

BLOCK-TRANSITIVE 3-DESIGNS WITH AFFINE AUTOMORPHISM GROUP

Greg Gamble

Let $X = (\mathbb{Z}_p)^d$ where p is an odd prime and $d \in \mathbb{N}$, and let $B \subseteq X$, $|B| = k$. Then it was shown by Praeger that the set $\mathcal{B} = \{B^g \mid g \in \text{AGL}_d(p)\}$ is the block-set of a 3-design if and only if the number $q_1(k)$ of collinear triples of points of B is

$$q_1(k) = \frac{k(k-1)(k-2)(p-2)}{6(p^d-2)}.$$

We give an explicit method for determining all k such that $3 \leq k < p^d/2$ and $q_1(k)$ is an integer. For $p = 3$ the smallest value of d for which there is such an integral value of $q_1(k)$ is $d = 7$ and the smallest $k \geq 3$ giving integral values of $q_1(k)$ are $k = 115$ and $k = 116$. We construct many examples of 3-designs (X, \mathcal{B}) with $k = 115$ or 116 admitting $\text{AGL}_7(3)$ as automorphism group.

1. INTRODUCTION

A t - (v, k, λ) design is a pair $\mathcal{D} = (X, \mathcal{B})$ where X is a set of v points and \mathcal{B} is a set of k -subsets of X called *blocks* such that any t points are contained in exactly $\lambda > 0$ blocks. If \mathcal{B} contains all k -subsets of X then \mathcal{D} is said to be *trivial*. Let $G = \text{Aut } \mathcal{D} = \{g \in \text{Sym}(X) \mid \mathcal{B}^g = \mathcal{B}\}$. That is, G is the set of all permutations of X that fix \mathcal{B} setwise. The group G is said to be *block-transitive* if $\mathcal{B} = B^G$ for $B \in \mathcal{B}$, where $B^G = \{B^g \mid g \in G\}$. In this case we say that \mathcal{D} is block-transitive. Similarly, G is *point-transitive* if $X = x^G$ for some $x \in X$, where $x^G = \{x^g \mid g \in G\}$.

By [2], G block-transitive implies that G is point-transitive and thus that G is a transitive subgroup of $\text{Sym}(X)$. Also by [3, Proposition 1.1] (or see [5]), if (X, B^G) is a block-transitive t - (v, k, λ) design and $G \leq H \leq \text{Sym}(X)$ then (X, B^H) is a block-transitive t - (v, k, λ^*) design for some $\lambda^* \geq \lambda$. Hence in searching for non-trivial block-transitive t -designs we may start by considering maximal subgroups of $\text{Sym}(X)$. As noted by [5],

the O’Nan-Scott theorem implies that if G is a transitive maximal subgroup of S_v then it is of one of the following types:

1. imprimitive: $G = S_c \text{ wr } S_d$ for some $c, d \in \mathbb{N}$ such that $v = cd$, $c > 1$, $d > 1$;
2. affine: $G = \text{AGL}_d(p)$ for some $p, d \in \mathbb{N}$ such that $v = p^d$, p prime, $d \geq 1$;
3. product: $G = S_c \text{ wr } S_d$ for some $c, d \in \mathbb{N}$ such that $v = c^d$, $c \geq 5$, $d > 1$;
4. simple diagonal: $G = T^d.(\text{Out } T \times S_d)$ for some $d \in \mathbb{N}$ and some group T such that $v = |T|^{d-1}$, $d > 1$ and T is nonabelian and simple;
5. almost simple: $T \leq G \leq \text{Aut } T$ for some nonabelian simple group T .

We are concerned with the second of these cases, $G = \text{AGL}_d(p)$. We say a group G is t -homogeneous on a set X if it is transitive on the set of t -subsets of X . If G is t -homogeneous then for any k and any k -subset B of X , (X, B^G) is a t -design; and, further, if G is k -homogeneous the design is trivial. The group $\text{AGL}_d(p)$ is 2-transitive and hence 2-homogeneous for all d, p and $\text{AGL}_d(2)$ is 3-transitive and hence 3-homogeneous for all $d \geq 2$. Thus we consider the more interesting problem of the existence of block-transitive t -designs admitting $G = \text{AGL}_d(p)$ with $t \geq 3$ for p odd, and in particular we consider the case where $t = 3$.

The following lemma is essentially Lemma 1.10(c) of [4] (or see [3, Proposition 1.3] or see [5]). It is a corollary of Theorem 2.1, a proof of which was supplied to the author by Praeger [6] and is reproduced with minor modifications in the next section.

1.1. LEMMA. (X, B^G) is a block-transitive t -design if and only if $(X, (X \setminus B)^G)$ is a block-transitive t -design.

This result allows us to restrict our attention to designs for which $3 = t \leq k < p^d/2$ where k is the block-size, as if there is no design for a k in this range then there is certainly no design for k satisfying $p^d/2 \leq k < p^d - 2$ and, of course, for $k \in \{p^d - 2, p^d - 1, p^d\}$, all blocks B such that $|B| = k$ give rise to trivial designs.

For p an odd prime, $d \geq 2$ and $G = \text{AGL}_d(p)$ Praeger [5, Lemma 2.1] has shown that (X, B^G) is a block-transitive 3-design if and only if the number of collinear triples in the block B is

$$q_1(k) = \frac{k(k-1)(k-2)(p-2)}{6(p^d-2)},$$

where $k = |B|$. We prove this result in Section 2. In Section 2 we prove a number of lemmas which are needed to prove Theorem 3.1, from which the following theorem is a corollary. The theorem shows how to construct the set Ω' of all k such that $q_1(k) \in \mathbb{N}$ and $3 \leq k < p^d/2$.

1.2. THEOREM. Let $2 \neq p$ prime, $d \geq 2$, $q_1(k) = \frac{k(k-1)(k-2)(p-2)}{6(p^d-2)}$ and $D =$

$(p^d - 2, p - 2)$. Let $N = \frac{p^d - 2}{D'} = \prod_{i=1}^n p_i^{\varepsilon_i}$, where p_i are distinct primes, $n, \varepsilon_i \in \mathbb{N}$ and

$$D' = \begin{cases} D & \text{if } 3D \nmid p^d - 2, \\ D/3 & \text{if } 3D \mid p^d - 2. \end{cases}$$

Suppose $u_i = \frac{N}{p_i^{\varepsilon_i}}$ and $t_i \in \mathbb{Z}$ satisfy $\sum_{i=1}^n u_i t_i = 1$.

Let $\Omega' = \{k \mid q_1(k) \in \mathbb{N} \text{ and } 3 \leq k \leq p^d/2\}$. Then

(i) Each element k of Ω' has the form $k = (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) + lN$, where $\alpha_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$ and $0 \leq l < D'/2$.

(ii) $|\Omega'| = \frac{D' \cdot 3^n - 3}{2}$.

The t_i of the theorem may be calculated by Algorithm 3.2. An immediate consequence of this theorem is an observation of Praeger [5, p. 196], namely that there are no nontrivial block-transitive 3-designs admitting $G = \text{AGL}_d(3)$ for $d \in \{2, \dots, 6\}$, as for each of these values of d the number n of distinct prime divisors of N is 1, so that the set Ω' is empty. However for $d = 7$ we find Ω' is not empty. Praeger [5, p. 196] posed the question: Is there a block-transitive 3 - $(3^7, k, \lambda)$ design of this type? In Section 4 we show, for at least two values of k that indeed there are such designs.

