On the existence of translation nets

Dirk Hachenberger

Angaben zur Veröffentlichung / Publication details:

Hachenberger, Dirk. 1992. "On the existence of translation nets." *Journal of Algebra* 152 (1): 207–29. https://doi.org/10.1016/0021-8693(92)90096-5.

On the Existence of Translation Nets*

DIRK HACHENBERGER[1]

Mathematisches Institut, Justus-Liebig-Universität Giessen,
Arndtstrasse 2, 6300 Giessen, Germany

Communicated by E. Kleinfeld

Received June 26, 1990

The existence of a translation net of order s and degree r with translation group G is equivalent to the existence of r mutually disjoint subgroups of G of order s. In this paper we consider p-groups G of odd square order p^{2n} and improve the known general upper bound on the number of mutually disjoint subgroups of order p^n in G provided that G is not elementary abelian. This solves problem 8.2.14 in (D. Jungnickel, Latin squares, their geometries and their groups. A survey, *in* "Coding Theory and Design Theory II" (D. K. Ray-Chaudhuri, Ed.), pp. 166–225, Springer, Berlin/New York, 1990.) We determine all groups of order p^4 which are translation groups of translation nets with at least three parallel classes for all prime numbers p. Furthermore, we construct (p^3, p^2+1)-translation nets with non-abelian translation group of order p^6 for all odd prime numbers p.

1. INTRODUCTION

A Bruck-net of order s and degree r (for short an (s, r)-net) is an incidence structure with parallelism satisfying the following axioms:

(N1) Any two points are joined by at most one line.

(N2) Given any point-line-pair (v, l), there is a unique line l^* with $l \parallel l^*$ and $v \in l^*$.

(N3) Any two non-parallel lines intersect in a unique point.

(N4) There exist $r \geqslant 3$ parallel classes each consisting of s lines.

By these axioms an (s, r)-net is the same as an affine 1-design $S_r(1, s, s^2)$.

In this paper we examine a special class of (s, r)-nets, namely, the translation nets:

* The results of this paper will form part of the author's doctoral thesis. He thanks his supervisor, Professor Dr. Dieter Jungnickel, for helpful discussions.

[1] Present address: Fachbereich Mathematik der Universität Kaiserslautern, Erwin Schrödinger-Strasse, 6750 Kaiserslautern, Germany.

1.1. Definition. A translation net of order s and degree r is a pair (N, G), where N is an (s, r)-net and $G \leqslant \mathrm{Aut}(N)$ is an automorphism group of N acting regularly on the set of points of N and fixing each parallel class of N. G is called a translation group of N.

We remark that a translation net is considered as a pair (N, G) as it is possible for a net to be a translation net with respect to even non-isomorphic translation groups. We refer the reader to [11], where examples of this situation are given.

Proposition (1.3) as well goes back to [11]. It reduces the problem of finding translation nets to a combinatorial problem in group theory. We need a further definition first.

1.2. Definition. Let G be a group of order s^2 and assume that there exists a set $\mathscr{H} = \{H_1, ..., H_r\}$ of $r \geqslant 3$ subgroups of G satisfying

(i) $|H_i| = s$ for all $i = 1, ..., r$ and

(ii) $H_i H_j = G$ for all $i \neq j$.

(Because of (i), (ii) is equivalent to $H_i \cap H_j = 1$ for all $i \neq j$). $\mathscr{H}$ is called a partial congruence partition with parameters s and r (for short (s, r)-PCP). The elements of $\mathscr{H}$ are called components.

1.3. Proposition. *Let $\mathscr{H}$ be an (s, r)-PCP in a group G of order s^2, then the incidence structure*

$$N(\mathscr{H}) = (G, \{H_i g : i = 1, ..., r;\ g \in G\}, \in)$$

is an (s, r)-translation net with translation group G. Conversely, every translation net can be represented in this way.

We only use the group theoretic notion of translation nets in this paper. We omit a proof of (1.3). The interested reader is referred to [8, 11].

In the following section we summarize some results on translation nets and introduce some further notations. After proving some "factorization theorems" in Section 3 we are able to determine all groups of order p^4 (p a prime number) which admit a (p^2, r)-PCP satisfying $r \geqslant 3$ in Section 4. Because of (1.3) this characterizes the groups of order p^4 which are translation groups for translation nets of order p^2 and degree $r \geqslant 3$. In Section 5 we generalize a theorem of D. Frohardt [4]. We improve the known general upper bound for the number r of parallel classes in a translation net (N, G), where G is a p-group of odd order p^{2n}. We conclude with a construction of $(p^3, p^2 + 1)$-PCPs in a nonabelian group of order p^6 for every odd prime number p in Section 6.

2. Existence Results for Translation Nets, A Survey

We assume that G is a group of order s^2 and $\mathscr{H} = \{H_1, ..., H_r\}$ is an (s, r)-PCP in G. By Definition (1.2) one obtains $r(s-1) \leqslant s^2 - 1$ and therefore the number r of parallel classes in a translation net does not exceed $s+1$. We mention that this bound is sharp precisely for elementary abelian groups (see e.g. [10]).

The following notation is the same as in [10]:

$$T(G) := \max\{r \leqslant s+1\text{: there exists an } (s, r)\text{-PCP in } G\}, \tag{2.1}$$

$$T(s) := \max\{T(G)\text{: } G \text{ a group of order } s^2\}. \tag{2.2}$$

The following theorem shows that the structure of G is very restricted, if some components in G are normal subgroups of G. As we need this result several times we include a short proof.

2.3. Theorem (A. P. Sprague [11]). (i) *If H_1 is a normal subgroup of G then $H_2 \cong H_3 \cong \cdots \cong H_r$.*

(ii) *If H_1 and H_2 are normal subgroups of G then $G \cong H_1 \times H_2$ and all components are isomorphic.*

(iii) *If $\mathscr{H}$ contains three normal components, then G is abelian.*

Proof. Let H_1 be a component of $\mathscr{H}$. By definition of an (s, r)-PCP in G we can regard each other component $H_2, ..., H_r$ as a complete set of right coset representatives of H_1 in G. For $i, j \in \{2, ..., r\}$ and $i \neq j$ we consider the mapping

$$\Gamma_{i,j}\colon H_i \to H_j, \qquad h \to \Gamma_{i,j}(h),$$

where $\Gamma_{i,j}(h)$ is uniquely determined by $H_1 h = H_1 \Gamma_{i,j}(h)$. Now it is not difficult to show, that all mappings $\Gamma_{i,j}$ are isomorphisms provided that H_1 is a normal subgroup of G. This proves part (i).

Part (ii) is a direct consequence of part (i).

