THE KRAMER-MESNER METHOD WITH TACTICAL DECOMPOSITIONS: SOME NEW UNITALS ON 65 POINTS

VEDRAN KRČADINAC, ANAMARI NAKIĆ, AND MARIO OSVIN PAVČEVIĆ

Abstract. We propose a combination of two known computational methods for the construction of designs with prescribed groups of automorphisms: the Kramer-Mesner method and the method of tactical decompositions. This combined method is used to construct new unitals with parameters 2-$(65, 5, 1)$.

1. Introduction

A t-(v, k, λ) design is a finite incidence structure consisting of v points and a number of blocks, such that every block contains k points and every t-subset of points is contained in λ blocks. The number of blocks and other parameters such as the number of blocks containing a given point can be computed from t, v, k, and λ. Parameters satisfying all known necessary conditions for the existence of designs are called *admissible*.

The question to decide whether designs with admissible parameters actually exist can be very difficult. Some prominent open problems include the existence of projective planes of non-prime power order, the question whether there are infinitely many symmetric designs for a fixed $\lambda \geq 2$, determining the existence spectrum of Steiner 2-designs with fixed $k \geq 6$, and the existence of simple t-designs with $t \geq 10$ and small v. A construction is often attempted for a single set of parameters, and some additional constraints on the design structure are assumed in order to make the search computationally feasible. A natural constraint is the assumption that a given group of automorphisms acts on the design. Two basic computational methods for the construction of designs with prescribed automorphism groups have been in widespread use: the Kramer-Mesner method and the method of tactical decompositions. The book [11] contains explanations of both of

Date: November 4, 2010.
1991 *Mathematics Subject Classification.* 05B05.
Key words and phrases. t-design; automorphism group; unital.

them, as well as some other attempts for classifying designs with given parameters and additional constraints.

Suppose we are looking for a t-(v, k, λ) design $\mathcal{D}$ with the point set $\mathcal{P}$. In Kramer and Mesner [13], a group G of permutations of $\mathcal{P}$ is assumed to be an automorphism group of the design. The induced action of G splits the t-subsets of $\mathcal{P}$ and the k-subsets of $\mathcal{P}$ into orbits. The goal is to choose a suitable subset of the k-element orbits, covering every t-element orbit exactly λ times. Then the blocks of $\mathcal{D}$ are the k-subsets belonging to the chosen orbits. The problem can be set up as a system of linear equations $A_{tk}^G \cdot x = \lambda j$. Here j is the all-one vector; the system matrix A_{tk}^G has rows and columns labeled by the t-element and k-element orbits, respectively, and its entries count incidences. The solution vector x must be a binary vector if we want simple designs, otherwise non-negative integer entries are allowed. This method was used for the construction of many t-designs with large t and small v; examples include [3], [4], [15], [16], [17], and [23].

For $t = 2$ the method of Kramer and Mesner has not yielded as many new designs. The size of the system to be solved grows rapidly with k, and many parameters of interest for 2-designs have prohibitively large k for the Kramer-Mesner method to be applied successfully. In some of these cases designs were constructed by another computational method, based on tactical decompositions.

Now the action of the group G needs to be prescribed both on the point set $\mathcal{P}$ and on the block set $\mathcal{B}$ of the design. The action induces a tactical decomposition of the design; its incidence matrix M is split into submatrices M_{ij} corresponding to the point and block orbits. These submatrices have constant row and column sums, leading to a "condensed form" of M. In the case of a 2-design, it is known that the entries of the condensed incidence matrix satisfy a system of linear and quadratic equations, depending on the orbit lengths and on the parameters of the design. The first step of the construction is to classify all integer matrices satisfying these equations; they are usually called *orbit matrices* or *tactical decomposition matrices*. In the second step, an expansion of each of the orbit matrices to a full incidence matrix is attempted. The entries of an orbit matrix are replaced by appropriate 0-1 matrices, invariant under the action of G. This step is sometimes called *indexing*. Z. Janko used this method to solve the existence question of symmetric designs for several parameter triples, the last being $(105, 40, 15)$; for details, see [9] and [10]. Some other works employing the second method are [8], [12], [14], [25], and [26].

Our goal is to combine these two methods for the construction of designs with prescribed groups of automorphisms. A starting point for the new method is a generalization of the orbit matrix concept. We shall show that the condensed incidence matrix of a t-design satisfies a system of equations of order up to t. For the combined method, a permutation representation of G on the point set $\mathcal{P}$ must be prescribed, while on the block set it suffices to prescribe the orbit lengths. If all feasible orbit length distributions are considered, and a complete classification of orbit matrices is performed, no generality is lost over the standard Kramer-Mesner method. At the same time, significant reductions of the search space can be obtained.

Alternatively, the combined method can be thought of as a new way to perform indexing in the method of tactical decompositions. In previous works this has typically been achieved by custom-made backtracking algorithms, tailored to a specific permutation representation of G on both the point set $\mathcal{P}$ and the block set $\mathcal{B}$. Now we have a way to translate the problem to a system of linear equations over the integers, which can be solved by more general algorithms. Furthermore, this system does not depend on the specific permutation representation of G on $\mathcal{B}$ (just on the permutation representation on $\mathcal{P}$, the block orbit lengths, and on the chosen orbit matrix).

Section 2 of the paper is devoted to the generalization of orbit matrices to t-designs. A description of the combined construction method is given in Section 3, together with some implementation details. In Section 4 the new method is applied to 2-$(65, 5, 1)$ designs with various groups of automorphisms. Many new examples are constructed; these designs belong to an important family, the *unitals*. Finally, Section 5 contains some concluding remarks and acknowledgements.

