

## NEW 3-DESIGNS OVER THE BINARY FIELD

MICHAEL BRAUN

(Communicated by Erdal ÖZÜSAĞLAM)

ABSTRACT. Designs over finite fields arise from ordinary designs on sets by replacing the sets by vector spaces over finite fields and orders of sets by dimension of vector spaces, i. e. a  $t - (v, k, \lambda; q)$  design is a set  $\mathcal{B}$  of  $k$ -subspaces of  $\mathbb{F}_q^v$  such that each  $t$ -subspace of  $\mathbb{F}_q^v$  is contained in exactly  $\lambda$  elements of  $\mathcal{B}$ . Nearly 25 years have been gone, since Simon Thomas published the first results on designs over finite fields and only a few designs with parameters  $t = 2$  and exactly one design with  $t = 3$  have been discovered so far. In this paper we give a second new parameter set with  $t = 3$  for which designs over finite fields exist.

### 1. INTRODUCTION

Let  $\mathbb{F}_q$  be the finite field with  $q$  elements where  $q$  is a prime power and let  $G_k(v, q)$  denote the set of  $k$ -subspaces of the  $v$ -dimensional vector space  $\mathbb{F}_q^v$ .

A  $t$ -design over  $\mathbb{F}_q$  or a  $t - (v, k, \lambda; q)$  design is a collection  $\mathcal{B}$  of  $k$ -subspaces of  $\mathbb{F}_q^v$  which are called blocks such that each  $t$ -subspace of  $\mathbb{F}_q^v$  is contained in exactly  $\lambda$  members of  $\mathcal{B}$ . More formally,  $\mathcal{B}$  is a  $t - (v, k, \lambda; q)$  design, if and only if

$$\mathcal{B} \subseteq G_k(v, q) \wedge \forall T \in G_t(v, q) : |\{K \in \mathcal{B} \mid T \subseteq K\}| = \lambda.$$

The design  $\mathcal{B}$  is called *simple* if no repeated blocks occur in  $\mathcal{B}$ , otherwise the design is called *non-simple*. We are interested in simple designs over finite fields.

Simple designs over finite fields were introduced by Thomas [10] in 1987. He constructed the first non-trivial 2-design over a finite field which is a design with parameters

$$2 - (v, 3, 7; 2)$$

for  $v \geq 7$  and  $\pm 1 \equiv v \pmod{6}$ . Thomas used a geometric construction in a projective plane.

In 1989 Suzuki [8, 9] extended Thomas' family of 2-designs to a family of designs with parameters

$$2 - (v, 3, q^2 + q + 1; q)$$

for  $v \geq 7$  and  $\pm 1 \equiv v \pmod{6}$  admitting a Singer cycle.

---

*Date:* Received: March 29, 2012. Accepted: October 6, 2013.  
*2000 Mathematics Subject Classification.* 51E10, 51E20, 05B05, 05E20.  
*Key words and phrases.* designs over finite fields, q-analogs.

In 1995 Miyakawa, Munemasa, and Yoshiara [6] gave a classification of

$$2 - (7, 3, \lambda; q)$$

designs for  $q = 2, 3$  with small  $\lambda$ .

Given a design with parameters

$$2 - (\ell, 3, q^3(q^{\ell-5} - 1)/(q - 1); q)$$

for  $\ell \equiv 5 \pmod{6(q-1)}$  which admits a Singer cycle of  $GL(\ell, q)$  Itoh [3] constructed in 1998 a new family of

$$2 - (m\ell, 3, q^3(q^{\ell-5})/(q - 1); q)$$

designs for an arbitrary  $m \geq 3$  which admits the action of  $SL(m, q^\ell)$ . This construction applied to Suzuki's designs provided a new family of 2-designs over  $\mathbb{F}_q$ .