Assume that we have three normal components H_1, H_2, and H_3 in $\mathscr{H}$, then H_1 centralizes H_2 and H_3 and therefore H_1 centralizes $G = H_2 H_3$. This implies that H_1 is a subgroup of the center $Z(G)$ of G. The same argument shows that H_2 as well lies in $Z(G)$ so that we obtain $G = H_1 H_2 \leqslant Z(G)$ and therefore G is abelian. ▌

We remark that the corresponding translation nets of partial congruence partitions containing one normal component are called semi-splitting translation nets in [6, Section 4]. There these objects are studied under a more geometric point of view and in relation to difference matrices. Structures of type (2.3)(ii) are called splitting translation nets by R. A. Bailey and D. Jungnickel in [2].

The following basic lemma is very useful in dealing with PCPs (see as well [4, 9, 11]). As we make use of it several times we again include a proof.

2.4. Lemma. (i) *Let G be a finite group and let H and K be subgroups of G with $HK=G$. Then $|H\cap K|=|H^x\cap K^y|$ for all x, y in G.*

(ii) *If $\{H_1, ..., H_r\}$ is an (s, r)-PCP in G, then the same is valid for $\{H_1^{g_1}, ..., H_r^{g_r}\}$ where $g_1, ..., g_r$ are arbitrarily chosen in G. Furthermore, if $H^G=\{h^g\colon h\in H, g\in G\}$, then $\sum_{i=1}^r(|H_i^G|-1)\leqslant|G|-1$.*

Proof. (i) It suffices to consider the case where $y=1$. By assumption we find elements h and k in H and K respectively satisfying $x=hk$. Then we obtain $|H^x\cap K|=|H^{hk}\cap K|=|H^k\cap K|=|(H\cap K)^k|=|H\cap K|$.

(ii) is a direct consequence of (i). ▮

Applying this lemma one can prove that an (s, r)-PCP in a group G of order s^2 induces a (p^n, r)-PCP in each p-Sylow subgroup P of G ($|P|=p^{2n}$). This was mentioned in [4] but follows also as a corollary of [9, Lemma 2.3]. We include again a proof as this is the main reason for studying p-groups in this paper.

2.5. Theorem. *Let G be a group of order s^2, $p_1^{a_1}\cdot\cdots\cdot p_k^{a_k}$ the canonical prime power factorization of s and let P_i be a p_i-Sylow subgroup of G for $i=1, ..., k$. Then*

(i) *$T(G)\leqslant\min\{T(P_i)\colon i=1, ..., k\}$ and*

(ii) *$T(G)\leqslant\min\{p_i^{a_i}+1\colon i=1, ..., k\}$.*

Proof. Let p be a prime divisor of s and P a p-Sylow subgroup of G. Let $|P|=p^{2n}$, then by assumption the p-Sylow subgroup of each component has order p^n. Let $\mathscr{H}$ be an (s, r)-PCP in G and H be any component of $\mathscr{H}$. By Sylow's theorem we can find an element g in G such that $H^g\cap P$ is a p-Sylow subgroup of H^g. As the PCP-properties in (1.2) remain valid in going over to conjugate subgroups (see (2.4)), $\mathscr{H}$ induces a (p^n, r)-PCP in P. This proves (2.5)(i). (2.5)(ii) holds since $T(P)\leqslant p^n+1$ if P is a p-group of order p^{2n}. ▮

We remark that equality can be realized in (2.5)(i) if G is a nilpotent group (see for example [2], where $T(G)$ is determined for all finite abelian groups), but there are also other examples (see [8, 9]). In general, equality does not hold in (2.5)(i) (we refer the reader to [10], where examples of this situation are given). One has equality in (2.5)(ii) if G is abelian and every p-Sylow subgroup of G is elementary abelian, but there are as well other examples. Under the assumptions of (2.5) we have therefore

$$T(s) = \min\{p_i^{a_i} + 1 : i = 1, ..., k\}.$$

Theorem (2.5) is the motivation for us to study PCPs in p-groups. Next we summarize what is known about $T(G)$, if G is a finite p-group of order p^{2n} which is not elementary abelian (note that we have $T(G) = p^n + 1$ in the elementary abelian case).

2.6. Theorem (D. Jungnickel [8]). $T(G) \leqslant p^{n-1} + \cdots + p + 1$.

2.7. Theorem (D. Frohardt [4]). *If $p = 2$ and $n \geqslant 4$, then $T(G) < 2^{n-1}$.*

In Section 5 we prove

2.8. Theorem. *If p is odd and $n \geqslant 4$, then $T(G) < p^{n-1}$.*

In [3] J. Dillon proved the following theorem:

Given a group G of order $4k^2$ and a $(2k, k)$-PCP $\mathscr{H}$ in G, then $D := \bigcup_{H \in \mathscr{H}} H - \{1\}$ is a $(4k^2, 2k^2 - k, k^2 - k)$-Hadamard difference set.

He posed the problem of classifying all such groups G. This was D. Frohardt's reason for studying PCPs in 2-groups in [4]. We return to this situation in Section 5 where we cite the main result of [4], deal with the case where p is an odd prime number, and give a proof of (2.8).

We mention once more that we investigate groups of order p^4, which covers the case $n = 2$. The existence of a maximal $(8, 4)$-PCP in a nonabelian group of order 64 (the case $p = 2$ and $n = 3$) was proved by A. P. Sprague in [11]. This result was later rediscovered by D. Gluck in [5]. In Sections 5 and 6 we investigate the case where p is odd and $n = 3$ and show among other things the existence of a $(p^3, p^2 + 1)$-PCP in a particular nonabelian group of order p^6 for all odd prime numbers p.

Suppose we have an (s, r)-PCP $\mathscr{H}$ in G and N is a normal subgroup of G. If we look at $\mathscr{H}_N := \{HN/N : H \in \mathscr{H}\}$ then we obtain a set of subgroups of the factor group G/N which satisfies $KL = G/N$ for all different K, L in $\mathscr{H}_N$. Of course K and L may have nontrivial intersection so that $\mathscr{H}_N$ is not necessarily a PCP in G/N. D. Jungnickel proved his bound (2.6) by studying this more general situation and actually obtained stronger results. We cite without proof the following:

2.9. Definition and Proposition. *Let p be a prime number and G be a group of order p^m $(m \geqslant 2)$ and let $\mathscr{H} = \{H_1, ..., H_w\}$ be a set of proper subgroups of G satisfying $w \geqslant 2$ and $H_i H_j = G$ whenever $i \neq j$. Then $\mathscr{H}$ is called* *a generalized partial congruence partition with parameter* $a = \max\{i$: *there exists an element* H *in* $\mathscr{H}$ *with* $|H| = p^i\}$ (*for short* $GPCP(a)$).

Then the following holds:

(i) $w \leqslant p^a + \cdots + p + 1$ *and*

(ii) $w \leqslant p^{a-1} + \cdots + p + 1$, *if* G *is not elementary abelian.*

We remark that (2.9) is proved only by using basic results about p-groups (see e.g. [7, Chap. III] or [12, Chap. IV]). We only apply (2.9)(i).

In Section 3 we study situations where the PCP-property remains valid if one proceeds to factor groups so that together with (2.9) we have two nice induction arguments.