2. Orbit matrices for t-designs

Let $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ be the point set and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ the block set of a design with parameters t-(v, k, λ). The design can be represented by a 0-1 matrix $M = [m_{ij}]$ of type $v \times b$, called the *incidence matrix*, its entry m_{ij} indicating whether the point p_i is contained in the block B_j. Suppose there is a partition $\mathcal{P} = \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_m$ of the point set and $\mathcal{B} = \mathcal{B}_1 \sqcup \cdots \sqcup \mathcal{B}_n$ of the block set, such that every submatrix M_{ij} of M, obtained as the intersection of rows corresponding to $\mathcal{P}_i$ and columns corresponding to $\mathcal{B}_j$, has a constant number of ones in each row and in each column (these two numbers may differ, of course). A decomposition with this property is called *tactical*.

There are two trivial tactical decompositions of a t-(v, k, λ) design. The first is when we take $m = n = 1$ and $M = M_{1,1}$, since the number r of blocks containing a point is constant, as well as the number k of points contained in a block. The second is if we take $m = v$, $n = b$. Often, there exist other, non-trivial tactical decompositions. For example, if an automorphism group G acts on the design, then its point orbits and block orbits form a tactical decomposition.

Denote by ρ_{ij} the number of ones appearing in each row of the submatrix M_{ij}, and by κ_{ij} the number of ones in each of its columns. If we denote $\langle p\rangle = \{B \in \mathcal{B} \mid p \in B\}$, for any $p \in \mathcal{P}$, then we can formulate the coefficients of the condensed incidence matrix as

$$\begin{aligned} \rho_{ij} &= |\langle p\rangle \cap \mathcal{B}_j|, \;\; p \in \mathcal{P}_i, \\ \kappa_{ij} &= |B \cap \mathcal{P}_i|, \;\; B \in \mathcal{B}_j. \end{aligned}$$

These numbers do not depend on the choice of $p \in \mathcal{P}_i$ and $B \in \mathcal{B}_j$ if and only if the decomposition is tactical. Counting the total number of ones in the submatrix M_{ij}, we get the following equation:

$$|\mathcal{P}_i| \cdot \rho_{ij} = |\mathcal{B}_j| \cdot \kappa_{ij}\,. \tag{1}$$

One can think of this equation as a double counting of the set of incident pairs

$$\{(p,B) \in \mathcal{P}_i \times \mathcal{B}_j \mid p \in B\}.$$

Now, fix a point $p \in \mathcal{P}_l$ and look at the following set:

$$\{(q,B) \in \mathcal{P}_i \times \mathcal{B} \mid p,q \in B\}.$$

A double counting of its elements yields

$$\sum_{j=1}^{n} \rho_{lj}\kappa_{ij} = \sum_{q\in\mathcal{P}_i} |\langle p\rangle \cap \langle q\rangle|. \tag{2}$$

In the case of a 2-design with parameters (v,b,r,k,λ), the right-hand side of this equation can be computed easily:

$$\sum_{q\in\mathcal{P}_i} |\langle p\rangle \cap \langle q\rangle| = \left\{ \begin{array}{cl} \lambda \cdot |\mathcal{P}_i|, & \text{for } i \neq l, \\ r + \lambda\cdot(|\mathcal{P}_i| - 1), & \text{for } i = l. \end{array} \right.$$

Applying (1), we can rewrite this equation as

$$\sum_{j=1}^{n} \frac{|\mathcal{P}_i|}{|\mathcal{B}_j|}\rho_{ij}\rho_{lj} = \lambda \cdot |\mathcal{P}_i| + \delta_{il}(r-\lambda). \tag{3}$$

Together with the obvious equations

$$\begin{aligned} \sum_{i=1}^{m} \frac{|\mathcal{P}_i|}{|\mathcal{B}_j|}\rho_{ij} &= k, \;\; j = 1,\ldots,n, \\ \sum_{j=1}^{n} \rho_{ij} &= r, \;\; i = 1,\ldots,m, \end{aligned} \tag{4}$$

we get the set of known necessary conditions for the coefficients of the condensed incidence matrix $[\rho_{ij}]$ of a 2-design. Any matrix with integer entries $0 \leq \rho_{ij} \leq |\mathcal{B}_j|$ satisfying these equations is called a *tactical decomposition matrix*, or an *orbit matrix* if the tactical decomposition is induced by the action of an automorphism group. Of course, a similar system of equations can be derived for the matrix $[\kappa_{ij}]$.

In the case of a t-(v, k, λ) design, one gets a system of equations similar to (3) by choosing a point $p \in P_l$, a number $s < t$, and double-counting the set

$$\{(q_1, \ldots, q_s, B) \in \mathcal{P}_{i_1} \times \cdots \times \mathcal{P}_{i_s} \times \mathcal{B} \mid p, q_1, \ldots, q_s \in B\}.$$

The formula analogous to (2) is now

$$\sum_{j=1}^{n} \rho_{lj}\kappa_{i_1 j} \cdots \kappa_{i_s j} = \sum_{q_1 \in \mathcal{P}_{i_1}} \cdots \sum_{q_s \in \mathcal{P}_{i_s}} |\langle p\rangle \cap \langle q_1\rangle \cap \cdots \cap \langle q_s\rangle|. \tag{5}$$

