Discrete Mathematics 338 (2015) 555–565

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Non-existence of a simple 3-(16, 7, 5) design with an automorphism of order 3

Anamari Nakić

University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Applied Mathematics, Unska 3, HR-10000 Zagreb, Croatia

ARTICLE INFO

Article history:
Received 27 September 2014
Received in revised form 17 November 2014
Accepted 26 November 2014
Available online 19 December 2014

Keywords:
t-design
Automorphism group
Tactical decomposition

ABSTRACT

Using recent results concerning tactical decompositions of t-designs with $t > 2$, we make a step forward on the long-standing question about the existence of a simple 3-(16, 7, 5) design; if such a design exists, then its full automorphism group has order a power of 2, possibly equal to 1.

1. Introduction

The smallest v for which the existence of a 3-design of order v is undecided is 16; indeed a 3-(16, 7, 5) design is still unknown [7]. Thus to solve this intriguing existence problem has turned out to be a challenge.

So far, the published results on this problem bring negative answers if some additional properties on the automorphism group of the desired design are assumed. In this article we also answer in the negative if we wanted to prescribe an automorphism of order three.

In [3] Z. Eslami showed that a simple 3-(16, 7, 5) design with an automorphism of prime order $p \geq 5$ does not exist. This result was obtained by determining, up to isomorphism, all 2-(15, 6, 5) designs possessing an automorphism of prime order $p \geq 5$ and then showing that none of these 1454 designs can be the derived design of a 3-(16, 7, 5) design.

At this moment, to classify all 2-(15, 6, 5) designs with an automorphism of order 3 seems to be unfeasible. Thus, for extending Eslami result to $p \geq 3$ we had to follow a new strategy. Indeed our proof is based on *tactical decompositions* [2]. They have been crucial for the construction of many 2-designs [5,8], but we are not aware of existence (or non-existence) results about t-designs with $t > 2$ obtained via them. The present article allowed the author to show the effectiveness of the equations for coefficients of tactical decomposition matrices obtained in [8,9]. Indeed they have been the key tool for the main result. Note that we are now able to state the following theorem.

Theorem 1.1. *If a simple* 3-(16, 7, 5) *design exists, then the order of its full automorphism group is a power of* 2.

We point out that our technique might also be used for proving that a putative 3-(16, 7, 5) design $\mathcal{D}$ is necessarily rigid. For this, it would be enough to show that the system of equations arising from the tactical decomposition associated with an automorphism of $\mathcal{D}$ of order 2 leads to an absurd. On the other hand we expect that the computations are extremely demanding in view of the larger sizes of the corresponding tactical decomposition matrix $\mathcal{K}$. We also point out that similar

E-mail address: anamari.nakic@fer.hr.

http://dx.doi.org/10.1016/j.disc.2014.11.016

arguments could be applied to get informations on the full automorphism group of other t-designs with $t > 2$. The most natural thing would be to consider a 3-(17, 7, 7) design whose existence is also in doubt (see Remark 4.45 in [7]). Here the reason for which we also expect too demanding computations is that the number of blocks, that is 136, is rather larger than the number of blocks of a 3-(16, 7, 5) design.

2. Preliminary results

Let t, v, k, λ_t be positive integers with $v > k \geq t$. A t-(v, k, λ_t) *design* is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ is a set of v elements called *points*, and $\mathcal{B}$ is a multiset of k-subsets of $\mathcal{P}$ called *blocks* such that every set of t distinct points is contained in precisely λ_t blocks. A design is said to be *simple* if there are no repeated blocks. One says that a point $P \in \mathcal{P}$ is *incident* with a block $B \in \mathcal{B}$ if $P \in B$. The set of all blocks of $\mathcal{D}$ containing a given set $\mathcal{S}$ of points will be denoted by $\mathcal{I}_{\mathcal{S}}$. If $\mathcal{S} = \{P\}$ is a singleton, we will simply write $\mathcal{I}_P$ rather than $\mathcal{I}_{\{P\}}$.

It is known that every t-(v, k, λ_t) design is also an s-(v, k, λ_s) design, $0 \leq s < t$, where $\lambda_s = \lambda_t \binom{v-s}{t-s} / \binom{k-s}{t-s}$. Applying this for $s = 1$ and $s = 0$ one finds, in particular, that $|\mathcal{I}_P| = \lambda_1$ for every point P, and that $|\mathcal{B}| = \lambda_0$.

In view of the above paragraph λ_s must be an integer for $0 \leq s < t$; these are the trivial necessary conditions for the existence of a t-(v, k, λ_t) design. Note, in particular, that the parameters 3-(16, 7, 5) satisfy these conditions:

$$\lambda_0 = 80, \qquad \lambda_1 = 35, \qquad \lambda_2 = 14. \tag{1}$$

An *automorphism* of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a permutation on $\mathcal{P}$ leaving $\mathcal{B}$ invariant. The set $\mathrm{Aut}\mathcal{D}$ of all automorphisms of $\mathcal{D}$ is a group under composition which is called *the full automorphism group* of $\mathcal{D}$. The group generated by an automorphism α is denoted by $\langle\alpha\rangle$. Obviously, if $\alpha \in \mathrm{Aut}\mathcal{D}$, then $\langle\alpha\rangle \leq \mathrm{Aut}\mathcal{D}$.

