Large sets of t-designs from t-homogeneous groups

R. Laue[c] G. R. Omidi[a,b] B. Tayfeh-Rezaie[a,1,2]

[a] *Institute for Studies in Theoretical Physics and Mathematics* (*IPM*), *P.O. Box* 19395-5746, *Tehran, Iran*

[b] *School of Mathematics, Statistics and Computer Science, University of Tehran, Tehran, Iran*

[c] *Mathematical Department, University of Bayreuth, D*-95440 *Bayreuth, Germany*

Abstract

A direct method for constructing large sets of t-designs is based on the concept of assembling orbits of a permutation group G on k-subsets of a v-set into block sets of t-designs so that these designs form a large set. If G is t-homogeneous, then any orbit is a t-design and therefore we obtain a large set by partitioning the set of orbits into parts consisting of the same number of k-subsets. In general, it is hard to find such partitions. We solve this problem when orbit sizes are limited to two values. We then use its corollaries to obtain some results in a special case in which a simple divisibility condition holds and no knowledge about orbit sizes is assumed.

Keywords: t-designs, large sets of t-designs, automorphism groups, homogeneous groups

MR Subject Classification: 05B05, 20B25, 05E20

[1] Corresponding author, email: tayfeh-r@ipm.ir

[2] Supported by a grant from IPM (No. 83050312).

1 Introduction

The problem of partitioning a set of subsets of a finite set into parts with some special regularity conditions has been dealt with extensively in combinatorics and graph theory. Large sets of t-(v, k, λ)-designs which are about partitioning the set of all k-subsets of a v-set into block sets of t-(v, k, λ) designs are examples of these kinds of problems. Large sets are powerful tools for the study of the existence problem of t-designs. In this direction, while there are known few extension theorems for t-designs, a considerable number of extension methods have been found for large sets, see [1, 2, 9, 10]. These methods are recursive in nature and produce infinite families from some starting large sets. For the construction of these starting objects, one usually has to use direct methods.

One direct method for constructing large sets is based on using homogeneous groups. Let G be a t-homogeneous permutation group on a v-set X. Then any orbit from the action of G on k-subsets of X is the block set of a t-(v, k, λ) design. Therefore we obtain a large set by partitioning the set of orbits into parts consisting of the same number of k-subsets. We can formulate the problem as follows. Given the multiset of the sizes of orbits of G on k-subsets of X, determine all values of N for which a large set of size N is constructible from combining the orbits. This is a bin-packing problem which is NP-hard and so in general, it is a hard problem. Nevertheless it can be tackled in some special cases. The problem was first discussed in [11] where the authors answered the case in which the orbits were of two sizes, say m and n, and m a multiple of n. We first extend this result to arbitrary m and n. We then use its corollaries to obtain some results in a special case in which a simple divisibility condition holds and no knowledge about orbit sizes is assumed.

2 Definitions

Let t, k, v and λ be integers such that $0 \leq t \leq k \leq v$ and $\lambda > 0$. Let X be a v-set and $P_k(X)$ denote the set of all k-subsets of X. A (*simple*) t-(v, k, λ) *design* is a pair $\mathcal{D} = (X, D)$ in which D is a subset of elements of $P_k(X)$ (called *blocks*) such that every t-subset of X appears in exactly λ blocks. A *large set* of t-(v, k, λ) designs of size N, denoted by $\mathrm{LS}[N](t, k, v)$, is a set of N disjoint t-(v,k,λ) designs (X, D_i) such that the D_i partition $P_k(X)$. Note that we must have $N = \binom{v-t}{k-t}/\lambda$. A set of well known necessary conditions for the existence of an $\mathrm{LS}[N](t,k,v)$ is

$$N \Big| \binom{v-i}{k-i}, \qquad 0 \le i \le t.$$

An *automorphism* of $\mathcal{D}$ is a permutation σ on X such that $\sigma(B) \in D$ for each $B \in D$. An *automorphism group* of $\mathcal{D}$ is a group whose elements are automorphisms of $\mathcal{D}$. A large set is said to be *G-uniform* if each of its designs admits the permutation group G as an automorphism group.

