Partial Spreads Over $\mathbb{Z}_q$

Dieter Jungnickel
Mathematisches Institut
Justus-Liebig-Universität Gießen
Arndtstraße 2
D-6300 Gießen, Federal Republic of Germany

Dedicated to Alan J. Hoffman on the occasion of his 65th birthday.

Submitted by Alexander Schrijver

ABSTRACT

Let p be a prime, $q = p^a$, and $G = \mathbb{Z}_q^{2n}$. We consider partial spreads in G, i.e. collections of pairwise disjoint subgroups of order q^n. It is shown that the maximum size of such a collection is exactly $p^n + 1$. The method of proof consists in representing partial spreads in G by invertible $n \times n$ matrices over $\mathbb{Z}_q$ and in finding a close relation to (ordinary) partial spreads over $\mathbb{Z}_p$. Geometrically, partial spreads over $\mathbb{Z}_q$ correspond to homogeneous translation nets.

1. INTRODUCTION

Let G be a group of order s^2 (written additively), and let $U_1, \ldots, U_r$ be subgroups of order s of G. One calls $\mathbf{U} = \{U_1, \ldots, U_r\}$ a *partial congruence partition* of *degree* r and *order* s [for short, an (s, r)-pcp] provided that the U_i are *pairwise disjoint*, i.e.

$$U_i \cap U_j = \{0\} \qquad (\text{equivalently,} \quad U_i + U_j = G) \tag{1}$$

for $i \neq j$. We call the U_i the *components* of $\mathbf{U}$. A pcp $\mathbf{U}$ is said to be *maximal* if no further component may be added. To avoid trivialities, we shall always assume that $r \geqslant 3$.

 0024-3795/89/$3.50

The best-known examples of pcp's arise in elementary abelian groups: If G is $\mathbb{Z}_p^{2n}$, a pcp is the same as a *partial spread* in G [to be precise, a partial $(n-1)$-spread]. Partial spreads have been studied extensively; see e.g. Beutelspacher [3], Bruen [7], Hirschfeld [12], Jungnickel [14], and the literature cited there. The case of pcp's in general groups has been considered by Sprague [17], Jungnickel [13, 15], and Frohardt [11].

It should be noted that pcp's admit an interesting geometric interpretation. Let $\mathbf{U}$ be an (s,r)-pcp in G, and define an incidence structure $\mathbf{D} = \mathbf{D}(\mathbf{U})$ as follows:

$$\mathbf{D} = (G, \{U_i + x : x \in G,\ i = 1, \ldots, r\}, \in).$$

Then $\mathbf{D}$ is a *Bruck net* of *order* s and *degree* r. (See Bruck [4] and Beth, Jungnickel, and Lenz [2] for details on nets.) In other words, $\mathbf{D}$ consists of s^2 *points* (the elements of G) and rs *lines* (the cosets $U_i + x$) which are partitioned into r *parallel classes* of s lines each (the cosets of the r subgroups U_i); each parallel class partitions the point set, and any two nonparallel lines intersect in precisely one point. Moreover, $\mathbf{D}(\mathbf{U})$ is in fact a *translation net* with *translation group* G: G acts as a point-regular collineation group of $\mathbf{D}$ fixing each parallel class (by right translation). It is easy to see that each translation net may be represented in this way (see e.g. [2, X.9.4] or [17]). Thus the geometric problem of studying translation nets is equivalent to the combinatorial problem of studying groups with pcp's.

Again, the best-known examples of translation nets are those corresponding to partial spreads. This goes back to André [1], who used spreads (i.e. partial spreads where the union of the components covers all of G) to represent affine translation planes; see also Bruck and Bose [5, 6], Hirschfeld [12], and Lüneburg [16]. Translation nets corresponding to partial spreads have been studied by Bruen [8–10] and Jungnickel [14] among other authors. Translation nets in general were considered by Sprague [17] and Jungnickel [13, 15].

It can be shown that pcp's with large values of r can only occur in elementary abelian groups; e.g., if $r > s - \sqrt{s}$ or if $r \geq s/(p-1)$, where p is the smallest prime dividing s, then G has to be elementary abelian (see [14, Theorem 2.1] and [15, Theorem 3.5], respectively.) In the present paper, we shall only consider abelian groups G; then already $r > \sqrt{s} + 1$ suffices to force G to be elementary abelian (see [13, Theorem 5.5]). It is easy to see that in the abelian case all components U_i are isomorphic and that G is the direct sum of any two components. Thus the structure of G is prescribed by the type of the components.