2. PRELIMINARY RESULTS

The following theorem is included mainly because the author feels it may eventually lead to new results of non-existence of t -designs. It is a self-contained version of Corollary 1.4(a) and Lemma 1.10(c) of Hughes and Piper [4].

2.1. THEOREM. [6] If $\mathcal{D} = (X, \mathcal{B})$ is a t - (v, k, λ) design then

(i) $\mathcal{D} = (X, \mathcal{B})$ is a t' - $(v, k, \lambda_{t'})$ design for all t' such that $0 \leq t' \leq t$ where

$$\lambda_{t'} = \frac{\binom{k}{t'}}{\binom{v}{t'}} \cdot |\mathcal{B}| ;$$

(that is, if $0 \leq t' \leq t$, $C \subseteq X$, $|C| = t'$ then

$$\lambda_{t'} := |\{B \in \mathcal{B} \mid C \subseteq B\}| = \frac{\binom{k}{t'}}{\binom{v}{t'}} \cdot |\mathcal{B}|$$

is independent of the choice of $C \in \{C \subseteq X \mid |C| = t'\}$;))

(ii) if $0 \leq i \leq t$, $D \subseteq C \subseteq X$, $|D| = i$, $|C| = t$ then $\mu_i := |\{B \in \mathcal{B} \mid D = C \cap B\}|$ is independent of C and the subset D of C , and

$$\begin{cases} \mu_t = \lambda_t = \lambda \\ \mu_i = \lambda_i - \sum_{j=1+i}^t \binom{t-i}{j-i} \cdot \mu_j \quad \text{for } 0 \leq i < t; \end{cases}$$

(iii) $\mathcal{D}' = (X, \mathcal{B}')$ is a t - (v, k, μ_0) design where $\mathcal{B}' = \{B' = (X \setminus B) \mid B \in \mathcal{B}\}$.

PROOF. (i) $\lambda_t = \lambda$ is independent of C as \mathcal{D} is a t -design.

Suppose $0 \leq i < t$ and λ_{i+1} is independent of $C \in \{C \subseteq X \mid |C| = i+1\}$.

Let $C_i \in \{C \subseteq X \mid |C| = i\}$, $\lambda_i(C_i) := |\{B \in \mathcal{B} \mid C_i \subseteq B\}|$ then counting two ways

$$|\{(x, B) \mid \{x\} \cup C_i \subseteq B, x \notin C_i, B \in \mathcal{B}\}| = \lambda_i(C_i) \cdot (k - i) = (v - i) \cdot \lambda_{i+1}.$$

That is, $\lambda_i = \lambda_i(C_i) = \frac{v-i}{k-i} \cdot \lambda_{i+1}$ is independent of $C_i \in \{C \subseteq X \mid |C| = i\}$.

Thus, by induction, λ_i is independent of $C \in \{C \subseteq X \mid |C| = i\}$ for all i such that $0 \leq i \leq t$.

Also $\lambda_0 = |\{B \in \mathcal{B} \mid \emptyset \subseteq B\}| = |\mathcal{B}|$, $\lambda_{i+1} = \frac{k-i}{v-i} \cdot \lambda_i$. Thus, by induction,

$$\lambda_i = \left(\prod_{j=0}^{i-1} \frac{k-j}{v-j} \right) \cdot \lambda_0 = \frac{\binom{k}{i}}{\binom{v}{i}} \cdot |\mathcal{B}|, \text{ for } 0 \leq i \leq t.$$

(ii) We write \sqcup for disjoint union.

Let $0 \leq i \leq t$, $D \subseteq C \subseteq X$, $|D| = i$, $|C| = t$, then

$$\begin{aligned} \lambda_i &= |\{B \in \mathcal{B} \mid D \subseteq B\}| = |\{B \in \mathcal{B} \mid D \subseteq C \text{ and } D \subseteq B\}| \\ &= |\{B \in \mathcal{B} \mid D \subseteq C \cap B\}|. \end{aligned}$$

If $i = t$ then $|D| = t$ and

$$D \subseteq C \cap B \iff D = C \cap B.$$

That is, $\mu_t = \lambda_t$ is independent of C and for each choice of C , $D = C$ is unique.

Suppose now that $0 \leq i < t$ and that μ_j is independent of C and the subset $D \in \{D \subseteq C \mid |D| = j\}$,

for $i < j \leq t$. Let $D_i \subseteq C$, $|D_i| = i$, $\mu_i(C, D_i) := |\{B \in \mathcal{B} \mid D_i = C \cap B\}|$. Then

$$\begin{aligned} \mu_i(C, D_i) &= |\{B \in \mathcal{B} \mid D_i \subseteq C \cap B \text{ and } |C \cap B| = i\}| \\ &= |\{B \in \mathcal{B} \mid D_i \subseteq C \cap B\} \setminus \{B \in \mathcal{B} \mid D_i \subseteq C \cap B \text{ and } |C \cap B| > i\}| \\ &= \lambda_i - |\{B \in \mathcal{B} \mid D_i \subseteq C \cap B \text{ and } |C \cap B| > i\}| \\ &= \lambda_i - \left| \bigsqcup_{j=i+1}^t \{B \in \mathcal{B} \mid D_i \subseteq C \cap B \text{ and } |C \cap B| = j\} \right| \\ &= \lambda_i - \sum_{j=i+1}^t |\{B \in \mathcal{B} \mid D_i \subseteq C \cap B \text{ and } |C \cap B| = j\}| \\ &= \lambda_i - \sum_{j=i+1}^t \left| \bigsqcup_{\substack{E \subseteq C \setminus D_i \\ |E|=j-i}} \{B \in \mathcal{B} \mid D_i \cup E = C \cap B\} \right| \\ &= \lambda_i - \sum_{j=i+1}^t \binom{t-i}{j-i} \cdot \mu_j \end{aligned}$$

is independent of C and the choice of $D_i \in \{D \subseteq C \mid |D| = i\}$. Thus, by induction,

$$\begin{aligned} \mu_i &:= |\{B \in \mathcal{B} \mid D = C \cap B\}| \\ &= \lambda_i - \sum_{j=i+1}^t \binom{t-i}{j-i} \cdot \mu_j \text{ for } 0 \leq i \leq t \end{aligned}$$

is independent of $C \in \{C \subseteq X \mid |C| = t\}$ and the choice of $D \in \{D \subseteq C \mid |D| = i\}$.

$$\begin{aligned} \text{(iii) } \mu_0 &= |\{B \in \mathcal{B} \mid B \cap C = \emptyset\}| = |\{B \in \mathcal{B} \mid C \subseteq B' = (X \setminus B)\}| \\ &= |\{B' \in \mathcal{B}' \mid C \subseteq B'\}| \end{aligned}$$

is independent of $C \in \{C \subseteq X \mid |C| = t\}$.

That is, $\mathcal{D}' = (X, \mathcal{B}')$ is a t - (v, k, μ_0) design. ■

The following theorem (noted in [5] or see [4, pp. 146–147] or [1]) allows us to reduce the problem of existence of designs to a fairly elementary number theory problem.

