On Small Congruence Covers

Dieter Jungnickel

Abstract

This note provides a group theoretic characterisation of small line covers of $PG(3,p)$ and, more generally, small congruence covers of $PG(2t+1,p)$. It is shown that any group of square order s^2 which admits a cover by at most $s+p-1$ subgroups of order s (where p is the smallest prime divisor of s) is necessarily elementary abelian; hence any such cover is in fact geometric, that is, a congruence cover of a suitable projective geometry. We also show that the preceding bound is essentially best possible: There exists a congruence cover with $s+p+1$ components in a suitable non-elementary abelian group whenever s is a proper power of a prime.

1 Introduction

Packing finite projective spaces with disjoint subspaces has for many years been a topic of considerable interest in Galois geometries. In particular, one studies *partial t-spreads*, that is, collections of pairwise disjoint t-dimensional subspaces in a space $PG(d,q)$. In spite of considerable effort, the fundamental question of determining the maximal size of a partial t-spread is still not settled in general; see Hirschfeld and Thas [12] for background. In contrast, the dual problem of *t-covers*, that is, minimal collections of t-dimensional subspaces covering $PG(d,q)$ is much better understood. The following result is due to Beutelspacher [3] (who determined the lower bound) and Eisfeld [7] (who gave the structural characterisation for the case of equality).

Result 1.1. *Let $\mathcal{C}$ be a t-cover of $PG(d,q)$, and write $d = a(t+1)+b$, where $0 \leq b \leq t$. Then*

$$|\mathcal{C}| \;\geq\; q^{b+1}(q^{(a-1)(t+1)} + \ldots + q^{2(t+1)} + q^{t+1} + 1) + 1,$$

Received by the editors January 1998.
Communicated by J. Thas.

and a t-cover of this size always exists. Moreover, in the case of equality, there exists a subspace U of dimension $t-b-1$ such that:

- *Each point not in U is in exactly one component of $\mathcal{C}$.*
- *Each point of U is in exactly $q^{b+1}+1$ components of $\mathcal{C}$.*

(Note that the subspace U is empty if $b=t$; thus $\mathcal{C}$ is a t-spread in this case.) ∎

The special cases that have generated most interest are those of *maximal partial spreads*, that is, maximal collections of pairwise skew lines of a 3-dimensional space $PG(3,q)$, and, dually, *minimal line covers*, that is, minimal collections of lines covering $PG(3,q)$. We refer the reader to Hirschfeld [11] for background on maximal partial spreads. Small minimal covers have been studied in the recent work of Blokhuis et. al. [5], and large minimal covers were considered by Bruen and Drudge [6]. A *proper* maximal partial spread $\mathcal{S}$ (that is, one that is not simultaneously a line cover and hence a *spread*, consisting of exactly q^2+1 lines) necessarily has a rather large *deficiency* d:

$$|\mathcal{S}| \;\leq\; q^2+1-d,$$

where the precise value of the smallest possible d is still not known, in spite of much effort. Certainly $d \geq \sqrt{2q}$ by a result of Blokhuis and Metsch [4]; see Metsch and Storme [17] for important recent progress. Again, the situation is quite different for minimal line covers: They may have *excess* e (that is, cardinality $|\mathcal{S}| = q^2+1+e$) for arbitrarily small values of e, as the following result of [5] shows.

Result 1.2. *In $PG(3,q)$, there exist minimal line covers with excess e for all e with $0 \leq e \leq q$.* ∎

By interpreting a partial t-spread in $PG(2t+1,q)$ as a collection of $(t+1)$-dimensional subspaces of the vector space $V(2t+2,q)$, one obtains a special type of *partial congruence partition* (*PCP*). In general, a *PCP* with parameters (s,r) is a collection of *pairwise disjoint* subgroups $U_1,\ldots,U_r$ of order s of a group G of order s^2, that is

$$U_i \cap U_j = \{1\} \quad \text{or, equivalently,} \quad U_iU_j = G,$$

whenever $i \neq j$ (we write groups multiplicatively and denote the unit element by 1). The importance of this concept is due to the fact that *PCP*'s are equivalent to "translation nets", see Jungnickel [13] or [2] for background. The geometric examples just discussed show that the elementary abelian groups $EA(s^2)$ always admit a *PCP* with $r = s+1$; it is well known that these *congruence partitions* in the sense of André [1] describe translation planes. By a result of [14], a *PCP* in a non- elementary abelian group necessarily has a comparatively large *deficiency* d:

Result 1.3. *Let $\mathcal{U}$ be a PCP with deficiency $d \leq \sqrt{s}+1$ in a group G of order s^2, where $s \neq 2,4$. Then G is necessarily an elementary abelian group.* ∎

In other words, *PCP*'s with small deficiency are *geometric*, that is, they belong to a partial t-spread in a suitable projective space $PG(2t+1,p)$. The aim of the present note is an analogous result for covers; to this end, we introduce the notion

of a *congruence cover* of *excess* e of a group G of square order s^2: This is a collection of subgroups $U_1, \ldots, U_r$ of order s the union of which is all of G, where $r = s+1+e$. We shall prove the following result which shows that congruence covers with small excess are likewise *geometric*, that is, they belong to a t-cover of a suitable projective space $PG(2t+1, p)$.

Theorem 1.4. *Any group of square order s^2 which admits a congruence cover of excess at most $p-2$, where p is the smallest prime divisor of s, is necessarily elementary abelian.*

The preceding theorem proves that small congruence covers are necessarily geometric. We emphasise that one cannot expect a group theoretic characterisation of this type for small line covers of $PG(3, q)$, unless q is a prime: Given any line cover $\mathcal{C}$ of $PG(3, q)$, where q is a proper power of a prime, say $q = p^m$ with $m \geq 2$, it is possible to construct a congruence cover of the same excess which is not a line cover. It suffices to view the lines of $PG(3, q)$ as $(2m-1)$-dimensional subspaces of $\Pi = PG(4m-1, p)$ and to apply a collineation of Π to $\mathcal{C}$ which moves some component U into a $(2m-1)$-dimensional subspace of Π that does not correspond to a line of $\mathcal{C}$.

The proof of Theorem 1.4 will proceed via a reduction to known bounds on the size of *PCP*'s. We will also show that the bound given there is essentially best possible; indeed, we will exhibit a congruence cover of excess p in a suitable non-elementary abelian group whenever s is a proper prime power. We also briefly address the general problem of covering a group by subgroups of a specified order, since we will require some information about this for constructing the examples just mentioned. A more detailed study of this interesting general problem will be postponed to a forthcoming paper [16].

2 Covering groups by subgroups

In this section, we collect some basic results concerning the general problem of covering a given group by subgroups of specified order. We begin with the following simple observation on the existence of such a cover.

Proposition 2.1. *Let G be a group of order v, and let s be a divisor of v. If G can be covered by subgroups of order s, then* $\exp G$ *divides s. Moreover, this necessary condition is also sufficient if G is nilpotent.*

Proof. The condition stated above is obviously necessary, as an element of an order not dividing s cannot be contained in a subgroup of order s. Conversely, assume that this condition is satisfied; hence every element $g \in G$ generates a subgroup H_g of some order dividing s. If G is a p-group, then H_g lies in a subgroup U_g of order s, by elementary results on p-groups, see e.g. Hall [10]. Then the U_g form the desired cover of G. Note that this argument carries over to arbitrary nilpotent groups, as these are the direct products of their Sylow p-subgroups. ∎

We note that Proposition 2.1 does not hold for arbitrary groups. To mention a trivial example, the symmetric group S_n cannot be covered by subgroups of order

$(n!)/2$. It would be an interesting (though probably difficult) problem to characterise all groups G which admit covers by subgroups of all orders s divisible by $\exp G$, provided that at least one such subgroup exists.

Given a group G which admits a cover by subgroups of order s, we will denote the smallest cardinality of such a cover by $c(G, s)$. In this notation, the smallest size of a congruence cover of a group G of square order is $c(G, \sqrt{|G|})$. In the present note, we will not address the general problem of determining the *covering numbers* $c(G, s)$; this will be the subject of a forthcoming paper [16]. Let us just note that Result 1.1 solves this problem for the class of elementary abelian groups. As we will require this as an auxiliary tool later, we shall now give the translation of Result 1.1 into the notation just introduced.