Let G be a finite permutation group on X. For $x \in X$, the *orbit* of x is $G(x) = \{gx|\ g \in G\}$ and the *stabilizer* of x is $G_x = \{g \in G|\ gx = x\}$. Orbits of size $|G|$ are called *regular* and other orbits are said to be *short*. If there is an $x \in X$ such that $G(x) = X$, then G is called *transitive*. The action of G on X induces a natural action on $P_t(X)$. If this latter action is transitive, then G is called *t-homogeneous*. All t-homogeneous groups for $t \ge 2$ are known, see for example [7]. For an example of these groups, we can name the group $\mathrm{PSL}(2,q)$ with its natural action on the projective line. It is 3-homogeneous for $q \equiv 3 \pmod 4$ and is proved to be very useful in constructing t-designs and large sets, see for example [3, 5, 6, 11, 12].

3 Combining orbits to large sets

In the sequel of the paper we let G be a t-homogeneous permutation group on a v-set X. It is easy to see that any orbit from the action of G on $P_k(X)$ is the block set of a t-(v,k,λ) design for some λ. A natural question which arises is for which values of N, an $\mathrm{LS}[N](t,k,v)$ can be obtained from a suitable combination of these orbits. This problem in general is a bin-packing problem which is known to be NP-hard. However, it can be answered in some special cases. First of all, suppose that all orbits are of the same size. In this case, the problem is trivial, since we only need N to be a divisor of the total number of orbits. It is worth noting that it may not be a trivial task to find the circumstances under which this situation happens. In [6], this has been discussed for the group $\mathrm{PSL}(2,q)$.

The next case is when the orbit sizes are limited to two values. A special situation of this case is discussed in [11] (see Corollary 3.1). Here, we give a complete solution. First we need to state the following lemma.

Lemma 3.1 *Let n,m and e be integers. Then the system of equations $\sum_{i=1}^{e} z_i = m$, $\sum_{i=1}^{e} iz_i = n$ has a nonnegative integer solution if and only if $0 \leq m \leq n \leq em$.*

Proof Let $0 \leq m \leq n \leq em$. If $n = em$, then we have the solution $z_e = m$ and $z_i = 0$, otherwise. So let $n < em$. Take $2 \leq f \leq e$ such that $(f-1)m \leq n < fm$. Then we have the solution $z_{f-1} = fm - n$, $z_f = n - (f-1)m$ and $z_i = 0$, otherwise. The converse is trivial. □

Theorem 3.1 *Suppose that there are exactly a_i orbits of size l_i $(i = 1, 2)$ in the action of G on $P_k(X)$. For $i = 1, 2$, let $f_i = l_i/(l_1, l_2)$, where (l_1, l_2) is the greatest common divisor of l_1 and l_2. Then there exists a G-uniform* LS$[N](t, k, v)$ *if and only if there are integers m_i $(i = 1, 2)$ such that $0 \leq (-1)^i m_i \leq (a_1 a_2)/(a_i f_i)$ and $N \Big| (a_1 - m_i f_2, a_2 + m_i f_1)$.*

Proof We have $l_1 a_1 + l_2 a_2 = \binom{v}{k}$. Let N be a natural number. Then there exist nonnegative integers x, y such that $l_1 x + l_2 y = \binom{v}{k}/N$ if and only if there is an integer m with $-a_2/f_1 \leq m \leq a_1/f_2$ and $N \Big| (a_1 - m f_2, a_2 + m f_1)$. This is easy to see, since we have $x = (a_1 - m f_2)/N$ and $y = (a_2 + m f_1)/N$.