2.2. THEOREM. *If B is a k -subset of X , $G \leq \text{Sym}(X)$, Q_1, \dots, Q_m are the G -orbits on t -sets of X , $q_i = |Q_i \cap B|$ for $1 \leq i \leq m$ then*

$$\begin{aligned} (X, B^G) \text{ is a } t\text{-design} &\iff \frac{q_1}{|Q_1|} = \dots = \frac{q_m}{|Q_m|} \\ &\iff \frac{q_j}{|Q_j|} = \frac{\sum_{i=1}^m q_i}{\sum_{i=1}^m |Q_i|} \text{ for } 1 \leq j \leq m. \end{aligned}$$

The group $G = \text{AGL}_d(p)$ has 2 orbits on the 3-sets of $X = (\mathbb{Z}_p)^d$ namely

$Q_1 :=$ collinear triples,

$Q_2 :=$ non-collinear triples,

where we say $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a *collinear triple* if and only if $\mathbf{u}, \mathbf{v}, \mathbf{w}$ are distinct and $\mathbf{w} = \mathbf{u} + \alpha(\mathbf{v} - \mathbf{u})$ for some $\alpha \in \mathbb{Z}_p$. Equivalently $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a *collinear triple* if and only if $\mathbf{v} \neq \mathbf{u}$ and $\mathbf{w} = \mathbf{u} + \alpha(\mathbf{v} - \mathbf{u})$ for some $\alpha \in \mathbb{Z}_p \setminus \{0, 1\}$. Thus we see that

$$|Q_1| = \frac{p^d \cdot (p^d - 1) \cdot (p - 2)}{3!}$$

as for ordered triples $(\mathbf{u}, \mathbf{v}, \mathbf{w})$ there are p^d choices for \mathbf{u} , leaving $p^d - 1$ choices for \mathbf{v} and then $p - 2$ choices for α (and hence \mathbf{w}). So by Theorem 2.2

$$\frac{q_1}{|Q_1|} = \frac{q_1 + q_2}{|Q_1| + |Q_2|} = \frac{\#\text{triples in } B}{\#\text{triples in } X} = \frac{\binom{k}{3}}{\binom{p^d}{3}}.$$

Hence we arrive at the conclusion of [5, Lemma 2.1],

$$q_1 = \frac{\binom{k}{3}}{\binom{p^d}{3}} \cdot \frac{p^d \cdot (p^d - 1) \cdot (p - 2)}{3!} = \frac{k(k-1)(k-2)(p-2)}{6 \cdot (p^d - 2)}.$$

Of course, q_1 is an integer. The following lemma gives a simpler equivalent condition for the integrality of q_1 , in terms of an integer N which is easy to calculate.

2.3. LEMMA. *Let $2 \neq p$ prime, $q_1 = \frac{k(k-1)(k-2)(p-2)}{6 \cdot (p^d - 2)}$, where $d, k \in \mathbb{N}$, and let $D = (p-2, p^d - 2)$. Then*

$$q_1 \in \mathbb{Z} \iff \frac{k(k-1)(k-2)}{N} \in \mathbb{Z}$$

where $N = \frac{p^d - 2}{D'}$ and $D' = \begin{cases} D & \text{if } 3D \nmid p^d - 2, \\ D/3 & \text{if } 3D \mid p^d - 2. \end{cases}$

PROOF. Firstly,

$$q_1 = \frac{k(k-1)(k-2)(p-2)}{6(p^d - 2)} = \frac{k(k-1)(k-2)a}{6b},$$

where $a = (p-2)/D$, $b = (p^d - 2)/D$. So $q_1 \in \mathbb{Z}$ if and only if $6b \mid k(k-1)(k-2)a$. Of course, for any $k \in \mathbb{N}$, $6 \mid k(k-1)(k-2)$. Observe that $2 \neq p$ prime implies that $2 \nmid (p^d - 2)$ and hence $2 \nmid b$. Also $(a, b) = 1$. Now we consider two cases.

Case 1. Assume $3 \nmid b$ (or equivalently $3D \nmid p^d - 2$). In this case we define $D' = D$, so that $N = (p^d - 2)/D' = b$. Thus $q_1 \in \mathbb{Z}$ if and only if $N = b \mid k(k-1)(k-2)$.

Case 2. Assume $3 \mid b$ (or equivalently $3D \mid p^d - 2$). In this case we define $D' = D/3$, so that $N = (p^d - 2)/D' = 3b$. As $(a, b) = 1$, and by assumption $3 \mid b$, we have $3 \nmid a$. Thus $q_1 \in \mathbb{Z}$ if and only if $N = 3b \mid k(k-1)(k-2)$.

So we have that, $q_1 \in \mathbb{Z}$ if and only if $k(k-1)(k-2)/N \in \mathbb{Z}$. ■

Note that if $3 \mid p^d - 2$ then $3 \mid p - 2$ (as suppose $3 \nmid p - 2$, then $p \equiv \varepsilon \not\equiv 2 \pmod{3}$ for some $\varepsilon \in \{0, 1\}$, and hence $p^d \equiv \varepsilon \not\equiv 2 \pmod{3}$, so that $3 \nmid p^d - 2$). Thus we see that in Lemma 2.3, D' is always an integer (as if $3 \mid b$ then $3 \mid p^d - 2$ and hence $3 \mid p - 2$, so that $3 \mid D$ and $D' = D/3 \in \mathbb{Z}$); and consequently N is at most $p^d - 2$.

From the following lemma we have information as to how to construct integers k satisfying the integrality condition given in Lemma 2.3. We show in Algorithm 3.2 how to construct the t_i of 2.4 (iii).

2.4. LEMMA. *Let $k \in \mathbb{Z}$, $N = \prod_{i=1}^n p_i^{\varepsilon_i}$, where $2 \neq p_i$ are distinct primes and $n, \varepsilon_i \in \mathbb{N}$. Then the following are equivalent.*

$$(i) \frac{k(k-1)(k-2)}{N} \in \mathbb{Z},$$

$$(ii) k \equiv \alpha_i \pmod{p_i^{\varepsilon_i}} \text{ for some } \alpha_i \in \{0, 1, 2\} \quad \forall i : 1 \leq i \leq n,$$

$$(iii) k \equiv \sum_{i=1}^n \alpha_i u_i t_i \pmod{N} \text{ for some } \alpha_i \in \{0, 1, 2\} \text{ where } u_i = \frac{N}{p_i^{\varepsilon_i}} \text{ and } t_i \in \mathbb{Z} \text{ satisfy } \sum_{i=1}^n u_i t_i = 1.$$

PROOF. Any prime divisor p_i of N divides at most one of k , $k-1$, $k-2$, as $p_i \geq 3$. So, for each i such that $1 \leq i \leq n$, if $\frac{k(k-1)(k-2)}{N} \in \mathbb{Z}$ then $p_i^{\varepsilon_i}$ divides exactly one of k , $k-1$, $k-2$, and thus $k \equiv 0, 1$ or $2 \pmod{p_i^{\varepsilon_i}}$. Hence (i) implies (ii). (ii) implies (i) is trivial.

For $n = 1$, the equivalence of (ii) and (iii) is trivial, as then $u_1 = t_1 = 1$. For $n \geq 2$, the equivalence of (ii) and (iii), follows by application of the Chinese Remainder Theorem. ■

In the following lemma we show the uniqueness of the expression given in Lemma 2.4 (iii).