Since a t-design is also an $(s+1)$-design, for all $s < t$, it is clear that the right-hand side can be expressed via parameters of the design under observation. For example, a 3-(v, k, λ) design is also a 2-(v, k, λ_2) design with $\lambda_2 = \frac{v-2}{k-2}\,\lambda$. For $s = 1$ we get the equation (3) with λ substituted by λ_2, whereas for $s = 2$ we get the following equation:

$$\sum_{j=1}^{n} \frac{|\mathcal{P}_{i_1}| \cdot |\mathcal{P}_{i_2}|}{|\mathcal{B}_j|^2}\,\rho_{lj}\rho_{i_1 j}\rho_{i_2 j} = \tag{6}$$

$$= \begin{cases} |\mathcal{P}_{i_1}| \cdot |\mathcal{P}_{i_2}| \cdot \lambda, & \text{for } l \neq i_1 \neq i_2 \neq l, \\ |\mathcal{P}_{i_2}| \cdot \lambda_2 + (|\mathcal{P}_{i_1}| - 1) \cdot |\mathcal{P}_{i_2}| \cdot \lambda, & \text{for } l = i_1 \neq i_2 \text{ or } l \neq i_1 = i_2, \\ r + 3\,(|\mathcal{P}_l| - 1) \cdot \lambda_2 + (|\mathcal{P}_l| - 1) \cdot (|\mathcal{P}_l| - 2) \cdot \lambda, & \text{for } l = i_1 = i_2. \end{cases}$$

For general t, the formulae for the right-hand side of (5) involve parameters λ_s when the design is considered as an s-design for $s \leq t$, the orbit lengths $|\mathcal{P}_i|$ and Stirling numbers of the second kind. It is not difficult to write down these formulae for given specific parameters, although we have not found an elegant way to do this for an arbitrary t.

To clarify the concept of orbit matrices for t-designs further, we consider a small example. Suppose a 3-$(10, 4, 1)$ designs admits an automorphism of order 3 with one fixed point and three fixed blocks. Such an action occurs on the design obtained by twice deriving the small Witt design with parameters 5-$(12, 6, 1)$. The induced tactical decomposition has point orbit lengths $|\mathcal{P}_1| = 1$, $|\mathcal{P}_2| = |\mathcal{P}_3| = |\mathcal{P}_4| = 3$, and block orbit lengths $|\mathcal{B}_1| = |\mathcal{B}_2| = |\mathcal{B}_3| = 1$, $|\mathcal{B}_4| = \cdots = |\mathcal{B}_{12}| = 3$. Since each of the fixed blocks contains the fixed point and one of the orbits $\mathcal{P}_2$, $\mathcal{P}_3$, $\mathcal{P}_4$, and the fixed point is contained in three of the orbits

$\mathcal{B}_4, \ldots, \mathcal{B}_{12}$, the following part of the matrix $[\rho_{ij}]$ can be written down without loss of generality:

$$\begin{bmatrix} 1 & 1 & 1 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & & & & & & & & & \\ 0 & 1 & 0 & & & & & & & & & \\ 0 & 0 & 1 & & & & & & & & & \end{bmatrix}.$$

This information could also be deduced directly from the equations (4). For the unknown part of the matrix, equations (4) yield

$$\sum_{i=2}^{4} \rho_{ij} = \begin{cases} 3, & \text{for } j = 4, 5, 6, \\ 4, & \text{for } j = 7, \ldots, 12, \end{cases}$$

$$\sum_{j=4}^{12} \rho_{ij} = 11, \quad \text{for } i = 2, 3, 4,$$

and equations (3) yield

$$\sum_{j=4}^{6} \rho_{ij} = 3, \quad \text{for } i = 2, 3, 4,$$

$$\sum_{j=4}^{12} \rho_{ij}\rho_{lj} = 12, \quad \text{for } i, l \in \{2, 3, 4\},\ i \neq l,$$

$$\sum_{j=4}^{12} \rho_{ij}^2 = 17, \quad \text{for } i = 2, 3, 4.$$

Up to rearrangements of rows and columns, there are exactly 8 matrices satisfying all constraints considered so far. We found them using an orderly classification algorithm described in [14]. These orbit matrices correspond to 2-$(10, 4, 4)$ designs, but since we are looking for 3-$(10, 4, 1)$ designs, equations (6) give further constraints:

$$\sum_{j=4}^{6} \rho_{i_1 j}\rho_{i_2 j} = 3, \quad \text{for } i_1, i_2 \in \{2, 3, 4\},\ i_1 \neq i_2,$$

$$\sum_{j=4}^{12} \rho_{2j}\rho_{3j}\rho_{4j} = 9,$$

$$\sum_{j=4}^{6} \rho_{ij}^2 = 3, \quad \text{for } i = 2, 3, 4,$$

$$\sum_{j=4}^{12} \rho_{i_1 j}^2 \rho_{i_2 j} = 18, \quad \text{for } i_1, i_2 \in \{2,3,4\},\ i_1 \neq i_2,$$

$$\sum_{j=4}^{12} \rho_{lj}^3 = 29, \quad \text{for } l = 2,3,4.$$

Only one of the 8 orbit matrices for 2-$(10,4,4)$ designs satisfies these new constraints:

$$\begin{bmatrix} 1 & 1 & 1 & 3 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 2 & 2 \end{bmatrix}. \tag{7}$$

Thus, this is the only orbit matrix for 3-$(10,4,1)$ designs with the chosen automorphism group, up to rearrangements of rows and columns.