Let h be the number of nonnegative integer solutions of $l_1 x + l_2 y = \binom{v}{k}/N$. If $h > 0$ and m_1 is the smallest m such that $-a_2/f_1 \leq m \leq a_1/f_2$ and $N \Big| (a_1 - m f_2, a_2 + m f_1)$, then the solutions are

$$(x_i, y_i) = (z - i f_2, y_i),$$

where $1 \leq i \leq h$ and $z = (a_1 + (N - m_1) f_2)/N$. There exists a G-uniform LS$[N](t, k, v)$ if and only if $h > 0$ and the system of equations $\sum_{i=1}^{h} n_i = N$, $\sum_{i=1}^{h} x_i n_i = a_1$ (in variables n_i) has a nonnegative integer solution (and equivalently so has the system of equations $\sum_{i=1}^{h} n_i = N$, $\sum_{i=1}^{h} i n_i = (Nz - a_1)/f_2$). By Lemma 3.1, the system has a a nonnegative integer solution for $h > 0$ if and only if $-a_2/f_1 \leq m_1 \leq a_1/f_2$ and

$$0 \leq N \leq \frac{Nz - a_1}{f_2} \leq hN,$$

or equivalently $-a_2/f_1 \leq m_1$ and

$$0 \leq (a_1 - m_2 f_2) \leq a_1 \leq (a_1 - m_1 f_2),$$

where $m_2 = (a_1 - Nx_h)/f_2$. This yields that there exists a G-uniform $\mathrm{LS}[N](t,k,v)$ if and only if there are integers $0 \leq m_2 \leq a_1/f_2, -a_2/f_1 \leq m_1 \leq 0$ such that $N \big| (a_1 - m_i f_2, a_2 + m_i f_1)$ for $i = 1, 2$. $\square$

The following special case of the above theorem frequently is applicable, since actions mostly contain regular orbits.

Corollary 3.1 **[11]** *Suppose that there are exactly a_1 orbits of size rl and a_2 orbits of size l in the action of G on $P_k(X)$. Then there exists a G-uniform* $\mathrm{LS}[N](t,k,v)$ *if and only if there is an integer m such that $0 \leq m \leq a_2/r$ and $N \big| (a_1 + m, a_2 - rm)$.*

Proof By taking $m_2 = a_1$ and $m_1 = -m$ in Theorem 3.1, the assertion follows. $\square$

Remark Note that the above results may also be useful in the general case. If we are able to combine the orbits to larger sets in a way such that all resulting sets are only of two sizes, then we can use the above results. This is demonstrated in the next corollary.

Corollary 3.2 *Suppose that the union of all short orbits in the action of G on $P_k(X)$ is of size $|G|r$. Then there exists a G-uniform* $\mathrm{LS}[N](t,k,v)$ *if and only if $N \big| \binom{v}{k}/|G|$ and $N \leq \binom{v}{k}/(|G|r)$.*

Proof Let $a_1 = 1, l = |G|$ and $m = N-1$ in Corollary 3.1. The assertion is immediate as explained in the above remark. $\square$

4 A special case

In this section we consider a special case in which we can establish the existence of some G-uniform large sets without having any knowledge about orbits. To do this, we will assume the extra condition $|G| \big| \binom{v}{k}$. First we state two related results.

Theorem 4.1 [11] *Suppose that each orbit from the action of G on $P_k(X)$ is of size either $|G|$ or $|G|/m$ for a fixed integer m. If $|G| \big| \binom{v}{k}$, then there exists a G-uniform* $\mathrm{LS}\left[\binom{v}{k}/|G|\right](t,k,v)$.

A similar theorem is the following.

Theorem 4.2 *Suppose that each orbit from the action of G on $P_k(X)$ is of size $|G|$, $|G|/m$, $|G|/n$ or $|G|/(mn)$ for fixed distinct integers m and n. Moreover, suppose that there is only one orbit of size $|G|/(mn)$. If $|G| \mid \binom{v}{k}$, then there exists a G-uniform* $\mathrm{LS}\big[\binom{v}{k}/|G|\big](t,k,v)$.