2.5. LEMMA. Let $N = \prod_{i=1}^n p_i^{\varepsilon_i}$, where $2 \neq p_i$ are distinct primes and $n, \varepsilon_i \in \mathbb{N}$, and let $u_i = \frac{N}{p_i^{\varepsilon_i}}$, $t_i \in \mathbb{Z}$ satisfy $\sum_{i=1}^n u_i t_i = 1$, and $\alpha_i, \beta_i \in \{0, 1, 2\}$. Then

$$\sum_{i=1}^n \alpha_i u_i t_i \equiv \sum_{i=1}^n \beta_i u_i t_i \pmod{N} \iff \alpha_i = \beta_i \quad \forall i : 1 \leq i \leq n.$$

PROOF. As $\sum_{i=1}^n u_i t_i = 1$ and $p_j^{\varepsilon_j} \mid u_i$ if $i \neq j$, we have $u_j t_j \equiv \sum_{i=1}^n u_i t_i \equiv 1 \pmod{p_j^{\varepsilon_j}}$ for $1 \leq j \leq n$.

Now suppose $\sum_{i=1}^n \alpha_i u_i t_i \equiv \sum_{i=1}^n \beta_i u_i t_i \pmod{N}$. Then

$$\alpha_j \equiv \alpha_j u_j t_j \equiv \sum_{i=1}^n \alpha_i u_i t_i \equiv \sum_{i=1}^n \beta_i u_i t_i \equiv \beta_j u_j t_j \equiv \beta_j \pmod{p_j^{\varepsilon_j}} \quad \forall j : 1 \leq j \leq n.$$

But $\alpha_j, \beta_j \in \{0, 1, 2\}$ and $p_j^{\varepsilon_j} \geq 3$ for $1 \leq j \leq n$. Hence $\alpha_j = \beta_j$ for $1 \leq j \leq n$. The converse is trivial. ■

We are now in a position to prove Theorem 3.1 which along with Algorithm 3.2 shows how to explicitly construct (and count) all k such that $q_1(k)$ is a positive integer and $3 \leq k < p^d/2$.

3. INTEGRALITY CONDITIONS

The following theorem shows how to construct the set Ω of all k such that $q_1(k) \in \mathbb{Z}$ and $0 \leq k \leq p^d$. We show that each k has a unique expression of a given form and that they occur in pairs (k, k') where $k' = p^d - k$. This is not surprising as, of course, if a block-transitive 3- (p^d, k, λ) design for some λ and admitting $\text{AGL}_d(p)$ exists then, by Theorem 1.1, its complementary design is a 3- (p^d, k', λ') design for some λ' . Below if $r \equiv \bar{r} \pmod{N}$ where $0 \leq \bar{r} < N$ then we take $(r \pmod{N}) + s$ to mean $\bar{r} + s$.

3.1. THEOREM. Let $2 \neq p$ prime, $d \geq 2$, $q_1(k) = \frac{k(k-1)(k-2)(p-2)}{6(p^d-2)}$ and $D = (p^d-2, p-2)$. Let $\Omega = \{k \mid q_1(k) \in \mathbb{Z} \text{ and } 0 \leq k \leq p^d\}$ and $\Omega' = \{k \in \Omega \mid 3 \leq k \leq p^d/2\}$. Let $N = \frac{p^d-2}{D'} = \prod_{i=1}^n p_i^{\varepsilon_i}$, where p_i are distinct primes, $n, \varepsilon_i \in \mathbb{N}$ and

$$D' = \begin{cases} D & \text{if } 3D \nmid p^d - 2, \\ D/3 & \text{if } 3D \mid p^d - 2. \end{cases}$$

Suppose $u_i = \frac{N}{p_i^{\varepsilon_i}}$ and $t_i \in \mathbb{Z}$ satisfy $\sum_{i=1}^n u_i t_i = 1$. Then

(i) Each element k of Ω is uniquely identified by an $(n+1)$ -tuple

$$(\alpha_1, \dots, \alpha_n, l),$$

where $k = (\sum_{i=1}^n \alpha_i u_i t_i \pmod{N}) + lN$, $\alpha_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$, $0 \leq l \leq D'$ and, if $l = D'$ then the α_i are all equal.

Also, if $k \in \Omega$ corresponds to $(\alpha_1, \dots, \alpha_n, l)$ then $k' = p^d - k \in \Omega$ and corresponds to

$$\begin{cases} (2 - \alpha_1, \dots, 2 - \alpha_n, D' - (l + 1)) & \text{if } \alpha_i \text{ not all equal,} \\ (2 - \alpha_1, \dots, 2 - \alpha_n, D' - l) & \text{if } \alpha_i \text{ all equal.} \end{cases}$$

$$(ii) |\Omega'| = \frac{D' \cdot 3^n - 3}{2}.$$

PROOF. (i) $q_1 \in \mathbb{Z} \iff \frac{k(k-1)(k-2)}{N} \in \mathbb{Z}$ (by Lemma 2.3)

$$\iff k \equiv \sum_{i=1}^n \alpha_i u_i t_i \pmod{N} \text{ for some } \alpha_i \in \{0, 1, 2\}, 1 \leq i \leq n$$

(by Lemma 2.4 (iii))

$$\iff k = (\sum_{i=1}^n \alpha_i u_i t_i \pmod{N}) + lN \text{ for some } \alpha_i \in \{0, 1, 2\},$$

$1 \leq i \leq n$, and $l \in \mathbb{Z}$.

Now suppose $\alpha_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$. Note that if the α_i are all equal then

$$\sum_{i=1}^n \alpha_i u_i t_i = \alpha_1 \left(\sum_{i=1}^n u_i t_i \right) = \alpha_1.$$

Hence by Lemma 2.5, $0 \leq (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) \leq 2$ if and only if the α_i are all equal. Thus

$$p^d - 2 = ND' \leq \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) + lN \leq ND' + 2 = p^d \\ \iff \alpha_i \text{ are all equal and } l = D'.$$

Consequently

$$0 \leq \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) + lN \leq p^d \iff \begin{cases} 0 \leq l < D' & \text{if } \alpha_i \text{ not all equal,} \\ 0 \leq l \leq D' & \text{if } \alpha_i \text{ all equal.} \end{cases}$$

Thus, each element k of Ω is identified by an $(n+1)$ -tuple, $(\alpha_1, \dots, \alpha_n, l)$, where $k = (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) + lN$, $\alpha_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$, $0 \leq l \leq D'$ and, if $l = D'$ then the α_i are all equal.

Now we show that each $k \in \Omega$ is uniquely identified by an $(n+1)$ -tuple of this form. Suppose that $k \in \Omega$ corresponds to both $(\alpha_1, \dots, \alpha_n, l_1)$ and $(\beta_1, \dots, \beta_n, l_2)$ then

$$\left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) + l_1 N = \left(\sum_{i=1}^n \beta_i u_i t_i \bmod N \right) + l_2 N,$$

so that

$$\left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) - \left(\sum_{i=1}^n \beta_i u_i t_i \bmod N \right) = (l_2 - l_1)N. \quad (*)$$

Considering the left-hand side of $(*)$, we have $-N < (l_2 - l_1)N < N$. Hence $l_2 - l_1 = 0$. That is $l_1 = l_2$. Having shown that the right-hand side of $(*)$ is zero. We have $(\sum_{i=1}^n \alpha_i u_i t_i \bmod N) = (\sum_{i=1}^n \beta_i u_i t_i \bmod N)$, so that by Lemma 2.5, we have $\alpha_i = \beta_i$ for $1 \leq i \leq n$. Hence each element k of Ω is uniquely identified by an $(n+1)$ -tuple $(\alpha_1, \dots, \alpha_n, l)$.