3. The combined method

Suppose a given permutation group G acts on the point set $\mathcal{P}$ of our sought after t-(v,k,λ) design as an automorphism group. As before, G splits $\mathcal{P}$ into orbits $\mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_m$. The induced action of G also splits the set $\mathcal{P}^t = \binom{\mathcal{P}}{t}$ of all t-subsets of $\mathcal{P}$ into orbits $\mathcal{P}_1^t \sqcup \cdots \sqcup \mathcal{P}_M^t$, as well as the set of all k-subsets $\mathcal{P}^k = \binom{\mathcal{P}}{k} = \mathcal{P}_1^k \sqcup \cdots \sqcup \mathcal{P}_N^k$. Again, the decomposition is tactical, i.e. the number $a_{ij} = |\{K \in \mathcal{P}_j^k \mid T \subseteq K\}|$ does not depend on the choice of $T \in \mathcal{P}_i^t$, for each $i = 1, \ldots, M$ and $j = 1, \ldots, N$. The matrix $[a_{ij}]$ is denoted by A_{tk}^G.

As explained in the introduction, searching for simple designs by the Kramer-Mesner method amounts to finding 0-1 solutions of the system of linear equations $A_{tk}^G \cdot x = \lambda j$. Solving linear systems over the integers is a well-known NP-complete problem, which quickly becomes intractable as the number of variables N grows. One way to reduce the search space for the Kramer-Mesner system is to prescribe the block orbit lengths $|\mathcal{B}_1|, \ldots, |\mathcal{B}_n|$. Then we can ignore the columns of A_{tk}^G corresponding to orbits $\mathcal{P}_j^k$ that are not of an appropriate size, i.e. such that $|\mathcal{P}_j^k|$ is not equal to any of the $|\mathcal{B}_{j'}|$. Furthermore, we can add an extra equation for each distinct orbit size s appearing e times in the multiset $\{|\mathcal{B}_1|, \cdots, |\mathcal{B}_n|\}$, specifying that e orbits with $|\mathcal{P}_j^k| = s$ have to be chosen.

An even greater reduction of the search space can be achieved if an orbit matrix is given. Note that the numbers ρ_{ij} coincide with entries of the matrix A_{1k}^G, except that the columns of $[\rho_{ij}]$ are labeled by orbits of the k-subsets being blocks of the design, while the columns of A_{1k}^G

are labeled by orbits of all k-subsets of $\mathcal{P}$. As before, we can ignore the orbits $\mathcal{P}_j^k$ for which the columns in A_{1k}^G do not match a column of the orbit matrix $[\rho_{ij}]$, and delete all the corresponding columns in the system matrix A_{tk}^G. Furthermore, each distinct column of the orbit matrix, appearing e' times in the matrix, yields an extra equation for the system, specifying that exactly e' of the orbits $\mathcal{P}_j^k$ with the corresponding column in A_{1k}^G have to be chosen.

In this way the number N of variables of the system $A_{tk}^G \cdot x = \lambda j$ is reduced, and the number M of equations is increased, making the system easier to solve. Of course, in order not to lose generality over the standard Kramer-Mesner method, all feasible block orbit length distributions have to be considered, and a complete classification of orbit matrices has to be performed in each case. We shall give examples illustrating that this can be well worth the effort, in the sense that the overall computation time is significantly reduced. In this section we go back to 3-$(10,4,1)$ designs with an automorphism of order 3, and in the next section we consider 2-$(65,5,1)$ designs with various groups of automorphisms.

In the previous section we obtained the orbit matrix (7) for a 3-$(10,4,1)$ design with an automorphism of order 3 fixing one point and three blocks. Suppose that $\mathcal{P} = \{1,\ldots,10\}$ and the automorphism group is $G = \langle(1)(2,3,4)(5,6,7)(8,9,10)\rangle$. The only 3-subsets of $\mathcal{P}$ fixed by G are $\{2,3,4\}$, $\{5,6,7\}$, $\{8,9,10\}$, and the only fixed 4-subsets are $\{1,2,3,4\}$, $\{1,5,6,7\}$, $\{1,8,9,10\}$. All the remaining G-orbits on $\mathcal{P}^3$ and $\mathcal{P}^4$ are of length 3. Thus, G acts on $\mathcal{P}^3$ in $M = 3 + \left(\binom{10}{3} - 3\right)/3 = 42$ orbits, and on $\mathcal{P}^4$ in $N = 3 + \left(\binom{10}{4} - 3\right)/3 = 72$ orbits. Using the software system GAP [6], one can compute the 42×72 matrix A_{34}^G. The Kramer-Mesner system $A_{34}^G \cdot x = j$ has nine 0-1 solutions, representing isomorphic designs.

All nine solutions contain the three fixed 4-subsets; therefore, the assumption that the automorphism fixes three blocks does not lead to a loss of generality over the standard Kramer-Mesner approach. However, we can reduce the search space a little bit if we assume this in advance, by adding two more equations to the system: $x_1+x_2+x_3 = 3$ and $x_4 + \ldots + x_{72} = 9$. Here, the first three orbits $\mathcal{P}_1^4$, $\mathcal{P}_2^4$, $\mathcal{P}_3^4$ are assumed to be fixed; this still leaves $\binom{69}{9}$ choices for the non-fixed orbits $\mathcal{P}_4^4,\ldots,\mathcal{P}_{72}^4$.