3. Variations of a Factorization Lemma

Lemma (3.1) is an essential tool for non-existence results on partial congruence partitions. It says under which conditions a PCP in G induces a PCP with the same number of components in a normal subgroup of G and the corresponding factor group.

3.1. Factorization Lemma. *Let* G *be a group of order* s^2, N *a normal subgroup of* G, *and* $\mathscr{H}$ *an* (s, r)-*PCP in* G *with* $r \geqslant 3$. *Assume the validity of*

$$N = (H \cap N)(K \cap N) \text{ for each pair of subgroups } H, K\ (H \neq K) \text{ in } \mathscr{H}. \qquad (*)$$

Then the following holds:

(i) *The order of* N *is a square, say* $|N| = n^2$; *the order of the factor group* G/N *is* $(s/n)^2$.

(ii) $\{H \cap N$: $H \in \mathscr{H}\}$ *is an* (n, r)-*PCP in* N.

(iii) $\{HN/N$: $H \in \mathscr{H}\}$ *is an* $(s/n, r)$-*PCP in* G/N.

Proof. Let H, K, L be pairwise different components of $\mathscr{H}$ and let h, k, l denote the intersection numbers $|H \cap N|$, $|K \cap N|$, and $|L \cap N|$, respectively. Because of (1.2) (ii) and our assumptions we have $|N| = hk = kl = hl$ and therefore $h = k = l$. This proves (i) and (ii). An elementary calculation shows furthermore $|HN/N \cap KN/N| = 1$, so that (iii) as well is satisfied. ▌

We now state some very useful applications of (3.1). Our notation is the same as in the assumptions of (3.1).

3.2. Application 1. *Let $N = Z(G)$ be the center of the group G and $\mathscr{H}$ an (s, r)-PCP consisting only of abelian components. Then $(*)$ holds. Furthermore, if G is a p-group of order p^{2n} and the class of G equals c then*

$$r \leqslant p^{[n/c]} + 1.$$

(Here $[x] := \max\{k \in \mathbb{N} \cup \{0\} \colon k \leqslant x\}$ for any rational number x.)

Proof. Let H and K be elements of $\mathscr{H}$ and z an element of $Z(G)$. Because of (1.2)(ii) we may write z as the product hk with h in H and k in K. Then $k = h^{-1}z$ centralizes H and K, as both components are assumed to be abelian. We therefore have $k \in K \cap Z(G)$. The same argument shows that h lies in $H \cap Z(G)$. This proves $Z(G) = (H \cap Z(G))(K \cap Z(G))$, the first assertion.

Now assume that G is a p-group of order p^{2n}. Let $Z_0 = 1$, $Z_1 = Z(G)$ and recursively Z_i such that $Z_i/Z_{i-1} = Z(G/Z_{i-1})$ for $i \geqslant 1$. $(Z_i)_{i \geqslant 0}$ is the lower central series of G. The class c of G is defined as the number $\min\{k \in \mathbb{N} \colon Z_k = G\}$.

Now define $\mathscr{H}_1 := \{H \cap Z_1 \colon H \in \mathscr{H}\}$, $\mathscr{H}_2 := \{HZ_1/Z_1 \cap Z_2/Z_1 \colon H \in \mathscr{H}\}$ and recursively $\mathscr{H}_{k+1} := \{HZ_k/Z_k \cap Z_{k+1}/Z_k \colon H \in \mathscr{H}\}$ for $k \leqslant c - 1$. It is not difficult to see that $\mathscr{H}_m$ are PCPs consisting of r components which are all abelian ($m = 1, \ldots, c$). Let $|HZ_k/Z_k \cap Z_{k+1}/Z_k| = p^{z_{k+1}}$, then $\mathscr{H}_{k+1}$ is a $(p^{z_{k+1}}, r)$-PCP in G/Z_k. Furthermore we obtain $r \leqslant \min\{p^{z_j} + 1 \colon j = 1, \ldots, c\}$ and since $n = \sum_{j=1}^{c} z_j$ we have $r \leqslant p^{[n/c]} + 1$. ▮

3.3. Application 2. *Let p be a prime divisor of $|Z(G)|$, $N = \Omega_p(Z(G)) = \langle x \in Z(G) \colon x^p = 1 \rangle$ the largest elementary abelian p-subgroup of $Z(G)$ and $\mathscr{H}$ an (s, r)-PCP consisting of abelian components only. Then $\mathscr{H}$ satisfies $(*)$.*

Proof. N is an elementary abelian normal subgroup of G. For every z in N we have by (3.2) $1 = z^p = (hk)^p = h^p k^p$ for some elements h, k in $H \cap Z(G)$ and $K \cap Z(G)$ respectively. Because of (1.2)(ii) we conclude $h^p = k^p = 1$ as $h^{-p} = k^p$ is an element of $H \cap K = 1$. ▮

We remark that $\Omega_p(Z(G)) \neq 1$ is always valid in a p-group G since p-groups have nontrivial centers. We mention that (3.3) as well is used by D. Frohardt in [4].

Now (3.3) implies the following bound (3.4) which is proved similarly as (3.2) by induction.

3.4. Application 3. *Let G be a group of order p^{2n}, $\mathscr{H}$ a (p^n, r)-PCP with abelian components. We define the following series of groups:*

$$G := G_1, \qquad C_1 := \Omega_p(Z(G_1)),$$

$$G_{i+1} := G_i/C_i, \qquad \textit{and} \qquad C_{i+1} := \Omega_p(Z(G_i)) \qquad \textit{for} \quad i \geqslant 1.$$

Let e be (the finite number) $\min\{x \in \mathbb{N}\colon G_x = C_x\}$, *then*

$$r \leqslant p^{[n/e]} + 1.$$

The next two applications of (3.1) are as well corollaries of a result on splitting translation nets (see [2]).

3.5. APPLICATION 4. *Let G be a group of order* s^2 *and* $\mathscr{H}$ *an* (s, r)*-PCP in G with two normal components H and K. Let* $N = G'$ *be the derived group of G, then* $(*)$ *is satisfied.*

Furthermore $\mathscr{H}' := \{H \cap G'\colon H \in \mathscr{H}\}$ *is a PCP with two normal components in G′ and leads therefore to a splitting translation net with translation group G′.*

For $s = p^n$ *and* $d := \min\{x \in \mathbb{N}\colon G^{(x)} = 1\}$, *where* $G^{(x)}$ *denotes the xth derived subgroup of G, we obtain*

$$r \leqslant p^{[n/d]} + 1.$$

Proof. By assumption we have $G \cong H \times K$, so that $K \leqslant C_G(H) = \{g \in G\colon gh = hg$ for every h in $H\}$ as well as $H \leqslant C_G(K)$. By $[a, b]$ we denote as usual the commutator $a^{-1}b^{-1}ab$. For $g_i = h_i k_i$ ($h_i \in H$, $k_i \in K$, $i = 1, 2$) we obtain $[g_1, g_2] = [h_1, h_2][k_1, k_2] \in H'K'$ which implies $G' = H'K'$. As $H' \cap K' = 1$ and H', K' are normal subgroups of G', we have $G' \cong H' \times K'$. Observe that for any component L of $\mathscr{H} - \{H, K\}$ (2.3)(ii) yields $L' \cong H'$. This implies that $(*)$ again is satisfied. The rest follows by a similar induction argument as in (3.2). ▌

