

A NOTE ON THE EXISTENCE OF NON-SIMPLE DESIGNS OVER FINITE FIELDS

MICHAEL BRAUN

(Communicated by Edoardo BALLICO)

ABSTRACT. Designs over finite fields arise by replacing finite sets by vector spaces and orders of sets by dimensions of vector spaces. More formally, a $t - (v, k, \lambda; q)$ design is a collection of k -subspaces over \mathbb{F}_q^v , called blocks, such that each t -subspace is contained in exactly λ blocks. Such a design over a finite field is called simple, if no repeated blocks occur in the collection. Otherwise, the design is called non-simple. In this paper we prove that for every parameter set $0 < t < k < v - t$ and each subgroup G of the general linear group $GL(v, q)$ a non-simple $t - (v, k, \lambda; q)$ design exists for some appropriate $\lambda > 0$ admitting G as a group of automorphisms.

1. INTRODUCTION

A $t - (v, k, \lambda; q)$ design is a collection \mathcal{B} of k -subspaces of the v -dimensional vector space \mathbb{F}_q^v over the finite field \mathbb{F}_q , called blocks, such that each t -subspace of \mathbb{F}_q^v is contained in exactly λ blocks of \mathcal{B} . The design \mathcal{B} is called *simple* if no repeated blocks occur in \mathcal{B} , otherwise the design is called *non-simple*.

Designs over finite fields have been studied now for almost 25 years, since Thomas [13] published the first family of simple 2-designs. Further results on the construction of simple 2- and 3-designs appeared in [1, 2, 4, 6, 11, 12, 14]. No simple t -designs over finite fields are known for $t > 3$. Necessary and sufficient conditions for the existence of simple $t - (v, k, 1; q)$ designs, also called q -Steiner systems were published in [3, 9]. No q -Steiner systems have been constructed so far with $t > 1$.

Furthermore, some families of non-simple 2- and 3-designs have been defined using quadratic forms in [8]. No further results are known for non-simple designs over finite fields.

In this paper we also consider *non-simple* t -designs over finite fields and prove the following main theorem:

Theorem 1. *Let $0 < t < k < v - t$ be natural numbers and let G be a subgroup of the general linear group $GL(v, q)$. Then there exists a non-simple $t - (v, k, \lambda; q)$ design admitting G as a group of automorphisms for some appropriate $\lambda > 0$.*

Date: Received: July 23, 2011 and Accepted: February 02, 2012.

2010 Mathematics Subject Classification. 05B25.

Key words and phrases. Designs over Finite Fields, Non-simple Designs.

2. INCIDENCE MATRICES

In this section we describe the well-known method which has been already applied successfully for the construction of simple designs over finite fields. The approach is due to Kramer and Mesner [5] and describes the construction of ordinary $t-(v, k, \lambda)$ designs on sets with a prescribed group of automorphisms, a subgroup of the symmetric group S_v , using an incidence matrix between orbits on the t -subsets and on the k -subsets.

Generalizing this construction we introduce some notation and define the incidence matrix between orbits on vector spaces.

If $V := \mathbb{F}_q^v$ denotes the v -dimensional vector space over the finite field \mathbb{F}_q with q elements, the set

$$\begin{bmatrix} V \\ k \end{bmatrix} := \{K \leq V \mid \dim(K) = k\}$$

denotes the set of k -subspaces of V . It is called the *Grassmannian*. The order of this set is the *Gaussian number*, also called *q -Binomial coefficient*. It is abbreviated by $\begin{bmatrix} v \\ k \end{bmatrix}_q$ and satisfies

$$\begin{bmatrix} v \\ k \end{bmatrix}_q := \left| \begin{bmatrix} V \\ k \end{bmatrix} \right| = \frac{(q^v - 1)(q^{v-1} - 1) \cdots (q^{v-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

A subgroup G of the general linear group $GL(v, q)$ acts on $\begin{bmatrix} V \\ k \end{bmatrix}$. The orbit of G on a k -subspace K is denoted by

$$G(K) := \{gK \mid g \in G\},$$

where the set of all orbits is abbreviated by $G \backslash \begin{bmatrix} V \\ k \end{bmatrix} := \{G(K) \mid K \in \begin{bmatrix} V \\ k \end{bmatrix}\}$.

The q -analog of a Kramer-Mesner matrix, also called q -Kramer-Mesner matrix, denoted by

$$A_{t,k}^G = (a_{TK}^G) = (\cdots | a_{*K}^G | \cdots)$$

is defined by

$$a_{TK}^G := |\{K' \in G(K) \mid T \subseteq K'\}|$$

where T resp. K runs through a transversal of the orbits of G on $\begin{bmatrix} V \\ t \end{bmatrix}$ resp. $\begin{bmatrix} V \\ k \end{bmatrix}$.