In this paper, we shall consider the case where the components are direct sums of copies of $\mathbb{Z}_q$ ($q = p^a$, p a prime). (It is easy to see that in the abelian

case one can restrict attention to p-groups, since any pcp of degree r will induce a pcp of degree r on any Sylow subgroup; cf. [13] or [17].) Thus let $G = \mathbb{Z}_q^{2n}$; our main result will be that each pcp in G has at most $p^n + 1$ components, where equality is possible. This result will be obtained by representing a pcp in G by a collection of invertible $n \times n$ matrices over $\mathbb{Z}_q$ and by establishing a close connection with partial spreads in the group $\mathbb{Z}_p^{2n}$. It turns out that the theory of pcp's in G is quite parallel to that of partial spreads (or spreads) over $\mathbb{Z}_p$ given by Bruck and Bose [5, 6]. For this reason, we shall call an (s, r)-pcp in $\mathbb{Z}_q^{2n}$ a *partial spread* over $\mathbb{Z}_q$; the corresponding translation nets might be called *homogeneous* translation nets.

2. A MATRIX REPRESENTATION

Let $U_1, \ldots, U_r$ be a partial spread in the group $G = \mathbb{Z}_q^{2n}$, where $q = p^a$, p a prime. As already mentioned, all components are then isomorphic to $U = \mathbb{Z}_q^n$. We may consider U as the additive group of the free module of rank n over $\mathbb{Z}_q$; the elements of U may be taken to be the column vectors $u = (u_1, \ldots, u_n)^T$. Then $G = U \oplus U$, and w.l.o.g. $U_1 = \{(u, 0) : u \in U\}$ and $U_2 = \{(0, u) : u \in U\}$.

Now let V be any other component. Since V and U_2 are disjoint, we have

$$V = \{(u, f(u)) : u \in U\}$$

for a suitable mapping $f : U \to U$. [Assuming (u, v) and $(u, v') \in V$, we would obtain $(0, v - v') \in V \cap U_2$, a contradiction for $v \neq v'$. For reasons of cardinality, V then has to contain an element of the form (u, v) for each $u \in U$.] Similarly, since V and U_1 are disjoint, we see that f has to be one-to-one, hence a bijection. Since U and V are groups, V has to contain the element

$$(u, f(u)) + (u', f(u')) \overset{!}{=} (u + u', f(u + u'))$$

for all $u, u' \in U$; thus f is an automorphism of U. Moreover, since $\mathbb{Z}_q$ is cyclic, f is in fact an automorphism of the free module of rank n over $\mathbb{Z}_q$, and may thus be written in the form $f(u) = Au$ for some invertible $n \times n$ matrix A over $\mathbb{Z}_q$.

Thus we obtain invertible $n \times n$ matrices $A_3, \ldots, A_r$ over $\mathbb{Z}_q$ such that

$$U_i = \{(u, A_i u) : u \in U\} \qquad \text{for} \quad i = 3, \ldots, r.$$

Since U_i and U_j are disjoint for $i \neq j$, we have to have $A_i u \neq A_j u$ for all $u \in U$, which implies that the mapping $u \to (A_i - A_j)u$ is one-to-one, hence a bijection. Therefore $A_i - A_j$ is an invertible matrix, too, whenever $i \neq j$.

Conversely, it is easily checked that given a set of matrices $A_3, \ldots, A_r$ satisfying the conditions just stated one may construct a partial spread over $\mathbb{Z}_q$. Thus we have proved the following result which generalizes the standard matrix description of (partial) spreads over $\mathbb{Z}_p$ (cf. Bruck and Bose [5, 6]):

THEOREM 2.1. *Let $A_3, \ldots, A_r$ be invertible $n \times n$ matrices over $\mathbb{Z}_q$ such that $A_i - A_j$ is invertible too whenever $i \neq j$. Put $U = \mathbb{Z}_q^n = \{u = (u_1, \ldots, u_n)^T : u_1, \ldots, u_n \in \mathbb{Z}_q\}$, $G = U \oplus U$, $U_1 = \{(u, 0) : u \in U\}$, $U_2 = \{(0, u) : u \in U\}$, and $U_i = \{(u, A_i u) : u \in U\}$ for $i = 3, \ldots, r$. Then $U_1, \ldots, U_r$ is a partial spread in G; moreover, every partial spread in G may be represented in this way.*