3.6. APPLICATION 5. *If* $N = Z(G)$ *and* $\mathscr{H}$ *is an* (s, r)*-PCP in G containing two normal components, then* $\{Z(H)\colon H \in \mathscr{H}\}$ *and* $\{HZ(G)/Z(G)\colon H \in \mathscr{H}\}$ *are as well PCPs with two normal components in* $Z(G)$ *and* $G/Z(G)$, *respectively. Furthermore, if G is a p-group of order* p^{2n} *and class c and* $\mathscr{H}$ *is a* (p^n, r)*-PCP in G which contains two normal components then*

$$r \leqslant p^{[n/c]} + 1.$$

Proof. Let H and K be two normal components of $\mathscr{H}$. As $G \cong H \times K$ we have $Z(G) \cong Z(H) \times Z(K)$ and as L is isomorphic to H for all L in $\mathscr{H}$ by (2.3) we obtain $Z(L) \cong Z(H)$ and, after some simple commutator calculations, $(*)$.

As $HZ(G)/Z(G)$ and $KZ(G)/Z(G)$ are normal components in $G/Z(G)$ we may again use the induction method sketched in the proof of (3.2) and obtain the desired result. ▌

Before we study a final application of (3.1) we cite some commutator formulas and a basic result on *p*-groups of class at most 2 (see for example [1, (8.6) and (23.11)]).

3.7. LEMMA. *Let G be a group, x, y elements of G and assume that $z := [x, y]$ centralizes x and y. Then*

(i) $[x^m, y^n] = z^{mn}$ *for all m, n in $\mathbb{Z}$.*

(ii) $(xy)^n = x^n y^n z^{-n(n-1)/2}$ *for all n in $\mathbb{N} \cup \{0\}$.*

If G is a group of class at most 2, then

(iii) $[ab, x] = [a, x][b, x]$ *and* $[a, xy] = [a, x][a, y]$.

Assume that additionally p is an odd prime number and G is a p-group of class at most 2. Then

(iv) $\Omega_p(G) = \langle x \in G \colon x^p = 1 \rangle$ *has exponent p.*

3.8. APPLICATION 6. *Assume p is odd and let G be a p-group of order p^{2n} and class 2 with elementary abelian derived subgroup G'. Let $\mathscr{H}$ be* any *(p^n, r)-PCP in G. Then $(*)$ holds with $N := \Omega_p(G)$.*

Proof. Since the class of G is assumed to be 2 we have $G' \leqslant Z(G)$, in particular any commutator centralizes every element of G. For $g \in \Omega_p(G)$ we have $g = hk$ (for suitable $h \in H$, $k \in K$; H, $K \in \mathscr{H}$) and since $\Omega_p(G)$ has exponent p by (3.7)(iv) one obtains $1 = g^p = h^p k^p [k, h]^{p(p-1)/2} = h^p k^p$. We have $h^{-p} = k^p \in H \cap K = 1$ and therefore $h, k \in \Omega_p(G)$, which proves (3.8). ▮

4. TRANSLATION NETS OF ORDER p^2 AND DEGREE $r \geqslant 3$

In this section we apply the Factorization Lemma to groups of order p^4 where p is as usual a prime number. We are able to characterize all such groups which admit a $(p^2, 3)$-PCP. Beside (2.3) and the results of Section 3 we only use elementary group theoretic results. In particular all basic facts about p-groups can be found in [7, 12].

Observe that all groups of order p^2 are abelian so that all components are either cyclic or elementary abelian.

If G is abelian then all components are normal in G and (2.3)(ii) asserts that G is isomorphic to $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ or $(\mathbb{Z}_p)^4$. If G is elementary abelian then $T(G) = p^2 + 1$, if $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ then $T(G) = p + 1$ (see [2, 8]).

We assume now that G is nonabelian, and thus $T(G) \leqslant p + 1$ by (3.2) or (2.6). Since the factor group $G/Z(G)$ is not cyclic and $\Omega_p(Z(G))$ is a nontrivial subgroup of G the assumption $r \geqslant 3$ together with (3.3) and (3.4) leads to

$$Z(G) = \Omega_p(Z(G)) \cong \mathbb{Z}_p \times \mathbb{Z}_p \cong G/Z(G). \tag{4.1}$$

We denote by $\Phi(G)$ the Frattini subgroup of G. Using [7, Chap. III, 3.14] we have that $G^p := \langle x^p \colon x \in G \rangle$ and G' are subgroups of $\Phi(G)$. As G is a

p-group and $\Phi(G)$ is the smallest normal subgroup N of G such that G/N is elementary abelian we obtain together with (4.1):

$$G^p, G' \leqslant \Phi(G) \leqslant Z(G), \qquad \text{in particular } G \text{ is of class 2.} \tag{4.2}$$

As the theory is different depending on whether p is odd or even, we deal with the odd case first:

Using (3.8), we look at the cases $\Omega_p(G) = Z(G)$ and $\Omega_p(G) = G$ separately.

4.3. THEOREM. *Let G be a nonabelian group of odd order p^4. Assume that G contains at least three mutually disjoint subgroups of order p^2.*

(i) *If $\Omega_p(G) = Z(G)$, then G is metacyclic and isomorphic to a semidirect product of $\mathbb{Z}_{p^2}$ with $\mathbb{Z}_{p^2}$. Moreover, $T(G) = p+1$.*

(ii) *If $\Omega_p(G) = G$ then G is isomorphic to $E(p^3) \times \mathbb{Z}_p$ where $E(p^3) = \langle a, x, z \mid a^p = x^p = z^p = 1,\ [a, x] = z,\ [a, z] = [x, z] = 1 \rangle$ is the extraspecial group of order p^3 and exponent p. Moreover, $T(G) = p+1$.*

Proof. *Part* (i). Let M be a maximal subgroup of G. Every maximal subgroup of a nilpotent group is normal in G and intersects $Z(G)$ nontrivially.

In our case M is abelian if and only if M contains $Z(G)$:

If $Z(G) \leqslant M$, then $|M/Z(M)| \leqslant p$, therefore $M/Z(M)$ is cyclic so that $Z(M) = M$ which means that M is abelian. On the other side, if M is abelian and M intersects $Z(G)$ in a group of order p, then we would find a complement N of order p of $M \cap Z(G)$ in $Z(G)$ and obtain that G is isomorphic to $M \times N$, hence abelian, which contradicts our assumption.

