combinatorial Theory, Series A*, 97:27–42, 2002.

[16] S. Thomas. Designs over Finite Fields. *Geometriae Dedicata*, 24:237–242, 1987.

[17] S. Thomas. Designs and Partial Geometries over Finite Fields. *Geometriae Dedicata*, 63:247–253, 1996.