AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **67(3)** (2017), Pages 470–475

Designs over the binary field from the complete monomial group

Michael Braun

Faculty of Computer Science
University of Applied Sciences
Darmstadt
Germany
michael.braun@h-da.de

Abstract

All known direct constructions of designs over finite fields arise by subgroups of the normalizer of a Singer cycle, by lifted special linear groups, or lifted general linear groups. Other types of non-trivial automorphism groups for which designs over finite fields do exist have not been mentioned so far. In this paper we construct the first non-trivial designs over finite fields admitting the lifted complete monomial group as group of automorphisms.

1 Introduction

In the following let V denote an n-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. A t-$(n,k,\lambda;q)$ design, also called t-(n,k,λ) design over $\mathbb{F}_q$, is a set $\mathcal{B}$ of k-dimensional subspaces, called blocks, of V if each t-dimensional subspace of V is contained in exactly λ members of $\mathcal{B}$.

More formally, if $\begin{bmatrix} V \\ k \end{bmatrix}$ denotes the set of k-dimensional subspaces of V the set $\mathcal{B}$ is a t-$(n,k,\lambda;q)$ design if

$$\mathcal{B} \subseteq \begin{bmatrix} V \\ k \end{bmatrix} \text{ and for all } T \in \begin{bmatrix} V \\ t \end{bmatrix} : |\{K \in \mathcal{B} \mid T \subseteq K\}| = \lambda.$$

Since Thomas [15] described the first non-trivial construction of t-designs over $\mathbb{F}_q$ with $t > 1$ in 1987, a family of 2-$(n,3,7;2)$ designs with $n \equiv \pm 1 \bmod 6$, only a few explicit constructions have been published. All these constructed designs over finite fields [1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14] admit

- non-trivial subgroups of the normalizer of a Singer cycle,
- the lifted special linear group, or
- the lifted general linear group.

In [6, 9] some of these designs were used as base for recursive constructions but automorphism groups of the resulting designs over finite fields have not been discussed.

In this paper we show that further subgroups can occur as groups of automorphisms. We show the following result.

Theorem 1. *There exist t-$(n,k,\lambda;q)$ designs for $t>1$ admitting the lifted complete monomial group as group of automorphisms.*

2 Automorphisms

By the fundamental theorem of projective geometry the automorphism group of the lattice of subspaces of V is the projective semilinear group $\mathrm{P\Gamma L}(V)$ for dimensions $n=\dim(V)\geq 3$. Any mapping $\alpha\in\mathrm{P\Gamma L}(V)$ is called an automorphism of a t-$(n,k,\lambda;q)$ design $\mathcal{B}$ if the blocks are mapped onto blocks of $\mathcal{B}$ again, i.e.

$$\alpha(\mathcal{B}):=\{\alpha(K)\mid K\in\mathcal{B}\}=\mathcal{B}.$$

The set of all automorphisms of $\mathcal{B}$ forms a subgroup of $\mathrm{P\Gamma L}(V)$ which is called the automorphism group of $\mathcal{B}$. It is denoted by $\mathrm{Aut}(\mathcal{B})$. Any subgroup $G\leq\mathrm{Aut}(\mathcal{B})$ is called a group of automorphisms of $\mathcal{B}$.

Let $G\leq\mathrm{P\Gamma L}(V)$. The orbit of G of a k-dimensional $K\in\begin{bmatrix}V\\k\end{bmatrix}$ is denoted by

$$G(K):=\{\alpha(K)\mid\alpha\in G\}$$

and the set of all orbits of G on the set of k-dimensional subspaces of V is indicated by

$$G\backslash\!\backslash\begin{bmatrix}V\\k\end{bmatrix}:=\left\{G(K)\mid K\in\begin{bmatrix}V\\k\end{bmatrix}\right\}.$$

Any t-$(n,k,\lambda;q)$ design $\mathcal{B}$ admits $G\leq\mathrm{P\Gamma L}(V)$ as a group of automorphisms if it consists of orbits of $G\backslash\!\backslash\begin{bmatrix}V\\k\end{bmatrix}$.