Since $\Omega_p(G) = Z(G)$, every element x in $G - Z(G)$ has order p^2. Therefore every maximal subgroup M of G contains an element of order p^2 and has therefore exponent p^2. We have to consider the two cases where M is abelian and nonabelian, respectively:

If M is nonabelian, then M is of type $M(p^3) := \langle x, y \mid x^{p^2} = y^p = 1, [x, y] = x^p \rangle$. We remark that $M(p^3)$ is the extraspecial group of order p^3 and exponent p^2 (a p-group is called extraspecial, if $\Phi(G) = Z(G) = G'$ and $\Phi(G)$ has order p). Using (4.2) we see that $M \cap Z(G) = \langle x^p \rangle$ and G is isomorphic to $M \times \langle z \rangle$, where z lies in $Z(G) - \langle x^p \rangle$. But then $\langle x^p, y, z \rangle$ is an elementary abelian subgroup of G of order p^3, which is a contradiction to $|\Omega_p(G)| = p^2$.

We have proved that every maximal subgroup of G is abelian and contains $Z(G)$. As $\Phi(G)$ is the intersection of all maximal subgroups of G we obtain together with (4.2) that $\Phi(G) = Z(G)$. Furthermore every maximal subgroup is of type $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$.

Using Burnside's basis theorem on p-groups (see e.g., [7, Chap. III, 3.15]) and observing that $\Phi(G)=Z(G)=\Omega_p(G)$ has order p^2 we obtain that G is generated by two elements x and y of order p^2. Consider the subgroups $\langle x\rangle$ and $\langle y\rangle$. If G^p has order p then any two cyclic subgroups of G of order p^2 would have nontrivial intersection. As we have only one elementary abelian subgroup of order p^2 in G (namely $Z(G)$), G would not contain three mutually disjoint subgroups of order p^2. Therefore $G^p=\Phi(G)$ and we may assume that $\langle x^p, y^p\rangle = G^p$ and that $\langle x\rangle$ and $\langle y\rangle$ have trivial intersection.

$G'=\langle [x, y]\rangle$ has order p and lies in $Z(G)$. We regard $Z(G)$ as a (multiplicatively written) vector space over the finite field $GF(p)$ of order p which is generated by x^p and y^p. Using the commutator calculations of (3.7) one has $(x^iy^j)^p = x^{ip}y^{jp}$, so that every element in $Z(G)$ is indeed the pth power of an element in G. We may therefore assume without loss of generality that x^p generates G'. But then $\langle x\rangle$ is a normal subgroup of G and $G/\langle x\rangle = \langle y\langle x\rangle\rangle$ is cyclic of order p^2 as y^p does not lie in $\langle x\rangle$.

This proves that G is metacyclic and isomorphic to a semidirect product of $\mathbb{Z}_{p^2}$ with $\mathbb{Z}_{p^2}$. Using the presentation of G one can show that

$$\{\langle xy^j\rangle : j\in GF(p)\}\cup\{\langle y\rangle\}$$

is a $(p^2, p+1)$-PCP in G so that we have the desired result.

Part (ii). As G is of class 2 we have by (3.7)(iii) and our assumptions that G is of exponent p. Let y and z be generators of $Z(G)$ and a an element of $G-Z(G)$, then $M := \langle a, y, z\rangle$ is elementary abelian of order p^3 and, as a maximal subgroup, normal in G.

Every x in $G-M$ induces by conjugation a linear mapping on M, when M is regarded as a vector space over the field $GF(p)$. Without loss of generality we choose the basis (a, y, z) so that the operation of x on M leads to the Jordan canonical form, that means $a^x = ay$, $y^x = y$ and $z^x = z$. $N := \langle a, x\rangle$ is a nonabelian subgroup of order p^3 and of exponent p and therefore isomorphic to $E(p^3)$, the extraspecial group of order p^3 and exponent p (see [7, Chap. III, 12.6]).

As $N\cap Z(G)=\langle y\rangle$ we see that G is isomorphic to $\langle a, x\rangle\times\langle z\rangle$. We have now a concrete presentation of G. It remains to construct $p+1$ mutually disjoint subgroups of order p^2 in G.

Define $H_\infty := \langle x, z\rangle$ and $H_m := \langle ax^m, yz^m\rangle$ for $m\in GF(p)$, then

$$\mathscr{H} := \{H_\infty, H_0, ..., H_{p-1}\}$$

is a $(p^2, p+1)$-PCP in G. This can be proved easily by calculating in G using our presentation and the commutator formulas of (3.7). ▌

We remark that the two nonabelian groups in (4.3) meet D. Jungnickel's bound (2.6) as well as the bound in (3.2). The metacyclic example in the proof of (4.3)(i) was also given in [8]. It is remarkable that both groups have a cyclic derived subgroup of order p which lies in exactly one of the components of *any* given PCP with $p+1$ components since $G' \leqslant Z(G)$ and as we obtain an induced PCP in $Z(G)$. The unique component containing G' is a normal subgroup in G so that these groups lead to semi-splitting translation nets. As mentioned in Section 2 these types of nets are studied in [6].

We are now going to discuss the case $p=2$.

4.4. THEOREM. *Let G be a nonabelian group of order* 16 *which contains at least three mutually disjoint subgroups of order* 4. *Then G is isomorphic to $D_4 \times \mathbb{Z}_2$, where D_4 denotes the dihedral group of order* 8, *or G is isomorphic to $\langle x, y \colon x^4 = y^4 = 1,\ [x, y] = x^2y^2,\ (x^2y^2)^2 = 1\rangle$, which is a semidirect product of $\mathbb{Z}_4$ with $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Let G be a nonabelian group of order 16 satisfying $Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong G/Z(G)$ (see (4.1)). As $\Phi(G) = G^2$ (see [7, Chap. III, 3.14]) and $\Phi(G) \neq 1$ we have that the exponent of G is 4 by (4.1) and (4.2).

As in the proof of (4.3), we have $Z(G) = \Phi(G)$ if and only if every maximal subgroup of G is abelian.

We assume first that every maximal subgroup M of G is abelian. Then by (4.1), $G^2 = Z(G)$ is elementary abelian of order 4. There exist elements x and y of order 4 in G satisfying $Z(G) = \langle x^2, y^2\rangle$. Furthermore $\langle x\rangle \cap \langle y\rangle = 1$ holds so that $\langle x, y\rangle = G$. $G' = \langle [x, y]\rangle$ has order 2 and is a subgroup of $Z(G)$ so that we have $[x, y] \in \{x^2, y^2, x^2y^2\}$. Using the commutator calculations of (3.7) (i) and (ii) one can show that in any case x^2y^2 is not the square of an element in G.

If there is no element in $G - Z(G)$ of order 2 then we have that all three components are cyclic of order 4 (since $|H \cap Z(G)| = 2$ for every component), but then x^2y^2 would be the square of an element, a contradiction.