In 2005 Braun, Kerber, and Laue [2] published the first (and until now only known) 3-design over a finite field, a

$$3 - (8, 4, 11; 2)$$

design admitting the normalizer of a Singer cycle, as well as the smallest 2-design known, a design with parameters

$$2 - (6, 3, 3; 2)$$

Further parameter sets on 2-designs were also published in [1].

## 2. THE CONSTRUCTION APPROACH

In this section we just recall the well-known method which has already been applied successfully to the construction of designs over finite fields [1, 2]. The approach is due to Kramer and Mesner [4] and describes the construction of ordinary  $t - (v, k, \lambda)$  designs on sets with a prescribed group of automorphisms, as subgroup of the symmetric group  $\text{Sym}(v)$ , using an incidence matrix between orbits on the  $t$ -subsets and on the  $k$ -subsets.

Generalizing this construction we introduce the incidence matrix between orbits on vectorspaces. Let  $G$  be a subgroup of the complete general linear group  $GL(v, q)$  and let  $G(T_0), \dots, G(T_{n-1})$  be the  $G$ -orbits on the set of  $t$ -subspaces of  $\mathbb{F}_q^v$  with representatives  $T_i$ ,  $0 \leq i < n$ . Furthermore, let  $G(K_0), \dots, G(K_{m-1})$  be the  $G$ -orbits on the set of  $k$ -subspaces with representatives  $K_j$ ,  $0 \leq j < m$ . The  $q$ -analog of a Kramer-Mesner matrix, also called  $q$ -Kramer-Mesner matrix, denoted by  $A_{t,k}^G$ , is an  $n \times m$  matrix with entries

$$a_{i,j}^G = |\{K \in G(K_j) \mid T_i \subseteq K\}|,$$

i. e. the entry counts the number of  $k$ -subspaces in the  $j$ th orbit on  $k$ -subspaces containing a fixed representative of the  $i$ th orbit on  $t$ -subspaces. The definition of these entries is independent from the chosen representative  $T_i$ . Now, the following theorem describes the construction of designs with a prescribed group of automorphisms:

**Theorem 1** ( $q$ -analog of Kramer-Mesner). *Let  $G$  be a subgroup of  $GL(v, q)$ . Then there exists a  $t - (v, k, \lambda; q)$  design having  $G$  as a group of automorphisms if and*

only if there exists a 0-1-solution  $x$  solving the system of Diophantine equations

$$A_{t,k}^G \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}.$$

If  $x = (\dots x_j \dots)^t$  denotes such a solution then

$$\mathcal{B} = \bigcup_{j:x_j=1} G(K_j)$$

defines the corresponding  $t - (v, k, \lambda; q)$  design.

### 3. NEW 3 - (8, 4, 15; 2)-DESIGNS

So far the only known  $t$ -design over a finite field with  $t > 2$  is the 3 - (8, 4, 11; 2) design (resp. the corresponding supplemented 3 - (8, 4, 20; 2) design) mentioned the first section. Now, in this paper we give four new 3-designs over the binary field  $\mathbb{F}_2$ , computed by the Kramer-Mesner approach.

To construct the  $q$ -Kramer-Mesner matrix  $A_{t,k}^G$  we used the computer algebra package DISCRETAQ [1] and to solve the Diophantine system of equations we applied the LLL-algorithm [5].

As group of automorphisms  $G \leq \langle \sigma, \phi^2 \rangle$  to be prescribed we used a subgroup of the normalizer of the Singer cycle, generated by the Singer cycle  $\sigma$ , a group of order 255 and the square  $\phi^2$  of Frobenius automorphism, a cyclic group of order 4:

$$\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\phi^2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

The  $q$ -Kramer-Mesner matrix  $A_{3,4}^G$  between the orbits of  $G$  on the set of 3- resp. 4-subspaces has 105 rows and 217 columns:

$$A_{3,4}^G = \left( \begin{array}{c|c} A^{(ul)} & A^{(ur)} \\ \hline A^{(bl)} & A^{(br)} \end{array} \right)$$

The four parts  $A^{(ul)}$ ,  $A^{(ur)}$ ,  $A^{(bl)}$ , and  $A^{(br)}$  of the matrix are depicted in Tables 1–4. Note, that the “dots” represent zero entries.