To obtain an appropriate selection of orbits of G on $\begin{bmatrix}V\\k\end{bmatrix}$ we consider the incidence matrix $A^G_{t,k}$ whose rows are indexed by the G-orbits on the set of t-subspaces of V and whose columns are indexed by the orbits on k-subspaces. The entry of $A^G_{t,k}$ corresponding to the orbits $G(T)$ and $G(K)$ is defined by

$$a^G_{T,K}:=|\{K'\in G(K)\mid T\subseteq K'\}|.$$

The following result is by Kramer and Mesner [10].

Theorem 2. *There exists a t-$(n,k,\lambda;q)$ design admitting the group $G\leq\mathrm{P\Gamma L}(V)$ as group of automorphisms if there is a 0-1-vector x satisfying*

$$A^G_{t,k}x=\begin{bmatrix}\lambda\\\vdots\\\lambda\end{bmatrix}.$$

The 0-1-vector x stands for the selection of G-orbits on $\begin{bmatrix}V\\k\end{bmatrix}$ whose union form the corresponding t-$(n,k,\lambda;q)$ design.

3 Lifting the complete monomial group

The complete monomial group $M(n,q)$ consists of all $n \times n$ matrices over $\mathbb{F}_q$ containing exactly one nonzero entry in each row and in each column. In fact $M(n,q)$ is isomorphic to the wreath product $S_n \wr_n \mathbb{F}_q^*$ where S_n denotes the symmetric group on n elements and it has the order $n!(q-1)^n$.

Let $\langle q^i \mid 0 \leq i < \ell \rangle$ denote the standard polynomial basis of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$ and let $\langle u_j \mid 0 \leq j < m \rangle$ denote the canonical basis of the vector space $\mathbb{F}_{q^\ell}^m$, i.e. u_i is the unit vector having a one in the position i and zero otherwise. Then $\langle b_k \mid 0 \leq k < m\ell \rangle$ where $b_{i+jm} = q^i u_j$ for $0 \leq i < \ell$ and $0 \leq j < m$ forms a basis of $\mathbb{F}_q^{m\ell}$. If $\alpha = [\alpha_{i,j}]$ denotes an element of $\mathrm{GL}(m, q^\ell)$ in matrix representation, it can be represented as an element of $\mathrm{GL}(m\ell, q)$ in matrix representation by $\bar{\alpha} = [\bar{\alpha}_{i,j}]$ where

$$\alpha b_j = \sum_{i=0}^{m\ell} \bar{\alpha}_{i,j} b_i, \quad 0 \leq i, j < m\ell.$$

Therefore any subgroup of $\mathrm{GL}(m, q^\ell)$ can be represented by elements of $\mathrm{GL}(m\ell, q)$. In particular the complete monomial group $M(m, q^\ell)$ can be considered as a subgroup of $\mathrm{GL}(m\ell, q)$ by lifting. In the following we consider the case $m > 1$ as lifting $M(1, q^\ell)$ gives exactly a Singer cycle of $\mathrm{GL}(\ell, q)$ which is not of interest in this paper since designs over finite fields are known to exist with this kind of groups of automorphisms. However in this paper we want to show that designs over finite fields do exist for other automorphism groups than the already mentioned ones in the introduction.

The monomial group $G = M(3,8) \leq \mathrm{GL}(3,8)$ which is generated by the following five matrices

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

yields the following isomorphic subgroup $\bar{G} \leq \mathrm{GL}(9,2)$

$$\left\langle \begin{bmatrix} Z & U & Z \\ U & Z & Z \\ Z & Z & U \end{bmatrix}, \begin{bmatrix} Z & U & Z \\ Z & Z & U \\ U & Z & Z \end{bmatrix}, \begin{bmatrix} S & Z & Z \\ Z & U & Z \\ Z & Z & U \end{bmatrix}, \begin{bmatrix} U & Z & Z \\ Z & S & Z \\ Z & Z & U \end{bmatrix}, \begin{bmatrix} U & Z & Z \\ Z & U & Z \\ Z & Z & S \end{bmatrix} \right\rangle$$

where

$$Z = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, S = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

The multiplication in the corresponding finite field $\mathbb{F}_8$ (in polynomial representation) is considered with respect to the irreducible reduction polynomial

$$p(z) = z^3 + z^2 + 1,$$

such that $2 \cdot 4 = 4 + 1$ holds which explains the submatrix S.