Let therefore a be an element of order 2 in $G - Z(G)$, then $M = \langle a, x^2, y^2\rangle$ is elementary abelian of order 8 and $xM = yM$. Now $x^{-1}y \in M$ and therefore $xy \in M$. But this means that xy has order 2 and we obtain $(xy)^2 = x^2y^2[y, x] = 1$ by (3.7). Therefore $[x, y] = x^2y^2$. Now $\langle x\rangle$, $\langle y\rangle$, $\{1, xy, x^2y^2, x^3y^3\}$ is a (4, 3)-PCP in G and G is isomorphic to the second group mentioned in the statement of the theorem (see also [6, Example 6.7]).

If G contains a nonabelian maximal subgroup M, then $\Phi(G)$ has order 2 and $\Phi(G) = M \cap Z(G)$. Furthermore we have that G is isomorphic to $D_4 \times \mathbb{Z}_2$ or $\mathbb{Q} \times \mathbb{Z}_2$ (here $\mathbb{Q}$ denotes the quaternion group of order 8) depending on the type of M.

As $\mathbb{Q} \times \mathbb{Z}_2$ contains 12 elements of order 4 and all elements of order 2 lie in the center of this group we see that all components have to be cyclic of order 4, as each component intersects the center in two elements by (3.2). But any two cyclic subgroups of order 4 contain $\Phi(G)=G^2$, which is of order 2. So $\mathbb{Q}\times\mathbb{Z}_2$ contains no (4, 3)-PCP.

With $D_4\times\mathbb{Z}_2=\langle a, b, z \mid a^4=b^2=z^2=1,\ [a,b]=a^2,\ [a,z]=[b,z]=1\rangle$ one sees that $\{\langle a\rangle, \langle ab, z\rangle, \langle a^2z, b\rangle\}$ is a (4, 3)-PCP. This completes the proof of (4.4). ∎

We finally collect the results of this section.

4.5. Theorem. *Let G be a group of order p^4 containing at least* three *mutually disjoint subgroups of order p^2. Then one has one of the following cases*:

(i) *$T(G)=p^2+1$ and G is elementary abelian.*

(ii) *$T(G)=p+1$ and G is isomorphic to $\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}$, $\langle x, y \mid x^{p^2}=y^{p^2}=1,\ [x,y]=x^p\rangle$ or $E(p^3)\times\mathbb{Z}_p$ in the odd case and $T(G)=3$ and G is isomorphic to $\mathbb{Z}_4\times\mathbb{Z}_4$, $\langle x, y \mid x^4=y^4=1,\ [x,y]=x^2y^2,\ (x^2y^2)^2=1\rangle$ or $D_4\times\mathbb{Z}_2$, when $p=2$.*

The results of Sections 3 and 5 imply that the groups in (4.5) (ii) are exactly the case where (2.6) is sharp.

5. A Generalization of a Theorem of D. Frohardt

In [4] D. Frohardt proved the following theorem:

5.1. Theorem. *Let G be a finite group of order $4k^2$ and assume $k>4$ and that G contains a $(2k, k)$-PCP. Then G is an elementary abelian 2-group.*

By using D. Frohardt's theorem (2.7) on 2-groups, A. P. Sprague's and D. Gluck's results on groups of order 36 and 64 (see [11] and [5, 11], respectively) and our results of Section 4 we prove

5.2. Theorem. *Let G be a group of order p^2k^2 where p is the smallest prime divisor of $|G|$ and $k\geqslant 3$. Assume that G contains a (pk, k)-PCP $\mathscr{H}$. Then one of the following cases is valid*:

If $p=2$ then G is

(i) *one of the following four groups of order 36*:

$$\mathbb{Z}_6\times\mathbb{Z}_6,\qquad \Sigma_3\times\Sigma_3,\qquad \Sigma_3\times\mathbb{Z}_6,$$

$$\mathbb{Z}_2\times\langle x, y, z \mid x^3=y^3=z^2=1,\ [x,z]=x,\ [y,z]=y,\ [x,y]=1\rangle,$$

(ii) *an elementary abelian 2-group,*

(iii) *the group* $\langle a, b, c, x, y, z\rangle$ *of order* 64 *where all generators have order* 2 *and all commutators are equal to* 1 *except* $[x, y]=a$ *and* $[x, z]=b$.

If p is odd then G is a p-group of order p^{2n}. Furthermore,

(iv) *if* $n=2$, *then G is one of the groups of order p^4 given in Theorem* (4.5);

(v) *if* $n\geqslant 4$, *then G is elementary abelian.*

The only case which is not covered in the statement of (5.2) is when G is a group of order p^6 and p is odd. Under the assumptions of (5.2) we can prove:

5.3. Theorem. *Let G be a group of order p^6, where p is an odd prime number. Assume that G is not elementary abelian.*

If G is the special group of exponent p with center of order p^3, then

$$T(G)\leqslant p^2+1.$$

In all other cases, one has $T(G)<p^2$.

Let G be the special group of exponent p with center of order p^3. In Section 6 we give a construction of a (p^3, p^2+1)-PCP in G. We therefore obtain $T(G)=p^2+1$ for all odd prime numbers p.

The proofs of (5.2) and (5.3) proceed in several steps. We first show that the existence of a large number of mutually disjoint subgroups forces G to be a p-group except in the case where $|G|=36$. From now on the assumptions are the same as in (5.2).

5.4. G is a p-group or $|G|=36$.

Proof. Assume $k=p^t n$, where p does not divide n. By (2.5), $\mathscr{H}$ induces a (p^{t+1}, k)-PCP in any p-Sylow subgroup P of G. Hence we may assume that $H\cap P$ is a p-Sylow subgroup of H for all components H in $\mathscr{H}$ and obtain

$$\sum_{H\in\mathscr{H}} |H\cap P-\{1\}|=(p^{t+1}-1)\,k\leqslant |P-\{1\}|=p^{2t+2}-1.$$

Therefore $n\leqslant p+p^t$. If $t>0$ then $n=1$ as p is the smallest prime divisor of $|G|$ and p does not divide n by assumption. If $t=0$ then $n=p+1$ is a prime number and therefore $p=2$, $n=3$ and $|G|=36$. ▌

A. P. Sprague determined every (6, 3) translation net in [11] by presenting the corresponding PCPs. The translation group is one of the groups listed in (5.2)(i).

From now on we assume that G is a p-group of order p^{2n} and $n\geqslant 3$, as we dealt with the case $n=2$ extensively in Section 4.

If G is abelian then it must be elementary abelian by (3.3) and (3.4).

The case where $p=2$ and $n \geqslant 4$ is discussed in [4] (see (2.7) and (5.1)); then G is elementary abelian.

If $n=3$ and $p=2$ then G has order 64 and there exist exactly two groups which admit an (8, 4)-PCP, the elementary abelian group of order 64 or the group in (5.2)(iii) which does not contain an (8, 5)-PCP (see [5, 11]).