Suppose now $k = (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) + lN \in \Omega$, so that $\alpha_i \in \{0, 1, 2\}$ for $1 \leq i \leq n$. Observe that the α_i not all equal implies that $2 < (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) < N$, or equivalently that $2 < 2 + N - (\sum_{i=1}^n \alpha_i u_i t_i \bmod N) < N$. Thus if the α_i are not all equal then

$$2 + N - \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) = \left(2 + N - \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) \bmod N \right) \\ = \left(2 + N - \sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) = \left(2 \sum_{i=1}^n u_i t_i + N - \sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) \\ = \left(\sum_{i=1}^n (2 - \alpha_i) u_i t_i \bmod N \right).$$

Hence

$$\begin{aligned}
k' &= p^d - k = 2 + (p^d - 2) - k = 2 + D'N - \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) - lN \\
&= \begin{cases} 2 + N - \left(\sum_{i=1}^n \alpha_i u_i t_i \bmod N \right) + N(D' - (l + 1)) & \text{if } \alpha_i \text{ not all equal,} \\ (2 - \alpha_1) + N(D' - l) & \text{if } \alpha_i \text{ all equal;} \end{cases} \\
&= \begin{cases} \left(\sum_{i=1}^n (2 - \alpha_i) u_i t_i \bmod N \right) + N(D' - (l + 1)) & \text{if } \alpha_i \text{ not all equal,} \\ \left(\sum_{i=1}^n (2 - \alpha_i) u_i t_i \bmod N \right) + N(D' - l) & \text{if } \alpha_i \text{ all equal.} \end{cases}
\end{aligned}$$

So k' corresponds to the $(n + 1)$ -tuple

$$\begin{cases} (2 - \alpha_1, \dots, 2 - \alpha_n, D' - (l + 1)) & \text{if } \alpha_i \text{ not all equal,} \\ (2 - \alpha_1, \dots, 2 - \alpha_n, D' - l) & \text{if } \alpha_i \text{ all equal.} \end{cases}$$

Moreover, as each $\alpha_i \in \{0, 1, 2\}$, we have $(2 - \alpha_i) \in \{0, 1, 2\}$ for $1 \leq i \leq n$.

When the α_i are not all equal, we have $0 \leq l < D'$ and hence $-1 < D' - l - 1 \leq D' - 1$, so that $0 \leq D' - (l + 1) < D'$. On the other hand, when the α_i are all equal, we have $0 \leq l \leq D'$ and hence $0 \leq D' - l \leq D'$. Thus $k' \in \Omega$.

(ii) $|\Omega| = D'.3^n + 3$. By (i) elements of Ω come in pairs (k, k') one of which is less than $p^d/2$ and the other greater than $p^d/2$. Thus $|\{k \in \Omega \mid k < p^d/2\}| = \frac{D'.3^n + 3}{2}$ and hence $|\{k \in \Omega \mid 3 \leq k < p^d/2\}| = \frac{D'.3^n + 3}{2} - 3 = \frac{D'.3^n - 3}{2}$. \blacksquare

The following algorithm based on the Euclidean Algorithm shows how the t_i of Theorem 3.1 may be constructed for $n \geq 2$. For $n = 1$, as noted in the proof of Lemma 2.4 (iii), we have $u_1 = t_1 = 1$ and in fact Theorem 3.1 (ii) shows that Ω' is empty. The case $n = 0$ does not occur as the condition $d \geq 2$ of Theorem 3.1 ensures that $N > 1$.

3.2. ALGORITHM. If $N = \prod_{i=1}^n p_i^{\varepsilon_i}$, p_i prime, $\varepsilon_i > 0$, $n \geq 2$ then $t_i \in \mathbb{Z}$ satisfying $\sum_{i=1}^n u_i t_i = 1$ where $u_i = N/p_i^{\varepsilon_i}$ are found as follows.

Step 0. Define $u_i^{(m)} := \frac{\prod_{j=1}^m p_j^{\varepsilon_j}}{p_i^{\varepsilon_i}}$ for $1 \leq i \leq m \leq n$.

Recursively we construct $t_i^{(m)}$ such that $\sum_{i=1}^m u_i^{(m)} t_i^{(m)} = 1$.

Step 1. Define $u_1^{(2)} := p_2^{\varepsilon_2}$, $u_2^{(2)} := p_1^{\varepsilon_1}$.

By the Euclidean Algorithm find $t_1^{(2)}, t_2^{(2)} \in \mathbb{Z}$ such that $u_1^{(2)} t_1^{(2)} + u_2^{(2)} t_2^{(2)} = 1$.

Step $m < n$. From the previous step we have $t_i^{(m)}$ such that $\sum_{i=1}^m u_i^{(m)} t_i^{(m)} = 1$. By the Euclidean Algorithm find x, y such that $p_{m+1}^{\varepsilon_{m+1}} \cdot x + u_{m+1}^{(m+1)} \cdot y = 1$, and then

$$\text{define } t_i^{(m+1)} := \begin{cases} t_i^{(m)} \cdot x & \text{for } 1 \leq i \leq m \\ y & \text{for } i = m + 1. \end{cases}$$

Step n. After $n - 1$ steps we take $u_i := u_i^{(n)}$ and $t_i := t_i^{(n)}$.

PROOF. Steps 1 through $n - 1$ are validated by induction.

At step 1 we have $\sum_{i=1}^2 u_i^{(2)} t_i^{(2)} = 1$. By the inductive assumption from step $m - 1$ we have $\sum_{i=1}^m u_i^{(m)} t_i^{(m)} = 1$. Observe $u_i^{(m)} \cdot p_{m+1}^{\varepsilon_{m+1}} = u_i^{(m+1)}$ for $1 \leq i \leq m$, so for the m th step we have

$$\begin{aligned} 1 &= \left(\sum_{i=1}^m u_i^{(m)} t_i^{(m)} \right) p_{m+1}^{\varepsilon_{m+1}} \cdot x + u_{m+1}^{(m+1)} \cdot y = \left(\sum_{i=1}^m (u_i^{(m)} \cdot p_{m+1}^{\varepsilon_{m+1}}) (t_i^{(m)} \cdot x) \right) + u_{m+1}^{(m+1)} \cdot y \\ &= \left(\sum_{i=1}^m (u_i^{(m+1)} t_i^{(m+1)}) \right) + u_{m+1}^{(m+1)} \cdot y = \sum_{i=1}^{m+1} u_i^{(m+1)} t_i^{(m+1)} \end{aligned}$$

as required. ■

3.3. REMARK. As noted above, Theorem 3.1 (ii) shows that for $n = 1$ (that is, for $N = p_1^{\varepsilon_1}$ for some prime p_1 and $\varepsilon_1 > 0$) the set Ω' is empty. As observed by Praeger [5, p. 196] this situation occurs if, for example, $p^d - 2 = p_1^\varepsilon$ for some prime p_1 and $\varepsilon > 0$ (as then $d \geq 2$ ensures that $p^d - 2 \neq p - 2$ and thus that $1 \neq N = p_1^{\varepsilon_1}$ for some $\varepsilon_1 > 0$). In particular Praeger observed that for $p = 3$ and $d \in \{2, \dots, 6\}$ that $p^d - 2$ is a prime or the square of a prime, and thus that $\Omega' = \emptyset$, and so no non-trivial block-transitive 3-designs exist for these values of p and d .