Knowing the orbit matrix (7) leads to a significant reduction of the search space. Only 45 of the 69 non-fixed orbits give rise to columns of A_{14}^G compatible with a column of the orbit matrix. The column

$(3,1,1,1)$ and each of the columns $(0,1,1,2)$, $(0,1,2,1)$, $(0,2,1,1)$ occur 9 times in A_{14}^G, while the columns $(0,2,2,0)$, $(0,2,0,2)$, $(0,0,2,2)$ occur 3 times. This can be encoded by 7 extra linear equations. Thus, instead of the original 42×72 Kramer-Mesner system, we get a 49×45 system of linear equations. The 7 extra equations effectively reduce the search space from $\binom{69}{9}$ possibilities to $\binom{9}{3} \cdot 9^3 \cdot 3^3$ possibilities. The new system also has 9 solutions, representing the same 3-$(10,4,1)$ designs.

We shall now consider some of the implementation issues for the combined construction method. The computation can be divided into four steps: finding all orbit matrices, building orbits and systems of linear equations from each orbit matrix, solving the systems, and testing the constructed designs for isomorphism. As already mentioned, for the first step we use an orderly classification algorithm from [14]. The algorithm was adapted to t-designs by including equations (6) and some of the equations for $t = 4$ and $t = 5$. For example, we can generate the orbit matrix (7) for 3-$(10,4,1)$ designs directly, instead of generating all orbit matrices for 2-$(10,4,4)$ designs and checking if they satisfy the additional equations for $t = 3$, as described in Section 2.

In the second step of the computation we use GAP [6]. We have implemented a series of routines for building the k-element orbits compatible with a given orbit matrix and setting up the Kramer-Mesner system. For bigger problems the total number of k-element orbits $\mathcal{P}_1^k, \ldots, \mathcal{P}_N^k$ can be very large. We do not have to generate all of them, and then check their compatibility with the orbit matrix. Instead, we can build just those k-element orbits $\mathcal{P}_j^k$ compatible with a column of the orbit matrix. For that, the matrix $[\kappa_{ij}]$ is better suited than $[\rho_{ij}]$, because a column of the first matrix describes the intersection pattern of a block from $\mathcal{B}_j$ with the point orbits $\mathcal{P}_1, \ldots, \mathcal{P}_m$. The two matrices are related by (1) and we can switch between them at will.

The third step is to find all 0-1 solutions of the systems of linear equations obtained in this way. Any 0-1 solver can be used for this task, such as the one by A. Wassermann based on lattice basis reduction [27]. However, general-purpose solvers may not exploit the reduction of search space imposed by the extra equations. Therefore, we have built a simple backtracking program in C, suited to the particular form of our systems. In many cases this has proved more efficient than using the solver [27].

As the final step, once the designs have been constructed, we perform isomorphism testing and compute their full automorphism groups. For this we use `nauty` by B.D. McKay [20].

4. Some new unitals $(65, 5, 1)$

Unitals are designs with parameters 2-$(q^3 + 1, q + 1, 1)$. Given a projective plane of order q^2 with a unitary polarity, the set of absolute points and non-absolute lines forms a unital. Since the desarguesian projective planes of square order admit unitary polarities, unitals exist for each prime-power q (these are the *classical* or *hermitian* unitals). Unitals also exist for $q = 6$, see [1] and [18].

The smallest non-trivial unitals are 2-$(28, 4, 1)$ designs. Brouwer [5] found 11 examples embedded in the projective planes of order 9 and more than 100 non-embeddable examples, thus answering several questions posed by Piper [22]. Brouwer's search was not complete; later Penttila and Royle [21] classified all embeddable $(28, 4, 1)$s (there are 17 up to isomorphism), and in [14] all $(28, 4, 1)$s with non-trivial automorphism groups were classified (there are 4466). Betten, Betten and Tonchev [2] also found 187 examples with a trivial full automorphism group.

The next case are unitals for $q = 4$, i.e. 2-$(65, 5, 1)$ designs. Stoichev and Tonchev [24] performed a non-exhaustive search for unitals in the known projective planes of order 16 and report to have found 38 non-isomorphic examples. We were able to increase this number by also considering the dual unitals. Furthermore, the point sets $SEMI4.1$ and $HALL.4$ listed in [24] represent unitals in both of the planes (the semi-field plane with kernel $GF(4)$ and the Hall plane). Similarly, some of the dual sets represent unitals in several planes. By dualizing the duals we found another unital in the Lorimer-Rahilly plane, reproduced here according to [24, Table 2]:

Solution	Unital
$LMRH.2$	2 5 12 13 19 20 25 31 34 37 44 45 48
	49 55 62 67 68 73 79 80 81 87 94 99 100
	105 111 114 117 124 125 134 136 138 139 144 145 151
	158 162 165 172 173 176 177 183 190 192 193 199 206
	210 213 220 221 227 228 233 239 243 244 249 255 272

In this way we found 73 non-isomorphic unitals $(65, 5, 1)$ embedded in projective planes of order 16 using Stoichev's and Tonchev's data. They appear as the first 73 examples in the list of incidence matrices available at `http://web.math.hr/~krcko/results/steiner.html`.

It is clear that there should be many more 2-$(65, 5, 1)$ designs not embedded in a projective plane of order 16. However, apparently only two examples with cyclic automorphism groups appear in published sources [19]. Their full automorphism groups are of order 780 and 260, and they are represented by incidence matrices no. 74 and 75 in the aforementioned list. As an illustration of our combined method, we shall classify the unitals $(65, 5, 1)$ with a non-abelian automorphism group of order 39, and construct further examples by assuming other automorphism groups.