From now on we assume that p is odd, $n \geqslant 3$, and $\mathscr{H}$ is a (p^n, p^{n-1})-PCP in G, where G is nonabelian. Similar as in [4], we study G depending on the order ω of the elementary abelian subgroup $\Omega := \Omega_p(Z(G))$ of G.

The Case $\omega \geqslant p^{n+1}$. We regard Ω as a vector space over the field $GF(p)$ and choose any $(n+1)$-dimensional subspace V of Ω. For every component H of $\mathscr{H}$ we have $|H \cap V| \geqslant p$ with equality if and only if $G = HV$.

Assume that there are at least two components X and Y of $\mathscr{H}$ satisfying $|X \cap V| = |Y \cap V| = p$ with $\langle x \rangle = X \cap V$ and $\langle y \rangle = Y \cap V$. As $\langle x \rangle \cap \langle y \rangle = 1$ we can extend $\{x, y\}$ to a basis $(x, y, v_1, ..., v_{n-1})$ of V and look at the n-dimensional subspace $W = \langle xy, v_1, ..., v_{n-1} \rangle$ of V. By construction $X \cap W = Y \cap W = 1$ holds so that $\{W, X, Y\}$ is a $(p^n, 3)$-PCP in G. As W is a subgroup of $Z(G)$ the components W, X and Y are normal in G. Using (2.3) (iii) one obtains that G is abelian, a contradiction.

$\mathscr{H}$ contains therefore at least $p^{n-1}-1$ components H with $|H \cap V| \geqslant p^2$. Since at most one component is a subgroup of V, $\mathscr{H}$ leads to a GPCP $\{HV/V\colon H \in \mathscr{H}, |H \cap V| \geqslant p^2\}$ in G/V with parameter $a \leqslant n-2$ and at least $p^{n-1}-2$ components. Now (2.9)(i) implies $p^{n-1}-2 \leqslant p^{n-2} + \cdots + p + 1$, a contradiction to $p \neq 2$.

Under the assumptions we have proved

$$\omega \leqslant p^n. \tag{5.5}$$

Next, we calculate an upper bound for the order of the Frattini subgroup $\Phi(G)$ in G (see also [4, 8]).

$$|\Phi(G)| \leqslant p^n. \tag{5.6}$$

Proof. Each component of $\mathscr{H}$ lies in at least one maximal subgroup of G so that $G/\Phi(G)$ contains at least p^{n-1} maximal subgroups. As $G/\Phi(G)$ is elementary abelian, this leads (because of duality) to at least p^{n-1} one-dimensional subspaces in $G/\Phi(G)$. Therefore $|G/\Phi(G)| \geqslant (p-1)\, p^{n-1}+1$. As the order of $|G/\Phi(G)|$ is a power of p, we have the desired result. ∎

The Case $\omega \leqslant p^{n-2}$. Similar to [4] we study the set $\mathscr{A} := \{H \in \mathscr{H}\colon H \cap \Omega = 1\}$. Let $a := |\mathscr{A}|$. The number t of components which intersect Ω nontrivially is bounded by $(\omega-1)/(p-1)$ so that we have $a \geqslant p^{n-1} - (p^{n-2}-1)/(p-1)$.

Because of (3.3) and (3.1) there exist at least $a-1$ nonabelian components in $\mathscr{A}$ so that we have at least $a-1$ components H in $\mathscr{A}$ satisfying $\Phi(H)\neq 1$ and therefore $H\cap\Phi(G)\neq 1$. Let H be a nonabelian element of $\mathscr{A}$. By definition of $\mathscr{A}$, H contains no nontrivial normal subgroup of G as otherwise H would intersect $Z(G)$ and therefore Ω nontrivially. We calculate a lower bound for

$$\tau=|(H\cap\Phi(G))^G|=|\{h^g\colon h\in H,\ g\in G\}|.$$

The only difficult situation is when $H\cap\Phi(G)$ has order p. Let therefore $\langle x\rangle=H\cap\Phi(G)$ be a subgroup of order p. Of course $\tau>p$ holds since $\langle x\rangle$ is not normal in G. Assume first $x^i\in x^G$ for all $i=1, ..., p-1$, then $\tau=|x^G|\geqslant p^2$. Otherwise, x^i does not lie in the orbit of x for all $i=1, ..., p-1$ and thus $\tau\geqslant(p-1)\,p+1$. (Observe that x does not lie in the center of G!) In any case we can assume that $\tau\geqslant p^2-p+1$. Since $H^G\cap K^G=1$ for different components H and K in $\mathscr{H}$ (see (2.4)), we have that $\Phi(G)$ contains at least $(a-1)(\tau-1)+1$ elements. Using the lower bounds of a and τ given above, after some calculations one obtains a contradiction to (5.6).

We have proved

$$\omega\geqslant p^{n-1}. \tag{5.7}$$

We now show

$$\omega\neq p^{n-1}. \tag{5.8}$$

Proof. Assume $\omega=p^{n-1}$. As $p^{n-1}(p-1)+1>\omega$ there exists a component H of $\mathscr{H}$ which intersects Ω trivially. $H\Omega$ is a maximal subgroup of G, hence normal in G. Because $H\Omega$ is isomorphic to $H\times\Omega$ we have $\Phi(H\Omega)=\Phi(H)$. $\Phi(H)$ is a characteristic subgroup of $H\Omega$ and therefore a normal subgroup of G. The assumption $\Omega\cap H=1$ yields $\Phi(H)=1$ and therefore H is elementary abelian.

The number of components which intersect Ω nontrivially does not exceed $(p^{n-1}-1)/(p-1)$. Therefore the number r of (elementary) abelian components in $\mathscr{H}$ satisfies $r\geqslant p^{n-1}-(p^{n-1}-1)/(p-1)$. But (3.4) yields $r\leqslant p^{(n-1)/2}+1$. We have the desired contradiction. ▌

The Case $\omega=p^n$. Similarly to the preceding step we see that the existence of a component H satisfying $H\cap\Omega=1$ would imply that $G=H\Omega$ is elementary abelian. Thus $H\cap\Omega\neq 1$ for all $H\in\mathscr{H}$ and G/Ω contains at least p^{n-1} maximal subgroups, namely $\{H\Omega/\Omega\colon H\in\mathscr{H}\}$. Now the same argument as in the proof of (5.6) shows that G/Ω is elementary abelian. Therefore we obtain $G'\leqslant\Phi(G)\leqslant\Omega$ which yields that G is of class 2.

From now on, without explicitly stating it, we make use of the commutator formulas in (3.7).

Next, we prove that the center of G is equal to Ω and is therefore elementary abelian. Assume that $|Z(G)|\geqslant p^{n+1}$ and choose any subgroup

Z of $Z(G)$ of order p^{n+1}. Each component H of $\mathscr{H}$ satisfying $HZ=G$ is a normal subgroup of G so that (2.3)(iii) implies that $b:=|\{H\in\mathscr{H}: HZ=G\}|\leqslant 2$. Therefore at least $p^{n-1}-2$ components K of $\mathscr{H}$ have at least p^2 elements in common with Z. These components lead to a GPCP $\{KZ/Z: K\in\mathscr{H}, |K\cap Z|\geqslant p^2\}$ with parameter $a\leqslant n-2$. As a consequence of (2.9)(i) we have the contradiction $p^{n-1}-2\leqslant p^{n-2}+\cdots+p+1$.