4 Result

We construct a new 2-$(9, 3, 49; 2)$ design admitting the lifted complete monomial subgroup $\bar{G} \leq \mathrm{GL}(9, 2)$ (which was described in the previous section) as group of automorphisms. Up to our knowledge a design with these parameters has not yet been constructed. As vector space we consider the canonical vector space $V = \mathbb{F}_2^9$. The design is given by a set of orbit representatives of $M(3, 8)$ on the set of 3-dimensional subspaces of V which can be obtained by solving the Kramer–Mesner system given in Theorem 2. Each orbit representative is a 3-dimensional subspace of V which is represented by a 9×3 matrix over $\mathbb{F}_2$

$$\Gamma = \begin{bmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \\ x_4 & y_4 & z_4 \\ x_5 & y_5 & z_5 \\ x_6 & y_6 & z_6 \\ x_7 & y_7 & z_7 \\ x_8 & y_8 & z_8 \end{bmatrix}$$

whose columns form a basis of the subspace. To get a compact representation of Γ we use the triple of integers

$$\left[\sum_{i=0}^{8} x_i 2^i, \sum_{i=0}^{8} y_i 2^i, \sum_{i=0}^{8} z_i 2^i \right].$$

Table 1 shows the orbit representatives of the constructed 2-$(9, 3, 49; 2)$ design.

Table 1: Orbit representatives of a 2-$(9, 3, 49; 2)$ design admitting the lifted complete monomial group

[100,128,256]	[132,32,256]	[212,32,256]	[76,32,256]	[204,32,256]
[132,160,256]	[148,160,256]	[84,160,256]	[12,160,256]	[140,160,256]
[92,160,256]	[68,96,256]	[196,96,256]	[20,96,256]	[84,96,256]
[140,96,256]	[92,96,256]	[220,96,256]	[148,224,256]	[12,224,256]
[76,224,256]	[204,224,256]	[28,224,256]	[92,224,256]	[146,36,256]
[114,36,256]	[242,36,256]	[10,36,256]	[74,36,256]	[42,36,256]
[170,36,256]	[234,36,256]	[218,36,256]	[58,36,256]	[105,36,256]
[187,36,256]	[210,164,256]	[114,164,256]	[202,164,256]	[234,164,256]
[201,164,256]	[105,164,256]	[217,164,256]	[121,164,256]	[219,164,256]
[388,144,288]	[196,144,288]	[452,144,288]	[332,144,288]	[204,144,288]
[324,400,288]	[196,400,288]	[452,400,288]	[76,400,288]	[132,80,288]
[388,80,288]	[68,80,288]	[12,80,288]	[140,80,288]	[460,80,288]
[132,336,288]	[68,336,288]	[196,336,288]	[204,336,288]	[132,464,288]
[324,464,288]	[452,464,288]	[140,464,288]	[402,260,288]	[338,260,288]
[466,260,288]	[330,260,288]	[458,260,288]	[329,260,288]	[473,260,288]
[219,260,288]	[475,260,288]	[146,132,288]	[402,132,288]	[210,132,288]
[10,132,288]	[74,132,288]	[330,132,288]	[154,132,288]	[346,132,288]
[17,132,288]	[81,132,288]	[209,132,288]	[9,132,288]	[73,132,288]
[457,132,288]	[89,132,288]	[339,132,288]	[139,132,288]	[203,132,288]
[459,132,288]	[27,132,288]	[155,132,288]	[91,132,288]	[475,132,288]
[210,388,288]	[394,388,288]	[74,388,288]	[202,388,288]	[154,388,288]
[410,388,288]	[346,388,288]	[273,388,288]	[337,388,288]	[73,388,288]
[201,388,288]	[473,388,288]	[339,388,288]	[219,388,288]	[458,68,288]
[154,68,288]	[410,68,288]	[474,68,288]	[145,68,288]	[209,68,288]
[201,68,288]	[457,68,288]	[147,68,288]	[403,68,288]	[139,68,288]
[459,68,288]	[155,68,288]	[219,68,288]	[74,148,288]	[458,148,288]
[73,148,288]	[201,148,288]	[75,148,288]	[331,148,288]	[475,148,288]
[202,404,288]	[218,404,288]	[474,404,288]	[201,404,288]	[457,404,288]
[217,404,288]	[75,404,288]	[331,404,288]	[459,404,288]	[475,404,288]
[138,84,288]	[458,84,288]	[410,84,288]	[474,84,288]	[393,84,288]
[201,84,288]	[153,84,288]	[395,84,288]	[203,84,288]	[411,84,288]
[475,84,288]	[458,340,288]	[410,340,288]	[201,340,288]	[409,340,288]
[155,340,288]	[410,212,288]	[329,212,288]	[331,212,288]	[74,468,288]
[73,146,292]	[329,146,292]	[233,402,292]	[89,402,292]	[345,402,292]
[377,402,292]	[233,82,292]	[153,338,292]	[153,202,292]	