Considering the Kramer-Mesner system of Diophantine equations

$$A_{3,4}^G \cdot x = \begin{pmatrix} 15 \\ \vdots \\ 15 \end{pmatrix}$$

and running a LLL-based solver yields four 0/1-solution vectors:

$$x^{(0)} = (0010101111001010001111100010100100001100110111010101001000111011110100110001111001111001111001101100100001010100111000011010100001000001100101000011110101001110000101111100101111000000111101000110001100)^t$$

$$x^{(1)} = (001110011100101110110100001000010000111010111100011101100011101101000101001101101010001100011110011100111010001010011010101100001110000100110011100100111010100100110110101100001111000000111100001010110101000101001100)^t$$

$$x^{(2)} = (0110001010011001111110001101110010011001100000001011100110001000110110100011100110110100100101010110101100000011111111010100101111000110011000001001000111010010001100111000110000011101010110001000010111011010010)^t$$

$$x^{(3)} = (0111000011011000110110001111010010011010111000010011110110010100111100000110000110110001110001010110110011001000111111100100001111110001000010100001110000010100110001001110001010000111010011100100001100011111010010)^t$$

Every of these solutions corresponds to a new  $3 - (8, 4, 15; 2)$  design.

#### REFERENCES

- [1] Braun, M., Designs over Finite Fields. Bayreuther Mathematische Schriften, 74(2005), 58–68.
- [2] Braun, M., Kerber, A. and Laue, R., Systematic Construction of  $q$ -Analogues of Designs. Designs, Codes and Cryptography, 34(2005), no.1, 55–70.
- [3] Itoh, T., A New Family of 2-Designs over  $GF(q)$  Admitting  $SL_m(q^t)$ . Geometriae Dedicata, 69(1998), 261–286.
- [4] Kramer, E. and Mesner, D.,  $t$ -Designs on Hypergraphs. Discrete Mathematics, 15(1976), no:3, 263–296.
- [5] Lenstra, A.K., Lenstra, H.W. and Lovász, L., Factoring Polynomials with Rational Coefficients. Mathematische Annalen, 261(1982), no.4, 515–534.
- [6] Miyakawa, M., Munemasa, A. and Yoshiara, S., On a Class of Small 2-Designs over  $GF(q)$ . Journal of Combinatorial Designs, 3(1995), 61–77.
- [7] Ray-Chaudhuri, D.K. and Schram, E.J., Designs on Vectorspaces Constructed Using Quadratic Forms. Geometriae Dedicata, 42(1992), 1–42.

- [8] Suzuki, H., 2-Designs over  $GF(2^m)$ . *Graphs and Combinatorics*, 6(1990), 293–296.
- [9] Suzuki, H., 2-Designs over  $GF(q)$ . *Graphs and Combinatorics*, 8(1992), 381–389.
- [10] Thomas, S., Designs over Finite Fields. *Geometriae Dedicata*, 24(1987), 237–242.
- [11] Thomas, S., Designs and Partial Geometries over Finite Fields. *Geometriae Dedicata*, 63(1996), 247–253.

UNIVERSITY OF APPLIED SCIENCES DARMSTADT, FACULTY OF COMPUTER SCIENCE, GERMANY  
*E-mail address:* michael.braun@h-da.de









TABLE 4. Kramer-Mesner-matrix: part  $A^{(br)}$

Matrix content: A grid of numerical values (0, 1, 2, 3, 4, 13, 21, 24, 31, 41, 112, 113, 114, 115, 121, 122, 123, 124, 125, 131, 132, 133, 134, 141, 142, 143, 144, 145, 151, 152, 153, 154, 155, 161, 162, 163, 164, 165, 171, 172, 173, 174, 175, 181, 182, 183, 184, 185, 191, 192, 193, 194, 195) arranged in a grid pattern.