3. REDUCTION mod p

Using Theorem 2.1, we will now establish a close connection between partial spreads over $\mathbb{Z}_q$ and partial spreads over $\mathbb{Z}_p$. Thus let $U_1, \ldots, U_r$ be a partial spread in $G = \mathbb{Z}_q^{2n}$, represented by matrices $A_3, \ldots, A_r$ as in Theorem 2.1. We may consider the matrices A_i as matrices with integer entries. Since A_i is invertible over $\mathbb{Z}_q$, its determinant $\det_q A_i$ over $\mathbb{Z}_q$ is a unit. Since $\det_q A_i$ is the reduction modulo q of the determinant $\det_{\mathbb{Z}} A_i$ of A_i over the integers, we see that $\det_{\mathbb{Z}} A_i$ is not divisible by p. Now denote by B_i the reduction of A_i modulo p (componentwise). Then $\det_p B_i$, the determinant of B_i over $\mathbb{Z}_p$, is $\neq 0$ in $\mathbb{Z}_p$, and thus B_i is an invertible matrix over $\mathbb{Z}_p$. Similarly, $B_i - B_j$ is an invertible matrix over $\mathbb{Z}_p$ whenever $i \neq j$, since the corresponding condition holds for the $A_i - A_j$ (over $\mathbb{Z}_q$). Thus $B_3, \ldots, B_r$ describes a partial spread over $\mathbb{Z}_p$, by Theorem 2.1. Thus we have:

PROPOSITION 3.1. *The existence of a partial spread with r components in $\mathbb{Z}_q^{2n}$ implies that of a partial spread with r components in $\mathbb{Z}_p^{2n}$.*

Since any partial spread in $\mathbb{Z}_p^{2n}$ has at most $p^n + 1$ components (as is well known and easily seen by counting), we have:

COROLLARY 3.2. *Let $U_1, \ldots, U_r$ be a partial spread in $\mathbb{Z}_q^{2n}$, $q = p^a$. Then one has $r \leqslant p^n + 1$.*

Note that Corollary 3.2 is a special case of [13, Proposition 5.3]. The present method of proof has the advantage that it allows us also to prove a converse of Proposition 3.1, i.e. to "lift" partial spreads over $\mathbb{Z}_p$ to partial spreads over $\mathbb{Z}_q$.

PROPOSITION 3.3. *Assume the existence of a partial spread with r components in $\mathbb{Z}_p^{2n}$, p a prime. Then there also exists a partial spread with r components in $\mathbb{Z}_q^{2n}$, where $q = p^a$, a an arbitrary positive integer.*

Proof. Let $\overline{U}_1, \ldots, \overline{U}_r$ be a partial spread in $\mathbb{Z}_p^{2n}$, represented by invertible $n \times n$ matrices $A_3, \ldots, A_r$ over $\mathbb{Z}_p$ as in Theorem 2.1. We may regard $A_3, \ldots, A_r$ as matrices over the integers; then $\det A_i$ and $\det(A_i - A_j)$ $(i \neq j)$ are not divisible by p. Thus, viewing the A_i as matrices over $\mathbb{Z}_q$, $\det_q A_i$ and $\det_q(A_i - A_j)$ are units in $\mathbb{Z}_q$. Hence the A_i and $A_i - A_j$ are invertible over $\mathbb{Z}_q$ and may be used to construct the desired partial spread in $\mathbb{Z}_q^{2n}$, via Theorem 2.1. ∎

Summing up, we have the following result.