Theorem 2.2. *Let G be the elementary abelian group $EA(p^d)$ of order p^d, and write $d = at + b$, where $1 \leq b \leq t$. Then*

$$c(G, p^t) \;=\; p^b(p^{(a-1)t} + \ldots + p^{2t} + p^t + 1) + 1. \tag{1}$$

Moreover, if $\mathcal{C}$ is a cover of G by $c(G, p^t)$ subgroups of order p^t, then there exists a subgroup U of order p^{t-b} such that:

- *Each element not in U is in exactly one component of $\mathcal{C}$.*
- *Each element $\neq 1$ of U is in exactly $p^b + 1$ components of $\mathcal{C}$.* ∎

3 General lower bounds for congruence covers

Let G be a group of order s^2, and let $\mathcal{C}$ be a congruence cover of G with excess e. Given any $g \in G$ with $g \neq 1$, the *multiplicity* μ_g of g is defined as the number of components of $\mathcal{C}$ containing g. Moreover, $\sigma_g := \mu_g - 1$ is called the *surplus* of g, and the quantity

$$\sigma(\mathcal{C}) \;:=\; \sum_{g \in G \setminus \{1\}} \sigma_g$$

is the *total surplus* of $\mathcal{C}$. Trivially,

$$\sigma(\mathcal{C}) \;=\; e(s-1). \tag{2}$$

Now assume $\sigma(C) \neq 0$. We then select any element $g \in G$ with positive surplus and remove some component U of $\mathcal{C}$ containing g, so that the surplus of g is reduced by 1 in the resulting collection $\mathcal{C}' := \mathcal{C} \setminus \{U\}$ of subgroups of order s. (We may use the notion of surplus not only for congruence covers but for arbitrary collections of subgroups of order s, as long as we apply it only to elements covered by some component.) Note that every element $h \neq 1$ in the subgroup $\langle g \rangle$ generated by g also has positive surplus $\sigma_h \geq \sigma_g$ in $\mathcal{C}$, and that its surplus has likewise been reduced by 1 in $\mathcal{C}'$. As $\langle g \rangle$ has order at least p, where p is the smallest prime divisor of s, the total surplus of $\mathcal{C}'$ satisfies

$$\sigma(C') \;\leq\; \sigma(\mathcal{C}) - (p-1).$$

By continuing in the same manner, we will eventually reduce the surplus of every $g \in G$ to 0 and hence produce a *PCP* in G; in view of equation (2), this process requires removing at most $e(s-1)/(p-1)$ components of $\mathcal{C}$. If we denote the maximum size of a *PCP* in G by $\pi(G)$, we obtain the inequality

$$s + 1 + e - \frac{e(s-1)}{p-1} \;\leq\; \pi(G).$$

Rearranging terms gives the following useful result.

Lemma 3.1. *Let G be a group of square order s^2 which admits a congruence cover of excess e, let p be the smallest prime divisor of s, and denote the maximum size of a PCP in G by $\pi(G)$. Then*

$$e \;\geq\; \frac{(p-1)(s+1-\pi(G))}{s-p}. \qquad \blacksquare$$

In order to apply the preceding Lemma, we require the following bounds on $\pi(G)$ due to the author [13, 15]. (There are stronger, considerably more involved bounds due to Hachenberger [8, 9]; however, in conjunction with Lemma 3.1, these bounds do not lead to stronger results on congruence covers.)

Result 3.2. *Let G be a group of square order s^2 which is not elementary abelian. Then the following bounds on the maximum size $\pi(G)$ of a PCP in G hold:*

1. *If s is a prime power, say $s = p^d$, then $\pi(G) \;\leq\; p^{d-1} + \ldots + p^2 + p + 1$.*
2. *If s is not a prime power, say $s = q_1 \ldots q_n$, where the q_i are powers of pairwise distinct primes p_i, then*

$$\pi(G) \;\leq\; \min\{\pi(S_i)\colon\, i = 1, \ldots, n\} \;\leq\; \min\{q_i + 1\colon\, i = 1, \ldots, n\},$$

where S_i denotes a Sylow p_i-subgroup of G. $\blacksquare$

We can now prove the following restatement of Theorem 1.4:

Theorem 3.3. *Let G be a group of square order s^2 which is not elementary abelian, and let $\mathcal{C}$ be any congruence cover of G. Then $\mathcal{C}$ has excess $e \geq p-1$, where p is the smallest prime divisor of s.*

Proof. First assume that s is a prime power, say $s = p^d$. By Lemma 3.1 and Result 3.2, we obtain

$$e \;\geq\; \frac{(p-1)(p^d+1) - (p^d-1)}{p^d - p} \;=\; \frac{p^d - 2p^{d-1} + 1}{p^{d-1} - 1}.$$

This gives $e \geq p-1$, as e is an integer. Now let $s = q_1 \ldots q_n$, where $n \geq 2$ and where the q_i are powers of pairwise distinct primes p_i. Put $q := \min\{q_i\colon\, i = 1, \ldots, n\}$, and write $q = p^d$. Again using Lemma 3.1 and Result 3.2, we obtain

$$e \;\geq\; \frac{(p-1)(s-p^d)}{s-p} \;=\; \frac{sp - s - p^{d+1} + p^d}{s-p} \;>\; \frac{sp - 2s - p^2 + 2p}{s-p} \;=\; p-2,$$

as $s \geq qq' > p^{d+1} > p^{d+1} - p^d - p^2 + 2p$, where q' is a term $\neq q$ in the prime power factorisation of s. Again,this implies $e \geq p-1$. $\blacksquare$

In Section 4, we will show that the bound of Theorem 3.3 is essentially best possible for p-groups. However, in the general case, this bound is probably not all that strong. We now give a stronger bound for the particularly important special case of nilpotent groups; again, we will show that this bound is best possible in Section 4.

Theorem 3.4. *Let $\mathcal{C}$ be a congruence cover of a group G of square order s^2, where $s = q_1 \dots q_n$ with $n \geq 2$ and where the q_i are powers of pairwise distinct primes p_i. If G is nilpotent, then*

$$|\mathcal{C}| \;\geq\; (q_1 + 1) \dots (q_n + 1).$$

Proof. For $i = 1, \dots, n$, let S_i denote the Sylow p_i-subgroup of G, so that $G = S_1 \times \dots \times S_n$. Note that each component of $\mathcal{C}$ is of the form $U = U_1 \times \dots \times U_n$, where U_i is a subgroup of S_i of order q_i (for $i = 1, \dots, n$). Hence each component of $\mathcal{C}$ contains exactly $(q_1 - 1) \dots (q_n - 1)$ elements of the form $g = (g_1, \dots, g_n)$ with $g_i \neq 1$ for all i; as there are altogether $(q_1^2 - 1) \dots (q_n^2 - 1)$ such elements, we obtain the assertion. ∎

4 Some examples of small congruence covers

In this section, we will provide some constructions for congruence covers with moderate excess. We will also determine the exact cardinality $\kappa(G)$ of a smallest congruence cover for some abelian groups G of square order. As our examples will indicate, solving this problem for arbitrary nilpotent groups seems to be difficult, even in the special case of abelian p-groups. Anyway, our examples will at least demonstrate that the bounds given in the preceding section are essentially best possible. The following simple construction shows this to be true for the bound of Theorem 3.4.

Proposition 4.1. *Let $G := EA(q_1^2) \times \dots \times EA(q_n^2)$, where $n \geq 2$ and where the q_i are powers of pairwise distinct primes p_i. Then*

$$\kappa(G) \;=\; (q_1 + 1) \dots (q_n + 1).$$

Proof. In view of Theorem 3.4, it suffices to construct a congruence cover of G of cardinality $(q_1 + 1) \dots (q_n + 1)$. Now each factor $EA(q_i^2)$ has a congruence cover $\mathcal{C}_i$ of cardinality $q_i + 1$. Then the set of all subgroups of G of the form

$$U = U_1 \times \dots \times U_n \quad \text{with} \quad U_i \in \mathcal{C}_i$$

is the desired congruence cover of G. ∎

It seems likely that equality in Theorem 3.4 is realised only by the group G considered in Proposition 4.1, but we have at present no proof for this assertion.