However for $p = 3$ and $d = 7$ we have $p^d - 2 = 3^7 - 2 = 5.19.23 = N$ (as $p - 2 = 1$); so that $n = 3$ and Ω' contains $(3^3 - 3)/2 = 12$ elements. Employing Algorithm 3.2 we find that $t_1 = 33, t_2 = -132, t_3 = 8$ where $p_1 = 5, p_2 = 19, p_3 = 23$ so that $u_1 = 19.23, u_2 = 5.23, u_3 = 5.19$. Thus we have for this case

$$\begin{aligned} \Omega' &= \{k = (\alpha_1 \cdot 33(19.23) + \alpha_2 \cdot -132(5.23) + \alpha_3 \cdot 8(5.19) \bmod 5.19.23) \mid \alpha_i \in \{0, 1, 2\}, \\ &\quad \text{and } 3 \leq k < 3^7/2\} \\ &= \{115, 116, 230, 437, 552, 646, 667, 760, 761, 875, 876, 990\}. \end{aligned}$$

In the next section we show that block-transitive 3 -($3^7, k, \lambda$) designs do exist for $k = 115$ and for $k = 116$, thus answering the question posed by Praeger [5, p. 196] affirmatively. In the following example we construct the t_i mentioned above.

3.4. EXAMPLE. We now apply Algorithm 3.2 to $N = 5.19.23$. Let $p_1 = 5, p_2 = 19, p_3 = 23$. Then at step 1 we have, $u_1^{(2)} = p_2 = 19, u_2^{(2)} = p_1 = 5$ and by the Euclidean Algorithm

$$-1 \cdot 19 + 4 \cdot 5 = 1.$$

Hence, $t_1^{(2)} = -1, t_2^{(2)} = 4$. At the second and last step we find x, y such that $p_3 x + u_3^{(3)} y = 1$ where $p_3 = 23$ and $u_3^{(3)} = p_1 p_2 = 95$. By the Euclidean Algorithm

$$-33 \cdot 23 + 8 \cdot 95 = 1$$

and so $x = -33, y = 8$. Hence finally

$$\begin{aligned} 1 &= -33(-1.19 + 4.5).23 + 8(5.19) \\ &= 33(19.23) - 132(5.23) + 8(5.19). \end{aligned}$$

That is, $t_1 = 33, u_1 = 19.23, t_2 = -132, u_2 = 5.23, t_3 = 8, u_3 = 5.19$.

4. CONSTRUCTIONS

In this section we show how to construct a block B of a block-transitive 3 - $(3^7, k, \lambda)$ design admitting $G = \text{AGL}_7(3)$. We do this by first constructing a large set W with no collinear triples. Then simply by adding 4 points to W we create a set Y with a large number of collinear triples. It turns out that we have a lot of control over modifying the set Y to get a block B of a block-transitive 3 - $(3^7, k, \lambda)$ design for $k = 115$ or 116 . First we introduce some notation that will be useful in describing these blocks B .

4.1. NOTATION. Let $S \subseteq (\mathbb{Z}_p)^d$ then denote by T_S the set of collinear triples of S , that is

$$T_S = \{ \{ \mathbf{u}, \mathbf{v}, \mathbf{w} \} \mid (\mathbf{u}, \mathbf{v}, \mathbf{w}) \in S^3 \text{ and } \{ \mathbf{u}, \mathbf{v}, \mathbf{w} \} \text{ is a collinear triple} \}.$$

In particular, if $p = 3$ then

$$\begin{aligned} T_S &= \{ \{ \mathbf{u}, \mathbf{v}, \mathbf{w} \} \mid \mathbf{w} = \mathbf{u} - 1 \cdot (\mathbf{v} - \mathbf{u}), \mathbf{u} \neq \mathbf{v}, (\mathbf{u}, \mathbf{v}, \mathbf{w}) \in S^3 \} \\ &= \{ \{ \mathbf{u}, \mathbf{v}, \mathbf{w} \} \mid \mathbf{u} + \mathbf{v} + \mathbf{w} = \mathbf{0}, \mathbf{u} \neq \mathbf{v}, (\mathbf{u}, \mathbf{v}, \mathbf{w}) \in S^3 \}. \end{aligned}$$

Denote by $T_S(\mathbf{u})$, the subset of T_S consisting of collinear triples that contain \mathbf{u} , that is

$$T_S(\mathbf{u}) = \{ \{ \mathbf{u}', \mathbf{v}', \mathbf{w}' \} \in T_S \mid \mathbf{u} \in \{ \mathbf{u}', \mathbf{v}', \mathbf{w}' \} \}.$$

Let \mathbf{e}_i be the i th standard basis vector of $(\mathbb{Z}_p)^d$, that is the vector with i th coordinate 1 and all other coordinates 0.

Let W be the subset of $(\mathbb{Z}_3)^7$ consisting of vectors with no coordinate zero, that is

$$W = \left\{ \sum_{i=1}^7 \varepsilon_i \mathbf{e}_i \mid \varepsilon_i \neq 0 \right\}.$$

Where it is important to stress that a union of sets is a *disjoint* union the symbol \sqcup will be used in place of \cup .

Below we will see there are a variety of ways to construct a block B of a 3-design by modifying the set W given above. The question is: how do we tell whether two different blocks B and B' belong to non-isomorphic designs? The following lemma will assist us in finding a partial answer to this question.

4.2. LEMMA. $B^G \neq B'^G \iff (X, B^G) \not\cong (X, B'^G)$.

PROOF. Let $\mathcal{D}_i = (X, \mathcal{B}_i)$ for $i \in \{1, 2\}$ be block-transitive t -designs admitting $\text{AGL}_d(p)$. Then $G = \text{AGL}_d(p) = \text{Aut } \mathcal{D}_i = \{g \in \text{Sym}(X) \mid \mathcal{B}_i^g = \mathcal{B}_i\}$.

Suppose now $\mathcal{D}_1 \cong \mathcal{D}_2$. Then $\mathcal{D}_1^\phi = \mathcal{D}_2$ for some $\phi \in \text{Sym}(X)$, that is, $\mathcal{B}_1^\phi = \mathcal{B}_2$, and thus $G^\phi = (\text{Aut } \mathcal{D}_1)^\phi = \text{Aut } \mathcal{D}_2 = G$. So that $\phi \in \mathbf{N}_{\text{Sym}(X)}(\text{AGL}_d(p)) = \text{AGL}_d(p) = \text{Aut } \mathcal{D}_1$.

So in fact $\mathcal{B}_1^\phi = \mathcal{B}_1$. That is $\mathcal{B}_1 = \mathcal{B}_2$.

Thus for any two t -designs (X, \mathcal{B}_1) and (X, \mathcal{B}_2) either $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ or $\mathcal{B}_1 = \mathcal{B}_2$. ■

The author is grateful to Praeger for the above proof. Now for k large, checking whether $B' \in B^G$ (and hence $B^G = B'^G$) may be difficult. Thus below we define a way of dividing up a block B into classes $C_j(B)$ of points. The numbers of points in each class of B provides a signature J_B for a design (X, B^G) . We shall see that all blocks of (X, B^G) have the same number of points in each class; and moreover so do all blocks of a design isomorphic to (X, B^G) . This suggests a way of coarsely partitioning the set of all designs into divisions containing designs of the same signature. A lower bound on the number of divisions then provides a lower bound for the number of pairwise non-isomorphic designs. This motivates the following definitions.