Proof Let $|G| \mid \binom{v}{k}$. Let a_i be the number of orbits of size $|G|/i$. From the assumptions, we have

$$a_1|G| + a_m\frac{|G|}{m} + a_n\frac{|G|}{n} + \frac{|G|}{mn} = \binom{v}{k}.$$

Dividing by $|G|$ yields

$$\frac{a_m}{m} + \frac{a_n}{n} + \frac{1}{mn} = \binom{v}{k}/|G| - a_1 = s,$$

where s is a natural number at least 1. Let $a_m = b_m m + a'_m$ with $0 \le a'_m < m$. Then we subtract b_m from both sides to reduce the first fraction to a value smaller than 1. We reduce the second fraction the same way and obtain

$$\frac{a'_m}{m} + \frac{a'_n}{n} + \frac{1}{mn} = s',$$

where s' is a natural number at least 1. We have

$$\begin{aligned} na'_m + ma'_n + 1 &\le mn - n + mn - m + 1 \\ &= 2mn - (m + n - 1) \\ &< 2mn. \end{aligned}$$

Thus, $s' < 2$ and so $s' = 1$.

We see from the computation that we can assemble b_m times m orbits of size $\frac{|G|}{m}$ to a family of $|G|$ k-subsets and as well b_n times n orbits of size $|G|/n$ to a family of $|G|$ k-subsets such that the union of the remaining orbits consists again of exactly $|G|$ k-subsets. We have partitioned $P_k(X)$ into parts each of size $|G|$ such that the claimed result holds. □

Lemma 4.1 *Let $p^f \equiv 3 \pmod 4$ and let G be the group $\mathrm{PSL}(2,p^f)$ acting on the projective line X. Let $k \ge 3$ be odd and p no divisor of $k-1$. In* *each of the following cases there exists exactly one orbit of size $|G|/l$ on $P_k(X)$:*

(i) *$l = k \big| p^f + 1$ and $((k-1)(k-2), p^f - 1) = 1$,*
(ii) *$l = k \big| p^f - 1$,*
(iii) *$l = k - 1 \big| p^f - 1$ and $(k, p^f + 1) = 1$,*
(iv) *$l = k - 2 \big| p^f - 1$ and $(k, p^f + 1) = 1$.*

Moreover, the condition that $|G|$ divides $\binom{p^f+1}{k}$ is fulfilled if and only if $k(k-1)(k-2)$ divides $2 \cdot \binom{p^f-2}{k-3}$.

The proof is obtained by the same arguments as in [11].

Example Let G and X be as in Lemma 4.1. For $k = q_1 \cdot q_2$ with two different odd primes q_1, q_2 dividing $p^f - 1$ and $k - 1$ not divisible by p, by Lemma 4.1, we obtain that there is exactly one orbit with a stabilizer of order k. There are

$$\frac{q_1}{p^f - 1}\left\{\binom{\frac{p^f-1}{q_1}}{q_2} - \frac{p^f - 1}{k}\right\} = \frac{1}{q_2}\left\{\binom{\frac{p^f-1}{q_1} - 1}{q_2 - 1} - 1\right\}$$

orbits with a stabilizer of order q_1 and the analogous number for q_2. Let for example $p^f = 31$ and $k = 15$. Then there are 1, 3, 25, 38010 orbits with stabilizer orders 15, 5, 3, 1, respectively. Since $|G| \big| \binom{32}{15}$, by Theorem 4.2, there exists an LS$[N](3, 15, 32)$ for $N = \binom{32}{15}/|G| = 38019$. Generally, for all prime powers p^f such that 15 divides $p^f - 1$ and $p > 7$, we have that there is exactly one orbit of 15-subsets with stabilizers of order 15, and $|G|$ divides $\binom{p^f+1}{15}$ if $p^f - 1 \equiv 3, 6, 9, 18 \pmod{27}$, $p^f - 1 \equiv 5, 10 \pmod{25}$ and $p^f \equiv 2, \ldots, 13 \pmod{13}$. By the Chinese Remainder Theorem and Dirichlet's Theorem [8] for each combination of the conditions, there exist infinitely many primes p that fulfill them such that there result infinitely many large sets of 3-designs with block size 15 from Theorem 4.2. Similar results can be obtained for other values of k. For example, if we let $p^f = 127$ and $k = 23$, we find an LS$[N](3, 23, 128)$ where

$$N = \frac{\binom{128}{23}}{128 \cdot 127 \cdot 63}.$$

Again, there are infinitely many cases of primes like 127 where the same congruences are fulfilled and large sets of block size 23 result.