The special case $G = \{1\}$ yields the ordinary incidence matrix

$$A_{t,k}^{\{1\}} = A_{t,k} = (a_{TK})$$

with entries

$$a_{TK} := \begin{cases} 1, & T \subseteq K \\ 0, & \text{otherwise,} \end{cases}$$

where T resp. K runs through all subspaces of $\begin{bmatrix} V \\ t \end{bmatrix}$ resp. $\begin{bmatrix} V \\ k \end{bmatrix}$. The addition of all columns yields:

$$\sum_K a_{*K}^G = \left(\begin{bmatrix} v-t \\ v-k \end{bmatrix}_q, \dots, \begin{bmatrix} v-t \\ v-k \end{bmatrix}_q \right)^t$$

Now with the generalization of the Kramer-Mesner-theorem [5] to non-simple designs and considering subspaces instead of subsets we get the following construction theorem:

Theorem 2. *Let G be a subgroup of $GL(v, q)$. Then a non-simple $t-(v, k, \lambda; q)$ design exists if and only if there is a solution vector x with non-negative integral entries of the Diophantine System of equations:*

$$A_{t,k}^G \cdot x = (\lambda, \dots, \lambda)^t$$

3. STRICT MONOTONY OF THE NUMBER OF ORBITS

An auxiliary result which will be used in the proof of our main theorem is about the orbit sizes: If $0 < t < k < v - t$ are natural numbers and if G denotes a subgroup of $GL(v, q)$, the orbits of G on the set of t - resp. k -subspaces satisfy the inequality $|G \setminus \binom{V}{t}| < |G \setminus \binom{V}{k}|$. This result is already known and was proven in paper [7, 10]. Since these proofs were made in a more general setting, namely in the theory of group actions on posets, we sketch the proof in our context of subspaces, for the sake of completeness. The idea is that we use a linear representation to determine the number of orbits and consider a linear transformation on factor spaces.

We define a $\binom{v}{k}_q$ -dimensional vector space over the field \mathbb{Q} of all rational numbers: The set

$$\mathbb{Q}_k := \{f : \binom{V}{k} \rightarrow \mathbb{Q}\}$$

forms a \mathbb{Q} vector space with basis vectors $\{f_K \mid K \in \binom{V}{k}\}$, where

$$f_K : \binom{V}{k} \rightarrow \mathbb{Q}, S \mapsto \begin{cases} 1, & S = K, \\ 0, & \text{otherwise.} \end{cases}$$

The dimension of \mathbb{Q}_k is obviously $\binom{v}{k}_q$. Now, we define a subspace \mathbb{Q}_k^G of \mathbb{Q}_k by

$$\mathbb{Q}_k^G := \langle f_K - f_{gK} \mid K \in \binom{V}{k}, g \in G \rangle.$$

The factor space $\mathbb{Q}_k / \mathbb{Q}_k^G$ is generated by the set $\{f_K + \mathbb{Q}_k^G \mid K \in \binom{V}{k}\}$, where some generating elements are equal, i.e. for all $K, K' \in \binom{V}{k}$ holds:

$$f_K + \mathbb{Q}_k^G = f_{K'} + \mathbb{Q}_k^G \iff K' \in G(K)$$

This equivalence follows immediately from the definition of \mathbb{Q}_k^G . Hence $\mathbb{Q}_k / \mathbb{Q}_k^G$ is generated by $\{f_K + \mathbb{Q}_k^G \mid K \in R\}$ where R is a transversal of the orbits of G on the set of k -subspaces. The dimension of $\mathbb{Q}_k / \mathbb{Q}_k^G$ is then $|R| = |G \setminus \binom{V}{k}|$, the number of orbits:

$$\dim(\mathbb{Q}_k / \mathbb{Q}_k^G) = |G \setminus \binom{V}{k}|$$

Now we consider the correspondance between \mathbb{Q}_t and \mathbb{Q}_k for $t \leq k$. We define a linear mapping $\zeta : \mathbb{Q}_k \rightarrow \mathbb{Q}_t$ by the images of all basis vector $f_K, K \in \binom{V}{k}$ of \mathbb{Q}_k , representend by the basis vectors $f_T, T \in \binom{V}{t}$ of \mathbb{Q}_t :

$$\zeta : \mathbb{Q}_k \rightarrow \mathbb{Q}_t, f_K \mapsto \sum_{T: T \subseteq K} f_T$$

The matrix representation of ζ is exactly the incidence matrix $A_{t,k}$. As this matrix has full row rank for all $0 < t < k < v - t$ the corresponding mapping ζ is surjective and also satisfies $\zeta(\mathbb{Q}_k^G) \subseteq \mathbb{Q}_t^G$. We obtain as immediate consequence, that $\zeta : \mathbb{Q}_k \rightarrow \mathbb{Q}_t$ induces a mapping on the corresponding factor spaces,

$$\zeta' : \mathbb{Q}_k / \mathbb{Q}_k^G \rightarrow \mathbb{Q}_t / \mathbb{Q}_t^G, f + \mathbb{Q}_k^G \mapsto \zeta(f) + \mathbb{Q}_t^G,$$

which is surjective and yields $\dim(\mathbb{Q}_t / \mathbb{Q}_t^G) < \dim(\mathbb{Q}_k / \mathbb{Q}_k^G)$. This proves, that $|G \setminus \binom{V}{t}| < |G \setminus \binom{V}{k}|$.