THEOREM 3.4. *Let $U_1, \ldots, U_r$ be a partial spread in $\mathbb{Z}_q^{2n}$, described by matrices $A_3, \ldots, A_r$ as in Theorem 2.1. Denote by B_i the matrix obtained from A_i by reducing all entries* mod p *($q = p^a$, p a prime). Then $B_3, \ldots, B_r$ determine a partial spread $\overline{U}_1, \ldots, \overline{U}_r$ in $\mathbb{Z}_p^{2n}$. Moreover, every partial spread in $\mathbb{Z}_p^{2n}$ arises in this manner. Finally, a partial spread in $\mathbb{Z}_q^{2n}$ is maximal if and only if the corresponding partial spread in $\mathbb{Z}_p^{2n}$ is maximal.*

As a corollary, we immediately have:

THEOREM 3.5. *The maximum size of a partial spread in $\mathbb{Z}_q^{2n}$, where $q = p^a$, p a prime, is precisely $p^n + 1$.*

Note that this shows that the bound of Corollary 3.2 is best possible. This was previously known only for the case $n = a = 2$ (see [13, 5.7]). Note that it seems difficult (if at all possible) to "lift" a partial spread over $\mathbb{Z}_p$ directly to $\mathbb{Z}_q$, without using the matrix representation of Section 2. It is certainly not possible to define U_i just as the subgroup of $\mathbb{Z}_q^{2n}$ generated by $\overline{U}_i$ (where one considers the elements of $\mathbb{Z}_p^{2n}$ as elements of $\mathbb{Z}_q^{2n}$). The converse process is much simpler: Our arguments imply that it is indeed possible to obtain a partial spread in $\mathbb{Z}_p^{2n}$ from one in $\mathbb{Z}_q^{2n}$ by just reducing all components of the elements of $\mathbb{Z}_q^{2n}$ (viewed as vectors of length $2n$) modulo p.

4. PARTIAL SPREADS OVER $\mathbb{H}_p$

Let $A_3, \ldots, A_r$ be a set of $n \times n$ matrices over $\mathbb{Z}_p$ defining a partial spread with r components in $\mathbb{Z}_p^{2n}$ as in Theorem 2.1. Viewing the A_i as matrices over $\mathbb{Z}_p, \mathbb{Z}_{p^2}, \mathbb{Z}_{p^3}, \ldots$, the method of the preceding section yields a series of partial spreads $\mathbf{U}_a = \{U_1^{(a)}, \ldots, U_r^{(a)}\}$ over $\mathbb{Z}_{p^a}$ for $a = 1, 2, \ldots$, defining corresponding translation nets $\mathbf{D}_a$ with translation group $G_a = (\mathbb{Z}_{p^a})^{2n}$. Denote by $\phi_a: \mathbb{Z}_{p^{a+1}} \to \mathbb{Z}_{p^a}$ the natural epimorphism (i.e., reduction mod p^a). Then we have the sequence of groups

$$\mathbb{Z}_p \xleftarrow{\phi_1} \mathbb{Z}_{p^2} \xleftarrow{\phi_2} \mathbb{Z}_{p^3} \xleftarrow{\phi_3} \cdots \leftarrow \mathbb{H}_p$$

with inverse limit $\mathbb{H}_p$, the ring of p-adic integers. Of course, we may also view the A_i as matrices over $\mathbb{H}_p$; this gives a partial spread $\mathbf{U} = \{U_1, \ldots, U_r\}$ in $\mathbb{H}_p^{2n}$ and an associated translation net $\mathbf{D}$. Then the ϕ_a induce corresponding epimorphisms ψ_a of the translation nets constructed, and we have the sequence

$$\mathbf{D}_1 \xleftarrow{\psi_1} \mathbf{D}_2 \xleftarrow{\psi_2} \mathbf{D}_3 \xleftarrow{\psi_3} \cdots \leftarrow \mathbf{D}$$

of translation nets, with inverse limit $\mathbf{D}$. Moreover, every translation net over the p-adic integers is essentially of this type: It is described by invertible matrices over $\mathbb{H}_p$, and we obtain it as an inverse limit by using the reductions of these matrices mod p, mod p^2, mod p^3, etc.

This rather curious observation may have a little interest, since inverse limits of geometric structures have been studied several times in the last years.