Let G be the non-abelian group of order 39. In terms of generators and relations, it can be represented as

$$G = \langle \rho, \sigma \mid \rho^{13} = 1, \sigma^3 = 1, \rho^\sigma = \rho^3 \rangle .$$

In order to eliminate some of the possibilities for the action of G, we note the following

Lemma 4.1. *An automorphism of order* 13 *of a unital with parameters* $(65, 5, 1)$ *acts without any fixed points or blocks.*

This is an easy consequence of [14, Lemma 2.2]. Thus, only two lengths of G-orbits are possible, 13 and 39. The set $\mathcal{P}$ of 65 points can be partitioned into orbits in two ways:

(1) five orbits of length 13 – we shall denote this case by $[13^5]_\mathcal{P}$,
(2) two orbits of length 13 and one orbit of length 39 – we shall denote this case by $[13^2, 39]_\mathcal{P}$.

It is an easy task to find the permutation representations of G on $\mathcal{P}$ corresponding to the cases (1) and (2). In either case, it is unique up to permutation isomorphism.

We first look at the standard Kramer-Mesner setup. A computation in GAP [6] shows that in case (1), there are 60 orbits on $\mathcal{P}^2$ and 211926 orbits on $\mathcal{P}^5$, and in case (2) there are 54 orbits on $\mathcal{P}^2$ and 211806 orbits on $\mathcal{P}^5$. Some of the $\mathcal{P}^5$-orbits cover a $\mathcal{P}^2$-orbit more than once, i.e. some entries of A_{25}^G are greater than 1. Since we are looking for designs with $\lambda = 1$, these $\mathcal{P}^5$-orbits and the corresponding columns of A_{25}^G can be discarded. In this way we get a 60×26421 Kramer-Mesner system in case (1), and a 54×83637 system in case (2). These systems are too large to be solved with the software available to us. Therefore we resort to the combined method, making use of tactical decomposition matrices.

To start with, we need to assume the block orbit lengths in advance. There are 6 ways of partitioning the set $\mathcal{B}$ of 208 blocks into orbits of length 13 and 39. We shall use the same notation as for partitions of $\mathcal{P}$. For example, $[13^7, 39^3]_\mathcal{B}$ denotes a partition of $\mathcal{B}$ into 7 orbits of length 13 and 3 orbits of length 39.

In the first subcase, for orbit lengths $[13^5]_\mathcal{P}$ and $[13, 39^5]_\mathcal{B}$, we got a unique solution of the equation system (3)-(4) using our classification program for orbit matrices. Hence, there is only one orbit matrix for this partition of points and blocks:

$$\begin{bmatrix} 1 & 6 & 6 & 3 & 0 & 0 \\ 1 & 6 & 0 & 0 & 6 & 3 \\ 1 & 3 & 0 & 6 & 0 & 6 \\ 1 & 0 & 6 & 0 & 3 & 6 \\ 1 & 0 & 3 & 6 & 6 & 0 \end{bmatrix}.$$

Here and in the sequel, the rows and columns corresponding to orbits of length 13 are written before the ones corresponding to orbits of length 39. In the second subcase, for $[13^5]_{\mathcal{P}}$ and $[13^4, 39^4]_{\mathcal{B}}$, we got one orbit matrix as well:

$$\begin{bmatrix} 2 & 2 & 2 & 1 & 6 & 3 & 0 & 0 \\ 2 & 2 & 2 & 1 & 0 & 0 & 6 & 3 \\ 1 & 1 & 1 & 1 & 0 & 6 & 0 & 6 \\ 0 & 0 & 0 & 1 & 6 & 0 & 3 & 6 \\ 0 & 0 & 0 & 1 & 3 & 6 & 6 & 0 \end{bmatrix}.$$

However, this matrix has some entries equal to 2 in the rows and columns corresponding to orbits of length 13. From the permutation representation of G on 13 points, it is clear that $\rho_{ij} \equiv 0, 1 \pmod 3$ must hold for these entries. Therefore, this orbit matrix cannot give rise to designs, i.e. such an action of the group G is not possible.

Table 1 contains numbers of inequivalent orbit matrices for all the subcases. The second number counts orbit matrices with $\rho_{ij} \equiv 0, 1 \pmod 3$ for all entries corresponding to orbits of length 13; we shall call such orbit matrices *feasible*. Only feasible orbit matrices can give rise to designs with an automorphism group isomorphic to G.

	$[13^5]_{\mathcal{P}}$	$[13^2, 39]_{\mathcal{P}}$
$[13, 39^5]_{\mathcal{B}}$	1 / 1	3 / 3
$[13^4, 39^4]_{\mathcal{B}}$	1 / 0	6 / 1
$[13^7, 39^3]_{\mathcal{B}}$	5 / 3	5 / 0
$[13^{10}, 39^2]_{\mathcal{B}}$	150 / 4	0 / 0
$[13^{13}, 39]_{\mathcal{B}}$	18707 / 3	0 / 0
$[13^{16}]_{\mathcal{B}}$	141009 / 3	0 / 0

TABLE 1. Numbers of inequivalent orbit matrices.

In the second step of the computation, we use GAP [6] to set up the Kramer-Mesner systems for each feasible orbit matrix. As before, columns of the system matrix with entries greater than 1 are automatically discarded, because we are looking for designs with $\lambda = 1$. Dimensions of the Kramer-Mesner systems are given in Table 2.