4. PROOF OF THE MAIN THEOREM

In this section we prove our main Theorem 1. We adopted the idea from the proof of the existence of non-simple designs over sets to designs over finite fields, but also considered the existence of a group of automorphisms, which means, that we have to use the G -incidence matrix $A_{t,k}^G$ instead of the ordinary incidence matrix $A_{t,k}$.

Proof of Theorem 1. To construct a non-simple $t - (v, k, \lambda; q)$ design with G as a group of automorphisms we use the Kramer-Mesner-theorem and construct a vector x with integral non-negative entries such that $A_{t,k}^G \cdot x = (\lambda, \dots, \lambda)^t$.

Since $0 < t < k < v - t$ we get from the previous section, that the number of orbits satisfy $|G \setminus \binom{V}{t}| < |G \setminus \binom{V}{k}|$, which means that the incidence matrix $A_{t,k}^G$ has more columns than rows. Hence the columns a_{*K}^G of $A_{t,k}^G$ are linearly dependent over the field \mathbb{Q} , i.e. there is a non-zero vector $z = (\dots, z_K, \dots)^t$ with entries in \mathbb{Q} , such that

$$A_{t,k}^G \cdot z = \sum_K a_{*K}^G z_K = (0, \dots, 0)^t.$$

Let α be the least common multiple of the non-zero denominators of all entries z_K of the vector z . If we set $y := \alpha z = (\dots, \alpha z_K, \dots)$ we also get

$$A_{t,k}^G \cdot y = \sum_K a_{*K}^G y_K = (0, \dots, 0)^t$$

but the vector $y = (\dots, y_K, \dots)$ has integral values $y_K \in \mathbb{Z}$. If β is the minimum of all values of y (it is obviously $\beta < 0$), the non-negative integral vector

$$x = (\dots, x_K, \dots)^t \quad \text{with} \quad x_K := y_K - \beta$$

satisfies

$$\begin{aligned} A_{t,k}^G \cdot x &= \sum_K a_{*K}^G x_K \\ &= \sum_K a_{*K}^G (y_K - \beta) \\ &= \sum_K a_{*K}^G y_K - \beta \sum_K a_{*K}^G \\ &= (0, \dots, 0)^t - \beta \left(\binom{v-t}{v-k}_q, \dots, \binom{v-t}{v-k}_q \right)^t \\ &= \left(-\beta \binom{v-t}{v-k}_q, \dots, -\beta \binom{v-t}{v-k}_q \right)^t. \end{aligned}$$

Finally, we have proven that the integral vector $x = (\dots, x_K, \dots)^t$ defines a non-simple $t - (v, k, \lambda; q)$ design having G as a group of automorphisms with value $\lambda = -\beta \binom{v-t}{v-k}_q$. \square

REFERENCES

- [1] Braun, M. 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*. Bayreuther Mathematische Schriften 74:58–68, 2005.
- [2] Braun, M., Kerber, A. and Laue, R. Systematic Construction of q -Analogues of Designs. *Designs, Codes and Cryptography*, 34(1):55–70, 2005.
- [3] Etzion, T. and Vardy, A. On q -Analogues 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.

- [4] Itoh, T. A New Family of 2-Designs over $GF(q)$ Admitting $SL_m(q^l)$. *Geometriae Dedicata*, 69:261–286, 1998.
- [5] Kramer, E. and Mesner, D. t -Designs on Hypergraphs. *Discrete Mathematics*, 15(3):263–296, 1976.
- [6] Miyakawa, M., Munemasa, A. and Yoshiara, S. On a Class of Small 2-Designs over $GF(q)$. *Journal of Combinatorial Designs*, 3:61–77, 1995.
- [7] Mnukhin, V.B. and Siemons I.J. On the Livingstone-Wagner Theorem. *The Electronic Journal of Combinatorics*, 11(R29):1–8, 2004.
- [8] Ray-Chaudhuri, D.K. and Schram, E.J. Designs on Vectorspaces Constructed Using Quadratic Forms. *Geometriae Dedicata*, 42:1–42, 1992.
- [9] Schwartz, M. and Etzion, T. Codes and Anticodes in the Grassman Graph. *Journal of Combinatorial Theory, Series A*, 97:27–42, 2002.
- [10] Stanley, R.P. Some Aspects of Groups Acting on Finite Posets. *Journal of Combinatorial Theory, Series A*, 32:132–161, 1982.
- [11] Suzuki, H. 2-Designs over $GF(2^m)$. *Graphs and Combinatorics*, 6:293–296, 1990.
- [12] Suzuki, H. 2-Designs over $GF(q)$. *Graphs and Combinatorics*, 8:381–389, 1992.
- [13] Thomas, S. Designs over Finite Fields. *Geometriae Dedicata*, 24:237–242, 1987.
- [14] Thomas, S. Designs and Partial Geometries over Finite Fields. *Geometriae Dedicata*, 63:247–253, 1996.

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