We now come to the main theorem.

Theorem 4.3 *Let* $|G| \big| \binom{v}{k}$ *and* $|G| = \prod_{i=1}^{r} p_i^{m_i}$, *where the* p_i *are distinct primes and* $p_i < p_j$ *if* $i < j$. *Then* $m = \sum_{i=1}^{r} \big(\prod_{j=i}^{r} p_j/(p_j - 1) \big) \leq 3r$ *and for any natural number* N *such that* $N \big| \binom{v}{k}/|G|$ *and* $N \leq \binom{v}{k}/(|G|m)$ *there exists a* G*-uniform* $\mathrm{LS}[N](t, k, v)$.

Proof First we show that $\sum_{i=1}^{r} \big(\prod_{j=i}^{r} p_j/(p_j - 1) \big) \leq 3r$. Let q_i be the ith prime number in the natural order of prime numbers. It is easily seen that $q_i/(q_i - 1) \leq \sqrt{(i-1)/(i-2)}$ for $i > 2$. We have

$$\begin{aligned}
\sum_{i=1}^{r} \big(\prod_{j=i}^{r} \frac{p_j}{p_j - 1}\big) &\leq \sum_{i=1}^{r} \big(\prod_{j=i}^{r} \frac{q_j}{q_j - 1}\big) \\
&\leq 3 \prod_{j=3}^{r} \sqrt{\frac{j-1}{j-2}} + \frac{3}{2} \prod_{j=3}^{r} \sqrt{\frac{j-1}{j-2}} + \sum_{i=3}^{r} \Big(\prod_{j=i}^{r} \sqrt{\frac{j-1}{j-2}} \Big) \\
&= \sqrt{r-1} \Big(\frac{9}{2} + \sum_{i=1}^{r-2} \frac{1}{\sqrt{i}} \Big) \\
&\leq \sqrt{r-1} \Big(\frac{9}{2} + \int_{1}^{r-2} \frac{1}{\sqrt{x}} dx + 1 \Big) \\
&\leq \sqrt{r-1} \Big(\frac{7}{2} + 2\sqrt{r-2} \Big) \\
&\leq 3r.
\end{aligned}$$

For a natural integer n, let $S(n)$ be the sum of its divisors. Then, by a well known result from number theory (see for example [8, Theorem 275]), if $n = \prod_{i=1}^{s} q_i^{n_i}$, where q_i are distinct primes, then

$$\begin{aligned}
S(n) &= \prod_{i=1}^{s} \frac{q_i^{n_i+1} - 1}{q_i - 1} \\
&\leq n \big(\prod_{i=1}^{s} \frac{q_i}{q_i - 1} \big). \qquad (4.1)
\end{aligned}$$

We know that any orbit size from the action of G on $P_k(X)$ is a divisor of $|G|$. For any divisor $f > 1$ of $|G|$, let $p(f)$ be the smallest prime divisor of f. If there are at least $p(f)$ orbits of size $|G|/f$, then we replace any $p(f)$ of them by their union. We repeatedly apply this procedure to all orbits and intermediate unions until it cannot be applied anymore. Now let O be the union of all sets of size nonequal to $|G|$. By the assumption, $|O| = l|G|$

for some integer l. From the procedure and (4.1), we have

$$\begin{aligned}
l|G| &\leq \sum_{f \big| |G|, f>1} \frac{(p(f)-1)|G|}{f} \\
&= \sum_{i=1}^{r} (p_i - 1)\Big(\sum_{p(f)=p_i} \frac{|G|}{f} \Big) \\
&= \sum_{i=1}^{r} (p_i - 1)\Big(\prod_{j=1}^{i-1} p_j^{m_j} \Big) S\Big(\frac{|G|}{p_i \prod_{j=1}^{i-1} p_j^{m_j}} \Big) \\
&\leq |G| \sum_{i=1}^{r} \Big(\prod_{j=i}^{r} \frac{p_j}{p_j - 1} \Big).
\end{aligned}$$