Proposition 4.2. *Let $G := \mathbb{Z}_{p^d} \times \mathbb{Z}_{p^d}$, where p is a prime. Then $\kappa(G) = p^d + p^{d-1}$.*

Proof. Trivially, any element g of order p^d is in a unique subgroup of this order, which therefore has to be included in any congruence cover $\mathcal{C}$ of G. Hence

$$\kappa(G) \;\geq\; \frac{p^{2d} - p^{2d-2}}{p^d - p^{d-1}} \;=\; p^d + p^{d-1}.$$

On the other hand, it is easily seen that the $p^d + p^{d-1}$ cyclic subgroups of order p^d of G cover all of G. ∎

The case $d = 2$ of Proposition 4.2 shows that the bound given in Theorem 3.3 can be sharp, even though it supplies only a single example for this phenomenon. The next result proves that the bound in question is essentially best possible for all prime powers s: It can be off by at most 1.

Proposition 4.3. *Let $G := \mathbb{Z}_{p^2} \times \mathbb{Z}_p^{2d-2}$, where p is a prime. Then $\kappa(G) = p^d + p + 1$.*

Proof. Write $G = H \times K$, where $H \cong \mathbb{Z}_{p^2}$. Note that we need at least

$$\frac{p^{2d} - p^{2d-1}}{p^d - p^{d-1}} \;=\; p^d$$

subgroups with order p^d and exponent p^2 to cover the elements of order p^2 of G, and that any two such subgroups intersect in the cyclic subgroup P of order p of H. Hence p^d such subgroups cover at most $p^d(p^{d-1} - p) + p - 1$ distinct elements of order p. This leaves at least $p^{d+1} - p$ elements of order p not yet covered; combinatorially, it might just be possible to cover these elements by p further subgroups of order p^d. We show now that this case is in fact impossible for structural reasons. Otherwise, we could select any two of these further subgroups, say U and V. Since U and V would have to be disjoint and consist of elements of order p only, we would obtain $G = U \times V \cong EA(p^{2d})$, a contradiction. Hence indeed $\kappa(G) \geq p^d + p + 1$.

We shall now construct a congruence cover of G of cardinality $p^d + p + 1$. Note that G has an elementary abelian factor group $\bar{G}$ of order p^{2d-1}; by Theorem 2.2, $\bar{G}$ admits a cover $\bar{\mathcal{C}}$ with $p^d + p + 1$ subgroups of order p^{d-1}. It is easily checked that the pre-image of $\bar{\mathcal{C}}$ under the natural epimorphism from G onto $\bar{G}$ is the desired congruence cover $\mathcal{C}$ of G. ∎

The construction given in the proof of Proposition 4.3 works because of the large elementary abelian factor of G, that is, because of the small Frattini subgroup $\Phi(G)$ of G. (Recall that $\Phi(G)$ is the smallest normal subgroup of G for which $G/\Phi(G)$ is elementary abelian, see e.g. Hall [10].) This observation allows us to prove the following general existence result.

Theorem 4.4. *Let G be a group of order s^2, where $s = p^d$ for some prime p. Assume that G is not elementary abelian, and write $|\Phi(G)| = p^f$. If $f \leq d/2$, then*

$$\kappa(G) \;\leq\; p^d + p^f + 1.$$

Proof. Put $\bar{G} := G/\Phi(G)$, so that $\bar{G} \cong EA(p^{2d-f})$. Note $2d - f = 2(d - f) + f$ and $1 \leq f \leq d - f$. By Theorem 2.2, $\bar{G}$ admits a cover $\bar{\mathcal{C}}$ by subgroups of order p^{d-f} with cardinality $|\bar{\mathcal{C}}| = p^f(p^{d-f} + 1) + 1$. Hence one obtains the desired congruence cover $\mathcal{C}$ of G as the pre-image of $\bar{\mathcal{C}}$ under the natural epimorphism from G onto $\bar{G}$. ∎

Of course, a similar construction is also possible if the size of the Frattini subgroup is larger than $\sqrt{s}$. The argument is slightly more involved than in the proof of Theorem 4.4, since it depends on the relation between f and $d - f$. In any case, the construction yields congruence covers with an excess in the order of magnitude of p^f. The precise result is as follows:

Theorem 4.5. *Let G be a group of order s^2, where $s = p^d$, p a prime, which is not elementary abelian, and assume $|\Phi(G)| = p^f$, where $f < d$. Write $2d - f = a(d-f) + b$, where $1 \leq b \leq d - f$. Then*

$$\begin{aligned} \kappa(G) &\leq p^b(p^{(a-1)(d-f)} + \ldots + p^{2(d-f)} + p^{d-f} + 1) + 1 \\ &= p^d + p^f + p^{2f-d} + \ldots + p^{b+d-f} + 1. \end{aligned}$$

■

5 Conclusion

In this note, we have characterised the elementary abelian groups of square order by the existence of small congruence covers. In other words, sufficiently small congruence covers are necessarily geometric. We have also demonstrated that our bounds are essentially best possible. Similar results for the general problem of covering a given group by subgroups of specified order will be discussed in a forthcoming paper [16].

The bounds and constructions presented in the present note suggest some questions. In particular, we mention the following open problems:

1. Does the bound of Theorem 3.4 carry over to arbitrary (or at least to solvable) groups?

2. Can Theorem 3.4 be strengthened to give the following bound for nilpotent groups:
$$\kappa(G) \geq \prod_{i=1}^{n} \kappa(S_i),$$
where S_i denotes the Sylow p_i-subgroup of G? Should the answer to this question be positive, the construction presented in the proof of Proposition 4.1 would reduce the determination of $\kappa(G)$ for nilpotent groups to the same problem for p-groups.

3. Let G be a p-group of square order. Our examples indicate that $\kappa(G)$ should depend on the exponent of G and on the order of the Frattini subgroup $\Phi(G)$. Are the constructions given in Theorems 4.4 and 4.5 essentially best possible?

4. What is the precise value of $\kappa(G)$ for abelian groups G?

Acknowledgement. The author thanks the referee for pointing out a mistake in his original proof of Proposition 4.3; thanks also to M.J. de Resmini and Andreas Enge for some helpful comments.

References

[1] J. André: Über nichtdesarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* **60** (1954), 156–186.

[2] T. Beth, D. Jungnickel and H. Lenz: *Design Theory (2nd edition)*. Cambridge University Press (1998).

[3] A. Beutelspacher: On t-covers in finite projective spaces. *J. Geom.* **12** (1979), 10–16.

[4] A. Blokhuis and K. Metsch: On the size of a maximal partial spread. *Designs, Codes and Cryptography* **3** (1991), 187–191.

[5] A. Blokhuis, C.M. O'Keefe, S.E. Payne, L. Storme and H. Wilbrink: Covers of $PG(3, q)$ and of finite generalized quadrangles. *Simon Stevin*, to appear.

[6] A.A. Bruen and K. Drudge: Large minimal covers of $PG(3, q)$. Manuscript

[7] J. Eisfeld: On smallest covers of finite projective spaces. *Archiv Math.* **68** (1997), 77–80.

[8] D. Hachenberger: On the existence of translation nets. *J. Algebra* **152** (1992), 207–229.

[9] D. Hachenberger: On a combinatorial problem in group theory. *J. Comb. Th. (A)* **64** (1992), 79–101.

[10] M. Hall, Jr.: *The theory of groups*. MacMillan, New York (1959).

[11] J.W.P. Hirschfeld: *Finite Projective Spaces of Three Dimensions*. Oxford University Press (1985).

[12] J.W.P. Hirschfeld and J.A. Thas: *General Galois Geometries*. Oxford University Press (1991).

[13] D. Jungnickel: Existence results for translation nets. In: *Finite geometries and designs* (Eds. P.J. Cameron, J.W.P. Hirschfeld and D.R. Hughes). Cambridge University Press (1981), pp. 172–196.

[14] D. Jungnickel: Maximal partial spreads and translation nets of small deficiency. *J. Algebra* **90** (1984), 119–132.

[15] D. Jungnickel: Existence results for translation nets II. *J. Algebra* **122** (1989), 288–298.

[16] D. Jungnickel and L. Storme: Packing and covering groups with subgroups. In preparation.

[17] K. Metsch and L. Storme: Partial spreads in $PG(3, q)$, q square. Manuscript.

Lehrstuhl für Diskrete Mathematik, Optimierung
und Operations Research
Universität Augsburg
D–86135 Augsburg, Germany