4.3. DEFINITION. Denote by $C_j(S)$, the class of points \mathbf{u} in S , that are contained in j distinct collinear triples of S . That is, for $j \geq 0$, define

$$C_j(S) = \{\mathbf{u} \in S \mid |T_S(\mathbf{u})| = j\}.$$

Also let J_S consist of those ordered pairs $(j, |C_j(S)|)$ for which $C_j(S)$ is a non-empty subset of S . That is,

$$J_S = \{(j, |C_j(S)|) \mid \emptyset \neq C_j(S) \subseteq S\}.$$

The importance of J_S is that is invariant, under the action of $G = \text{AGL}_d(p)$. That is,

$$J_{S^g} = J_S,$$

for $g \in G$. This is because $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a collinear triple of S if and only if $\{\mathbf{u}^g, \mathbf{v}^g, \mathbf{w}^g\}$ is a collinear triple of $S^g = \{\mathbf{x}^g \mid \mathbf{x} \in S\}$. The injectivity of $g: S \rightarrow S^g$ ensures that \mathbf{u} is contained by j collinear triples of S if and only if \mathbf{u}^g is contained by j collinear triples of S^g , and also that $(j, |C_j(S)|) \in J_S$ if and only if $(j, |C_j(S^g)|) \in J_{S^g}$. Thus designs (X, B^G) and (X, B'^G) with different sets J_B and $J_{B'}$ are necessarily non-isomorphic.

The following lemma shows us that the set W can have no collinear triples.

4.4. LEMMA. Let $a, b, c \in \mathbb{Z}_3 \setminus \{0\}$. Then $a + b + c = 0 \iff a = b = c$.

PROOF. Suppose without loss of generality that $a + b + c = 0$ and $a \neq b$ then $a + b = 0$ and so $c = 0$ (contradiction). ■

4.5. COROLLARY. $T_W = \emptyset$.

PROOF. Suppose $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a collinear triple of W , then considering the i th component of each point we have $u_i + v_i + w_i = 0$ and thus by Lemma 4.4 we have $u_i = v_i = w_i$. But then $\mathbf{u} = \mathbf{v} = \mathbf{w}$, contradicting that $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a collinear triple. Thus T_W is empty. ■

Now we modify W to produce constructions of blocks for designs for $k = 115$ and $k = 116$.

4.6. CONSTRUCTION. We may construct a block B , with $|B| = k = 115$ such that for $G = \text{AGL}_7(3)$ and $X = (\mathbb{Z}_3)^7$, (X, B^G) is a block-transitive 3-design.

Let $Y = W \sqcup \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ then

- (i) Neither W nor $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ has collinear triples. That is, both the sets T_W and $T_{\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}}$ are empty. This follows immediately from Lemma 4.4.
- (ii) For each collinear triple of $W \sqcup \{\mathbf{e}_i\}$, the i th coordinate of each point is 1 (follows from Lemma 4.4), and $\mathbf{u}_j = -\mathbf{v}_j$ for $j \neq i$. That is,

$$T_{W \sqcup \{\mathbf{e}_i\}} = \left\{ \left\{ \mathbf{e}_i, \sum_{j=1}^7 \varepsilon_j \mathbf{e}_j, 2\mathbf{e}_i - \sum_{j=1}^7 \varepsilon_j \mathbf{e}_j \mid \varepsilon_j \neq 0, \varepsilon_i = 1 \right\} \right\}.$$

Thus $|T_{W \sqcup \{\mathbf{e}_i\}}| = 2^6/2 = 32$, or putting it another way $C_{32}(Y) = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$. Observe that for any point \mathbf{u} of Y , other than $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4$, that the number of collinear triples of T_Y containing \mathbf{u} is determined by how many of the first four coordinates are 1. Thus Y contains another five classes, namely

$$C_j = \left\{ \sum_{i=1}^7 \varepsilon_i \mathbf{e}_i \mid \begin{array}{l} j \text{ elements of } \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\} \text{ are } +1, \\ 4 - j \text{ elements of } \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\} \text{ are } -1, \\ \varepsilon_i \neq 0 \text{ for } 5 \leq i \leq 7 \end{array} \right\},$$

for $0 \leq j \leq 4$. So Y consists of six classes. Notice that any collinear triple of S consists of one element from $C_j(S)$, one from $C_{32}(S)$ and one from $C_{5-j}(S)$ for some j satisfying $1 \leq j \leq 4$. Also we have $|C_0| = |C_4| = 8$, $|C_1| = |C_3| = 32$, $|C_2| = 48$, and thus $J_Y = \{(0, 8), (1, 32), (2, 48), (3, 32), (4, 8), (32, 4)\}$.

- (iii) The collinear triples of Y is a union of the four disjoint sets, $T_{W \sqcup \{\mathbf{e}_i\}}$, for $1 \leq i \leq 4$.

That is, $T_Y = \bigsqcup_{i=1}^4 T_{W \sqcup \{\mathbf{e}_i\}}$ and $|T_Y| = 4 \cdot 32 = 128$.

- (iv) $|Y| = |W| + 4 = 2^7 + 4 = 132$.

The idea now is to modify the set Y to get a block B of a 3-design. To get a block B with $|B| = k = 115$ we need $|T_B| = q_1(k) = 113$. Such a block B can be obtained from the set Y (which has $|Y| = 132$ points and $|T_Y| = 128$ collinear triples) by deleting 17 points from Y in such a way as to reduce the number of collinear triples by 15. This can be done, for example, if we find a solution of

$$\sum_{j=0}^4 n_j = 17, \quad \sum_{j=0}^4 j \cdot n_j = 15 \tag{†}$$

where n_j is the number of points in class $C_j(Y)$ to be deleted (assuming that no two points of the 17 points are elements of a common collinear triple – this turns out to be easily arranged). Each line of the following table is a solution of (†) subject to $0 \leq n_j \leq |C_j(Y)|$.

n_0	n_1	n_2	n_3	n_4	n_0	n_1	n_2	n_3	n_4	n_0	n_1	n_2	n_3	n_4
8	7	0	0	2	8	5	2	2	0	8	3	6	0	0
8	6	1	1	1	7	7	1	2	0	7	5	5	0	0
7	8	0	1	1	6	9	0	2	0	6	7	4	0	0
8	5	3	0	1	8	4	4	1	0	5	9	3	0	0
7	7	2	0	1	7	6	3	1	0	4	11	2	0	0
6	9	1	0	1	6	8	2	1	0	3	13	1	0	0
5	11	0	0	1	5	10	1	1	0	2	15	0	0	0
8	6	0	3	0	4	12	0	1	0					

Each of these 23 possibilities lead to design constructions. Consider, for example $n_0 = 8$, $n_1 = 7$, $n_2 = n_3 = 0$, $n_4 = 2$. Each point in $C_4(Y)$ lies in 4 collinear triples of Y – the other two points of each collinear triple being a point of $C_{32}(Y) = \{e_1, e_2, e_3, e_4\}$ together with a point from $C_1(Y)$. Thus after selecting 2 points \mathbf{x}, \mathbf{y} from $C_4(Y)$ we avoid 8 of the 32 points of $C_1(Y)$, namely those \mathbf{w} that satisfy $\mathbf{u} + \mathbf{v} + \mathbf{w} = \mathbf{0}$ where $\mathbf{u} \in \{\mathbf{x}, \mathbf{y}\}$ and $\mathbf{v} \in \{e_1, e_2, e_3, e_4\}$. This gives $\binom{8}{2} \cdot \binom{24}{7} \cdot \binom{8}{8}$ ways of obtaining a block B with the desired characteristics using this solution of (†). Of course, the 8 points of $C_1(Y)$ that were avoided above no longer belong to a collinear triple of the set $Y \setminus \{\mathbf{x}, \mathbf{y}\}$ – so one can delete any of these 8 points instead of the points of $C_0(Y)$ to obtain the block B . That is $|C_0(Y \setminus \{\mathbf{x}, \mathbf{y}\})| = 16$ and so the above number of ways can be multiplied by a factor of $\binom{16}{8}$.