Orbit lengths	KM system	No. solutions	No. designs
$[13^5]_{\mathcal{P}}$, $[13, 39^5]_{\mathcal{B}}$	66×351	10482	263
$[13^5]_{\mathcal{P}}$, $[13^7, 39^3]_{\mathcal{B}}$	70×6001	0	0
	70×3049	0	0
	68×3041	0	0
$[13^5]_{\mathcal{P}}$, $[13^{10}, 39^2]_{\mathcal{B}}$	69×2041	0	0
	71×4000	80	2
	71×4000	48	4
	71×4000	0	0
$[13^5]_{\mathcal{P}}$, $[13^{13}, 39]_{\mathcal{B}}$	72×4001	0	0
	72×4001	0	0
	72×4001	0	0
$[13^5]_{\mathcal{P}}$, $[13^{16}]_{\mathcal{B}}$	71×41	0	0
	71×41	0	0
	71×41	0	0
$[13^2, 39]_{\mathcal{P}}$, $[13^7, 39^3]_{\mathcal{B}}$	59×52342	86580	555
	60×38311	56940	184
	60×33475	86112	276
$[13^2, 39]_{\mathcal{P}}$, $[13^4, 39^4]_{\mathcal{B}}$	59×28019	0	0

Table 2. Dimensions of Kramer-Mesner systems and numbers of solutions.

Next, we compute all 0-1 solutions of these systems. For systems with fewer columns, both A. Wassermann's solver [27] and our own backtracking solver have been tried. The solutions agreed in each case. However, in the subcase $[13^2, 39]_{\mathcal{P}}$, $[13^7, 39^3]_{\mathcal{B}}$ the systems were too large for [27]. Our own solver could manage these systems due to the reduction of search space imposed by the extra equations. The total numbers of solutions are reported in the third column of Table 2.

Each solution represents a design, but many of these designs are isomorphic. As the final step, we use `nauty` [20] to determine numbers of non-isomorphic designs, and report them in the fourth column of Table 2. The total number of $(65, 5, 1)$ designs with an automorphism group isomorphic to G is obtained by adding these numbers. Theoretically, designs from different subcases could be isomorphic, but this does not happen (we used `nauty` once more to check for isomorphism). This finally proves the following theorem.

Theorem 4.2. *There are* 1284 *unitals on* 65 *points admitting an action of a non-abelian group of order* 39.

For most of these designs, namely 1277, G is the full automorphism group. The rest are the classical unital with full automorphism group of order 249600, the cyclic unital with full automorphism group of order 780, one unital with full automorphism group of order 156, and four unitals with full automorphism group of order 78. The new designs appear as incidence matrices no. 76 through 1357 in our list published on the web. The classical unital and the cyclic unital have already appeared as incidence matrices no. 1 and no. 74, respectively.

In Table 1 we see that the number of orbit matrices is very large in the case when all point orbits and block orbits are of size 13. Only three of the 141009 matrices are feasible for the group G of order 39, but all of them suit the cyclic group of order 13. Indeed, we tried to perform a complete classification of $(65, 5, 1)$ designs with an automorphism of order 13 using the standard approach, i.e. by indexing the orbit matrices directly. However, this computation is too large for the resources available to us. We could only examine a couple of orbit matrices, and in this way obtained 62 designs with full automorphism group of order 13. They appear as incidence matrices no. 1358 through 1419 in our list.

One may wish to construct more examples of $(65, 5, 1)$ designs with other automorphism groups. Then the advantage of the combined construction method quickly becomes apparent. Using the standard approach, a special program for indexing the orbit matrices is needed for each new group. On the other hand, with the new approach all that is needed is a permutation representation of the group on the point set $\mathcal{P}$. Feasible permutation groups can be obtained easily by taking subgroups of full automorphism groups of some of the known designs. We examined a non-abelian group of order 50 and got 143 more designs, and another non-abelian group of order 32 leading to 215 more designs. These designs appear in the final part of our list, as incidence matrices no. 1420 through 1777.

Thus, there are at least 1777 non-isomorphic 2-$(65, 5, 1)$ designs. We computed their full automorphism groups with `nauty`, and report the orders in Table 3.

|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#	|Aut|	#
249600	1	300	10	150	2	64	67	20	2
1200	1	260	1	128	82	50	24	16	12
780	1	256	12	100	89	48	7	13	62
768	3	200	17	96	5	39	1277	12	2
600	3	192	8	80	2	32	57	8	12
384	1	156	1	78	4	24	8	4	4

Table 3. Distribution of the 1777 designs by order of their full automorphism group.

5. Concluding remarks and acknowledgements

We have described an enhancement of the Kramer-Mesner method for constructing t-designs with prescribed groups of automorphisms. The main bottleneck of this general construction method is the size of the linear system which needs to be solved over the integers. If a classification of orbit matrices is performed beforehand, the Kramer-Mesner system can be replaced by several smaller systems, leading to a reduction of the overall computation time.

The Kramer-Messner approach was mostly used with very large permutation groups, in order to get sufficiently small systems of linear equations. The main advantage of the new method is that smaller groups can also be considered as prospective automorphism groups of the designs. For smaller groups G the number of columns of the Kramer-Mesner system grows, but the decomposition of point and blocks into G-orbits also gets finer. This leads to a stronger reduction of the k-element orbits when they are checked for compatibility with the orbit matrices. In this paper the new method was applied to 2-designs, but we hope that it will lead to new t-designs for $t > 2$ in the future. Considering the recent discovery of Steiner 5-designs with trivial full automorphism groups [7], it seems promising to examine some of the open cases with smaller groups than it was previously possible.