For an automorphism $\alpha \in \mathrm{Aut}\mathcal{D}$, we denote by $\mathrm{fix}(\alpha)$ the set of points of $\mathcal{D}$ fixed by α and, similarly, by $\mathrm{Fix}(\alpha)$ the set of blocks of $\mathcal{D}$ fixed by α. Throughout this article, we shall refer to the orbits of $\mathcal{P}$ or $\mathcal{B}$ under G as the point orbits or block orbits of $\mathcal{D}$ under G, respectively.

A *decomposition* of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a pair of partitions

$$\mathcal{P} = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_m$$
$$\mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n$$

of the point set and the block set, respectively. The decomposition is said to be *tactical* if there exist nonnegative integers ρ_{ij} and κ_{ij}, $i = 1, \ldots, m$, $j = 1, \ldots, n$, such that each point of $\mathcal{P}_i$ lies in precisely ρ_{ij} blocks of $\mathcal{B}_j$, and each block of $\mathcal{B}_j$ contains precisely κ_{ij} points from $\mathcal{P}_i$. The matrices $\mathcal{R} = [\rho_{ij}]$ and $\mathcal{K} = [\kappa_{ij}]$ are the corresponding *tactical decomposition matrices*.

There are two trivial examples of tactical decompositions; one is obtained by putting $n = m = 1$, and the other one by partitioning both $\mathcal{P}$ and $\mathcal{B}$ into singletons.

A non-trivial tactical decomposition of $\mathcal{D}$ can be obtained by considering the action of an automorphism group of $\mathcal{D}$ on $\mathcal{D}$. For further reading on the subject of t-designs and automorphism groups we refer the reader to [1,2,4,6]. Here we give well-known properties that shall be used extensively in our arguments.

Theorem 2.1. *Let G be an automorphism group of a design $\mathcal{D}$. Then the point orbits of $\mathcal{D}$ under G and the block orbits of $\mathcal{D}$ under G form a tactical decomposition of $\mathcal{D}$.*

Lemma 2.2. *Let $G = \langle\alpha\rangle$ be a cyclic automorphism group of a design $\mathcal{D}$, and let*

$$\mathcal{P} = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_m, \qquad \mathcal{B} = \mathcal{B}_1 \sqcup \cdots\ \mathcal{B}_n,$$

be the associated tactical decomposition of the orbits of $\mathcal{D}$ under G. Then the following holds.

(a) *For each point orbit $\mathcal{P}_i$, the set $\mathcal{I}_{\mathcal{P}_i}$ is a disjoint union of block orbits of $\mathcal{D}$ under G.*
(b) *Every block $B \in \mathrm{Fix}(\alpha)$ is a disjoint union of point orbits of $\mathcal{D}$ under G.*

The entries ρ_{ij} and κ_{ij} of the tactical decomposition matrices are related by the formula

$$|\mathcal{P}_i| \cdot \rho_{ij} = |\mathcal{B}_j| \cdot \kappa_{ij} \tag{2}$$

which can be easily obtained by means of a double counting of the size of $\mathcal{P}_i \times \mathcal{B}_j$. These entries also satisfy the system of equations given in the following theorem. We recall the reader that a Stirling number of the second kind is the number of ways to partition a set of n elements into k non-empty subsets.

Theorem 2.3 (*[9]*). *Let $(\mathcal{P}, \mathcal{B})$ be a t-(v, k, λ_t) design with a tactical decomposition*

$$\mathcal{P} = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_m, \qquad \mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n.$$

Let $\mathcal{P}_{i_1}, \ldots, \mathcal{P}_{i_s}$ be mutually distinct with $1 \leq s \leq t$ and let $m_1, \ldots, m_s$ be positive integers such that $m_1 + \cdots + m_s \leq t$. Then the entries of the associated tactical decomposition matrices $\mathcal{R} = [\rho_{ij}]$ and $\mathcal{K} = [\kappa_{ij}]$ satisfy the following equation in which $\left\{ {u \atop v} \right\}$ denotes a Stirling number of the second kind and $(u)_v := u(u-1)\cdots(u-v+1)$ denotes a falling factorial,

$$\sum_{j=1}^{n} \rho_{i_1 j} \kappa_{i_1 j}^{m_1 - 1} \kappa_{i_2 j}^{m_2} \cdots \kappa_{i_s j}^{m_s} = \sum_{\omega \in \Omega} \lambda_{\omega_1 + \omega_2 + \cdots + \omega_s} \left\{ {m_1 \atop \omega_1} \right\} (|\mathcal{P}_{i_1}| - 1)_{\omega_1 - 1} \prod_{j=2}^{s} \left\{ {m_j \atop \omega_j} \right\} (|\mathcal{P}_{i_j}|)_{\omega_j}, \tag{3}$$