Now we consider the question as to how many of the designs constructed in this fashion are pairwise non-isomorphic. Certainly, (X, B^G) and (X, B'^G) are non-isomorphic if $J_B \neq J_{B'}$. For example blocks B and B' , defined below are generated in the manner mentioned above, from the first line of the table.

$$\begin{aligned}
 B = Y \setminus \{ & (1, 1, 1, 1, -1, -1, -1), (1, 1, 1, 1, -1, -1, 1), \\
 & (1, -1, -1, -1, -1, -1, -1), (-1, 1, -1, -1, -1, -1, -1), \\
 & (-1, -1, 1, -1, -1, -1, -1), (-1, -1, -1, 1, -1, -1, -1), \\
 & (1, -1, -1, -1, -1, -1, 1), (-1, 1, -1, -1, -1, -1, 1), \\
 & (-1, -1, 1, -1, -1, -1, 1), (-1, -1, -1, -1, \varepsilon_5, \varepsilon_6, \varepsilon_7) \mid \varepsilon_i \neq 0 \text{ for } 5 \leq i \leq 7\},
 \end{aligned}$$

$$B' = (B \cup \{(-1, -1, 1, -1, -1, -1, 1)\}) \setminus \{(-1, -1, 1, -1, -1, 1, 1)\}.$$

They differ in that the ninth point deleted from Y (a point of $C_1(Y)$) is the point $(-1, -1, 1, -1, -1, -1, 1)$ for B , and $(-1, -1, 1, -1, -1, 1, 1)$ for B' . Checking we find that

$$J_B = \{(0, 9), (1, 18), (2, 48), (3, 32), (4, 4), (28, 3), (29, 1)\},$$

$$J_{B'} = \{(0, 9), (1, 17), (2, 49), (3, 33), (4, 3), (28, 3), (29, 1)\}.$$

So, in fact (X, B^G) and (X, B'^G) are non-isomorphic. In this way, each line of the table may give rise to several pairwise non-isomorphic designs. Note that as points are deleted from Y the point classes change (for example, suppose $\mathbf{x} \in C_j(Y)$ then j points of $C_{5-j}(Y)$ move into $C_{5-j-1}(Y \setminus \{\mathbf{x}\})$, and all other points of $Y \setminus \{\mathbf{x}\}$ remain in their previous class). An example of this was given above. With this in mind we may relax the restriction $n_j \leq |C_j(Y)|$. This opens up a further 21 possibilities for (n_0, \dots, n_4) – all of which are feasible. Considering, these possibilities as well as those already mentioned a preliminary computer investigation turned up 37 isomorphically distinct block-transitive 3 - $(3^7, 115, \lambda)$ designs.

4.7. CONSTRUCTION. In a similar way to the previous construction we may construct a block B , with $|B| = k = 116$ such that for $G = \text{AGL}_7(3)$ and $X = (\mathbb{Z}_3)^7$, (X, B^G) is a block-transitive 3-design. This time we need $|T_B| = q_1(k) = 116$. Thus from the set Y (which has $|Y| = 132$ points and $|T_Y| = 128$ collinear triples) we must delete 12 points in such a way as to reduce the number of collinear triples by 16. This can be done, for example, if we find a solution of

$$\sum_{j=0}^4 n_j = 16, \quad \sum_{j=0}^4 j \cdot n_j = 12. \quad (\ddagger)$$

Each line of the following table is a solution of (\ddagger) subject to $0 \leq n_j \leq |C_j|$.

n_0	n_1	n_2	n_3	n_4	n_0	n_1	n_2	n_3	n_4	n_0	n_1	n_2	n_3	n_4
8	6	1	0	1	7	7	1	1	0	6	8	2	0	0
7	8	0	0	1	6	9	0	1	0	5	10	1	0	0
8	6	0	2	0	8	4	4	0	0	4	12	0	0	0
8	5	2	1	0	7	6	3	0	0					

From these 11 possibilities take $n_0 = 8$, $n_1 = 6$, $n_2 = 1$, $n_3 = 0$, $n_4 = 1$. One solution generated from this solution of (\ddagger) is the following.

$$B = Y \setminus \{(1, 1, 1, 1, -1, -1, -1), (1, 1, -1, -1, -1, -1, -1), \\ (1, -1, -1, -1, -1, -1, -1), (-1, 1, -1, -1, -1, -1, -1), \\ (-1, -1, 1, -1, -1, -1, -1), (-1, -1, -1, 1, -1, -1, -1), \\ (1, -1, -1, -1, -1, -1, 1), (-1, 1, -1, -1, -1, -1, 1), \\ (-1, -1, -1, -1, \varepsilon_5, \varepsilon_6, \varepsilon_7) \mid \varepsilon_i \neq 0 \text{ for } 5 \leq i \leq 7\}.$$

Relaxing the restriction that $n_j \leq |C_j(Y)|$ yields 21 more possibilities for (n_0, \dots, n_4) . However, 4 of these appear to be infeasible. A preliminary computer investigation found the number of pairwise non-isomorphic block-transitive 3 - $(3^7, 116, \lambda)$ designs to be at least 34.

The usefulness of our set W finishes with these two constructions. It was not at all obvious how to generalise the above ideas. Thus we finish with the following questions.

4.8. QUESTION. *What constructions are possible for blocks B for which (X, B^G) is a 3-design admitting $\text{AGL}_7(3)$ and $|B| = k \in \{230, 437, 552, 646, 667, 760, 761, 875, 876, 990\}$?*

4.9. QUESTION. *Can the above techniques be applied in the construction of 3-designs for other values of (p, d, k) ?*

REFERENCES

- [1] ALLTOP, W. O. : Some 3-designs and a 4-design. *J. Algebra (2)* **11** (1971), 190–195
- [2] BLOCK, R. E. : On the orbits of collineation groups. *Math. Zeit* **96** (1967), 33–49
- [3] CAMERON, P. J. and PRAEGER, C. E. : Block-transitive t designs. I: point-imprimitive designs. *Discrete Math.* **118** (1993), 33–43
- [4] HUGHES, D. R. and PIPER, F. C. : *Design Theory* (Cambridge University Press, 1985)
- [5] PRAEGER, C. E. : Block-transitive designs and maximal subgroups of finite symmetric groups. *Australas. J. Combinatorics* **1** (1990), 193–205
- [6] PRAEGER, C. E. : *private communication* (1990)

Greg Gamble
 Department of Mathematics
 University of Western Australia
 Nedlands WA 6009
 Australia