References

[1] M. Braun, Some new designs over finite fields, In *ALCOMA'05—Proceedings of the Conference on Algebraic Combinatorics and Applications, Designs and Codes, April 3-10, 2005, Thurnau, Germany*, pp. 58–68. Bayreuther Mathematische Schriften 74 (2005).

[2] M. Braun, New 3-designs over the binary field, *Int. Electron. J. Geom.* 6(2) (2013), 79–87.

[3] M. Braun, New infinite series of 2-designs over the binary and ternary field, *Des. Codes Cryptogr.* 81(1) (2016), 145–152.

[4] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy and A. Wassermann, On the existence of q-analogs of Steiner systems, Forum of Mathematics, PI (2016), doi: 10.1017/fmp.2016.5.

[5] M. Braun, A. Kerber and R. Laue, Systematic construction of q-analogs of designs, *Des. Codes Cryptogr.* 34(1) (2005), 55–70.

[6] M. Braun, M. Kiermaier, A. Kohnert and R. Laue, Large sets of subspace designs, *J. Combin. Theory Ser. A* 147 (2017), 155–185.

[7] M. Braun, A. Kohnert, P. R. J. Östergård and A. Wassermann, Large sets of t-designs over finite fields, *J. Combin. Theory Ser. A* 124 (2014), 195–202.

[8] T. Itoh, A new family of 2-designs over $GF(q)$ admitting $SL_m(q^l)$, *Geom. Dedicata* 69 (1998), 261–286.

[9] M. Kiermaier and R. Laue, Derived and residual subspace designs, *Adv. Math. Commun.* 9(1) (2015), 105–115.

[10] E. Kramer and D. Mesner, t-Designs on hypergraphs, *Discrete Math.* 15(3) (1976), 263–296.

[11] M. Miyakawa, A. Munemasa and S. Yoshiara, On a class of small 2-designs over $GF(q)$, *J. Combin. Des.* 3 (1995), 61–77.

[12] H. Suzuki, 2-Designs over $GF(2^m)$, *Graphs Combin.* 6 (1990), 293–296.

[13] H. Suzuki, On the inequalities of t-designs over a finite field, *European J. Combin.* (1990) 11(6), 601–607.

[14] H. Suzuki, 2-Designs over $GF(q)$, *Graphs Combin.* 8 (1992), 381–389.

[15] S. Thomas, Designs over finite fields, *Geom. Dedicata* 24 (1987), 237–242.

(Received 17 Aug 2016)