We wish to thank the group of researchers at the University of Bayreuth (Germany), in particular Reinhard Laue, Axel Kohnert and Alfred Wassermann, for many fruitful discussions in which the main ideas of this work came to life, and for making their software system DISCRETA available. The first and the third author participated in an exchange program between Bayreuth and Zagreb, funded by the Deutsche Forschungsgemeinschaft and the Croatian Ministry of Science and Technology.

References

[1] S. Bagchi and B. Bagchi, *Designs from pairs of finite fields. I. A cyclic unital $U(6)$ and other regular Steiner 2-designs*, J. Combin. Theory Ser. A **52**(1989), 51–61.

[2] A. Betten, D. Betten and V.D. Tonchev, *Unitals and Codes*, Disrete Math. **267** (2003), 23–33.

[3] A. Betten, R. Laue, S. Molodtsov, A. Wassermann, *Steiner systems with automorphism groups* $\mathrm{PSL}(2,71)$*,* $\mathrm{PSL}(2,83)$*, and* $\mathrm{P\Sigma L}(2,3^5)$, J. Geom. **67** (2000), 35–41.

[4] A. Betten, R. Laue, A. Wassermann, *Simple 7-designs with small parameters*, J. Combin. Des. **7** (1999), 79–94.

[5] A.E. Brouwer, *Some unitals on 28 points and their embeddings in projective planes of order 9*, Geometries and Groups, Proc. Colloq. Berlin 1981, Lecture Notes in Math. **893** (1981), 183–188.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.4.12; 2008, (`http://www.gap-system.org`).

[7] M.J. Grannell, *Some rigid Steiner 5-designs*, to appear in J. Combin. Des.

[8] D. Held and M.O. Pavčević, *Symmetric $(79,27,9)$-designs admitting a faithful action of a Frobenius group of order 39*, European J. Combin. **18** (1997), 409–416.

[9] Z. Janko, *The existence of symmetric designs with parameters* $(105,40,15)$, J. Combin. Des. **7** (1999), 17–19.

[10] Z. Janko and Tran van Trung, *Construction of a new symmetric block design for $(78,22,6)$ with the help of tactical decompositions*, J. Combin. Theory A **40** (1985), 451–455.

[11] P. Kaski, P.R.J. Östergård, *Classification algorithms for codes and designs*, Springer, Berlin, 2006.

[12] E.S. Kramer, S.S. Magliveras and R. Mathon, *The Steiner systems $S(2,4,25)$ with nontrivial automorphism group*, Discrete Math. **77** (1989), 137–157.

[13] E.S. Kramer and D.M. Mesner, *t-designs on hypergraphs*, Discrete Math. **15** (1976), 263–296.

[14] V. Krčadinac, *Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms*, Glas. Mat. Ser. III **37(57)**(2002), 259–268.

[15] D.L. Kreher and S.P. Radziszowski, *Constructing 6-$(14,7,4)$ designs*, Contemp. Math. **111**, Amer. Math. Soc. 1990, pp. 137–151.

[16] R. Laue, *Constructing objects up to isomorphism, simple 9-designs*, in *Algebraic Combinatorics and Applications* (eds. A. Betten et al.), Springer, 2001, pp. 232–260.

[17] R. Laue and A. Wassermann, *Simple* 8-$(31,12,3080)$*,* 8-$(40,12,16\,200)$ *and* 8-$(40,12,16\,520)$ *designs from* $\mathrm{PSL}(3,5)$ *and* $\mathrm{PSL}(4,3)$, Discrete Math. **308** (2008), 166–174.

[18] R. Mathon, *Constructions for cyclic Steiner 2-designs*, Ann. Discrete Math. **34** (1987), 353–362.

[19] R. Mathon and A. Rosa, 2-(v,k,λ) *designs of small order*, in: *The Handbook of Combinatorial Designs, Second Edition* (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, 2007, pp. 25–58.

[20] B.D. McKay, `nauty` User's guide (version 1.5), Technical Report TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

[21] T. Penttila and G.F. Royle, *Sets of type* (m, n) *in the affine and projective planes of order* 9, Des. Codes Cryptography **6** (1995), 229–245.
[22] F. Piper, *Unitary block designs*, in: *Graph Theory and Combinatorics* (ed. R.J. Wilson), Res. Notes in Math. **34**, 1979, pp. 98–105.
[23] B. Schmalz, *The* t*-designs with prescribed automorphism group, new simple* 6*-designs*, J. Combin. Des. **1** (1993), 125–170.
[24] S.D. Stoichev and V.D. Tonchev, *Unital designs in planes of order* 16, Discrete Appl. Math. **102** (2000), 151–158.
[25] V.D. Tonchev, *Steiner triple systems of order* 21 *with automorphisms of order* 7, Ars Combin. **23** (1987), 93–96.
[26] S. Topalova, *Symmetric* 2-$(69, 17, 4)$ *designs with automorphisms of order* 13, J. Statist. Plann. Inference **95** (2001), 335–339.
[27] A. Wassermann, *Finding simple* t*-designs with enumeration techniques*, J. Combin. Des. **6** (1998), 79–90.

University of Zagreb, Faculty of Science, Department of Mathematics, Bijenička 30, HR-10000 Zagreb, Croatia
E-mail address: vedran.krcadinac@math.hr

University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Applied Mathematics, Unska 3, HR-10000 Zagreb, Croatia
E-mail address: anamari.nakic@fer.hr

University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Applied Mathematics, Unska 3, HR-10000 Zagreb, Croatia
E-mail address: mario.pavcevic@fer.hr