5. CONCLUDING REMARKS

We conclude this paper with a problem and a few remarks. Corollary 3.2 is a special case of the following result proved by the author in [13, Proposition 5.3]:

RESULT 5.1. *Let U be an abelian p-group for type $(a_1, \ldots, a_n)$ with $a_1 \geq a_2 \geq \cdots \geq a_n$. If $a_1 = \cdots = a_n$, put $h = n$; otherwise let h be defined by requiring $a_1 = \cdots = a_h > a_{h+1}$. Assume the existence of a pcp with r components in $G = U \oplus U$. Then $r \leq p^h + 1$.*

Theorem 3.5 shows that Result 5.1 is best possible in case $a_1 = \cdots = a_n$. It would be interesting to know if this is true for arbitrary types. As a simple consequence of Result 5.1, one obtains a result already mentioned in the introduction (see [13, 5.5]):

COROLLARY 5.2. *Assume the existence of a pcp with more than* $\sqrt{s}+1$ *components in an abelian group* G *of order* s^2. *Then* G *is elementary abelian.*

Again, Theorem 3.5 shows that this result is best possible. Using Result 5.1, one may also obtain the following result; the simple proof will be left to the reader.

COROLLARY 5.3. *Assume the existence of a pcp with exactly* $\sqrt{s}+1$ *components in an abelian group* G *of order* s^2. *Then* G *is either elementary abelian or a direct sum of copies of a group* $\mathbb{Z}_{p^2}$, *where* p *is a prime.*

It would be nice to characterize the abelian groups which are direct sums of copies of groups $\mathbb{Z}_{p^a}$ in a similar way (using pcp's). This seems, however, not possible. For instance, we may take $s = p^6$ and observe that we have pcp's with p^2+1 components in each of the groups $\mathbb{Z}_p^{12}$, $\mathbb{Z}_{p^2}^6$, $\mathbb{Z}_{p^3}^4$, and $\mathbb{Z}_{p^2}^4 \oplus \mathbb{Z}_p^4$. (The last of these is obtained by taking the direct sums of corresponding components of a pcp with p^2+1 components in $\mathbb{Z}_{p^2}^4$ and a pcp with p^2+1 components in $\mathbb{Z}_p^4$, respectively.)

Note added in proof: The problem mentioned in Section 5 is settled in the paper "Translation nets and fixed-point-free group automorphisms" by R. A. Bailey and D. Jungnickel (submitted), where the maximum number of components of a pcp in $G \times G$ is determined for every abelian group G.

REFERENCES

1 J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe, *Math. Z.* 60:156–186 (1954).

2 T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Bibliographisches Inst., Mannheim, and Cambridge U.P., Cambridge, 1985.

3 A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, Geom. *Dedicata* 9:425–449 (1980).

4 R. H. Bruck, Finite nets I. Numerical invariants, *Canad. J. Math.* 3:94–107 (1951).

5 R. H. Bruck and R. C. Bose, The construction of translation planes from projective spaces, *J. Algebra* 1:85–102 (1964).

6 R. H. Bruck and R. C. Bose, Linear representations of projective planes in projective spaces, *J. Algebra* 4:117–127 (1966).
7 A. A. Bruen, Partial spreads and replaceable nets, *Canad. J. Math.* 23:381–391 (1971).
8 A. A. Bruen, Unembeddable nets of small deficiency, *Pacific J. Math.* 43:51–54 (1972).
9 A. A. Bruen, Collineations and extensions of translation nets, *Math. Z.* 145:243–249 (1975).
10 A. A. Bruen, Blocking sets and translation nets, in *Finite Geometries* (N. L. Johnson, M. H. Kallaher, and C. T. Long, Eds.), Marcel Dekker, New York, 1983, pp. 77–92.
11 D. Frohardt, Groups with a large number of large disjoint subgroups, *J. Algebra* 107:153–159 (1987).
12 J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford U.P., Oxford, 1985.
13 D. Jungnickel, Existence results for translation nets, in *Finite Geometries and Designs*, London Math. Soc. Lecture Note Ser. 49, Cambridge U.P., Cambridge, 1981, pp. 172–196.
14 D. Jungnickel, Maximal partial spreads and translation nets of small deficiency, *J. Algebra* 90:119–132 (1984).
15 D. Jungnickel, Existence results for translation nets, II, to appear in *J. Algebra*.
16 H. Lüneburg, *Translation Planes*, Springer, Berlin, 1980.
17 A. P. Sprague, Translation nets, *Mitt. Math. Sem. Giessen* 157:46–68 (1982).

Received 22 June 1987; final manuscript accepted 29 March 1988