Therefore, $l \leq \sum_{i=1}^{r} \big(\prod_{j=i}^{r} p_j/(p_j - 1) \big)$. Now that we have one set of size $l|G|$ and the other sets are of size $|G|$, by Corollary 3.2, the proof is complete. $\square$

Theorem 4.4 *Let $|G| \big| \binom{v}{k}$. Suppose that all stabilizer sizes of orbits from the action of G on $P_k(X)$ are divisors of a fixed natural number n and $(n, |G|) = \prod_{i=1}^{r} p_i^{m_i}$, where the p_i are distinct primes and $p_i < p_j$ if $i < j$. Then $m = \sum_{i=1}^{r} \big(\prod_{j=i}^{r} p_j/(p_j - 1) \big) \leq 3r$ and there exists a G-uniform $\mathrm{LS}[N](t, k, v)$ for any natural number N such that $N \big| \binom{v}{k}/|G|$ and $N \leq \binom{v}{k}/(|G|m)$.*

Proof The proof is similar to that of theorem 4.3. $\square$

We finish the paper with two conjectures.

Conjecture 4.1 *We conjecture that it would be possible to let $m = r$ in Theorems 4.3 and 4.4.*

Conjecture 4.2 *Let q be an odd prime power and let $G = \mathrm{PSL}(2, q)$ if $q \equiv 3 \pmod 4$ and $G = \mathrm{PGL}(2, q)$, otherwise. If $|G| \big| \binom{q+1}{k}$, then there exists a G-uniform $\mathrm{LS}\big[\binom{q+1}{k}/|G|\big](3, k, q + 1)$.*

Using the results from [3] and [4], we have checked the second conjecture for $q < 60$, see [12].

References

[1] S. Ajoodani-Namini, Extending large sets of t-designs, *J. Combin. Theory Ser. A* **76** (1996), 139–144.

[2] S. Ajoodani-Namini and G. B. Khosrovshahi, More on halving the complete designs, *Discrete Math.* **135** (1994), 29–37.

[3] P. J. Cameron, H. R. Maimani, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PSL}(2, q)$, *Discrete Math.*, to appear.

[4] P. J. Cameron, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $\mathrm{PGL}(2, q)$, submitted.

[5] C. A. Cusack, S. W. Graham and D. L. Kreher, Large sets of 3-designs from $\mathrm{PSL}(2, q)$, with block sizes 4 and 5, *J. Combin. Des.* **3** (1995), 147–160.

[6] C. A. Cusack and S. S. Magliveras, Semiregular large sets of t-designs, *Des. Codes Cryptogr.* **18** (1999), 81–87.

[7] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, 163, Springer-Verlag, New York, 1996.

[8] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers,* Fourth edition, Oxford Press, 1965.

[9] G. B. Khosrovshahi and B. Tayfeh-Rezaie, Large sets of t-designs through partitionable sets: A survey, *Discrete Math.*, to appear.

[10] G. B. Khosrovshahi and B. Tayfeh-Rezaie, Root cases of large sets of t-designs, *Dicrete Math.* **263** (2003), 143–155.

[11] R. Laue, S. S. Magliveras and A. Wassermann, New large sets of t-designs, *J. Combin. Des.* **9** (2001), 40–59.

[12] R. Laue, G. R. Omidi and B. Tayfeh-Rezaie, New large sets of t-designs with prescribed automorphism groups, submitted.