An application of (3.7)(iii) and (3.8) shows now that G is of exponent p. Because of (3.3) $\mathscr{H}$ contains at least $p^{n-1}-p^{[n/2]}-1$ nonabelian components. We denote this set by $\mathscr{M}$. By definition every element H of $\mathscr{M}$ satisfies $H'\neq 1$. As $H'\leqslant G'$ we may calculate now $|G'|\geqslant|\mathscr{M}|(p-1)+1>p^{n-1}$ and therefore $|G'|\geqslant p^n$. By (5.6) and $G'\leqslant\Phi(G)$ we have $G'=\Phi(G)=Z(G)$.

In particular: G is a special group of order p^{2n} with exponent p and $|Z(G)|=p^n$.

Every subgroup U of G of order p^n intersects $\Phi(G)$ nontrivially, as otherwise $U\Phi(G)=G$ and therefore $G=U$, a consequence of the definition of the Frattini subgroup. We will now determine an upper bound for the maximal number of components in $\mathscr{H}$ which intersect the center of G in a one-dimensional subspace.

Let H be a component in $\mathscr{H}$ satisfying $|H\cap Z(G)|=p$, for example $H\cap Z(G)=\langle h\rangle$. We will see that the structure of G is very restricted:

Assume that H is abelian, then H is elementary abelian and we can choose $h_1, ..., h_{n-1}$ in H such that $(h_1, ..., h_{n-1}, h)$ is a basis of H. $HZ(G)$ is elementary abelian of order p^{2n-1}. For every x in $G-HZ(G)$ one obtains $G'=Z(G)=\langle[x, h_1], ..., [x, h_{n-1}]\rangle$ and therefore $\dim G'\leqslant n-1$ which contradicts $G'=Z(G)$.

This yields that H is nonabelian and $1\neq\Phi(H)=H'\leqslant H\cap Z(G)=\langle h\rangle$. By Burnside's basis theorem we can find $a_1, ..., a_{n-1}$ in H such that $\langle a_1, ..., a_{n-1}\rangle=H$ and $[a_1, a_2]=h$. Let Z_0 be a complement of $\langle h\rangle$ in $Z(G)$. $HZ(G)$ is isomorphic to $H\times Z_0$ and since Z_0 is elementary abelian of order p^{n-1} one has $\Phi(HZ(G))=\Phi(HZ_0)=\Phi(H)$. For every b in $G-HZ(G)$ we have furthermore $G'=\langle[b, a_1], ..., [b, a_{n-1}], [a_1, a_2]\rangle$ since $(HZ(G))'=H'=\langle[a_1, a_2]\rangle$.

$C_G(b)$, the centralizer of b in G, is equal to $\langle b, Z(G)\rangle$ and is an elementary abelian group of order p^{n+1}. Let K be a further component of $\mathscr{H}$ satisfying $|K\cap Z(G)|=p$ and without loss of generality. Let $b\in K$ (observe that there exists an element b in K which does not lie in $HZ(G)$, since otherwise H and K are subgroups of the proper subgroup $HZ(G)$ of G which contradicts $HK=G$). If we denote by z a generator of $\Phi(K)=K\cap Z(G)$, we obtain $C_G(b)\cap K=\langle b, z\rangle$. By Burnside's basis theorem every minimal set of generators of K contains $n-1$ elements. We can furthermore assume that b is one of the generators. Let K be generated by $b, y_1, ..., y_{n-2}$ where $[b, y_1]=z$.

If $n \geqslant 4$, the generator y_2 exists and is an element of $K - \langle b, y_1 \rangle$. Therefore y_2 does not centralize b. Since $K' = \langle z \rangle$ we may assume that $[b, y_2] = z$ and obtain $[b, y_1 y_2^{-1}] = [b, y_1][b, y_2]^{-1} = 1$ (see (3.7)). Therefore $y_1 y_2^{-1} \in C_G(b) \cap K = \langle b, z \rangle$ and one has $y_2 \in \langle b, z, y_1 \rangle = \langle b, y_1 \rangle$, a contradiction to the fact that y_2 together with b and y_1 belongs to a minimal set of generators of K.

We conclude that for $n \geqslant 4$ there is at most one component H satisfying $|H \cap Z(G)| = p$ and therefore at least $p^{n-1} - 1$ components L satisfying $|L \cap Z(G)| \geqslant p^2$. We obtain that $Z(G)$ contains at least $p + (p^{n-1} - 1)(p^2 - 1) > p^n$ elements, a contradiction, which completes the proof of (5.2).

To finish the proof of (5.3) it remains to check that $T(G) \leqslant p^2 + 1$, when G is special of order p^6 with exponent p and has a center of order p^3.

In determining $|H^G|$ for each subgroup H of G satisfying $|H \cap Z(G)| = p$ we prove that the maximum number of components in a PCP in G does not exceed $p^2 + 1$.

Observe that G is isomorphic to

$$\langle a, b, c, x, y, z \mid \text{all generators have order } p;\ [a, b] = x,\ [a, c] = y,\ [b, c] = z;\ \text{all further commutators are equal to } 1 \rangle.$$

As G is of class 2 one can use (3.7) and the presentation of G to show that $|g^G| = |G : C_G(g)| = p^2$ holds if and only if g does not lie in $Z(G)$. Furthermore $x^G \neq y^G$ if and only if $H \cap Z(G)\, x \neq H \cap Z(G)\, y$ for x, y in H. This leads to

$$|H^G| = |H \cap Z(G)| + (|H/H \cap Z(G)| - 1) \cdot p^2 = p^4 - p^2 + p,$$

if $|H \cap Z(G)| = p$. Now (2.4) yields $|\{H \in \mathscr{H} \colon |H \cap Z(G)| = p\}| \leqslant p^2$.

As at most one component intersects $Z(G)$ in a 2-dimensional subspace we obtain $|\mathscr{H}| \leqslant p^2 + 1$.

This completes the proof of (5.3). ▌

In the next section we show that for all odd prime numbers p there exists indeed a $(p^3, p^2 + 1)$-PCP in the special group of order p^6 with exponent p and center of order p^3.

We conclude this section summarizing our results in slightly different terminology to show that the bound in [9, Theorem 3.5] can be improved.

5.9. Corollary. *Let s be a positive integer with smallest prime divisor p. Then $T(s) \geqslant s/p$ if and only if $s = 6$ or s is a prime power.*

5.10. Corollary. *Let G be a group of order s^2 and p be the smallest prime dividing s. If $T(G) \geqslant s/p + 2$ then G is elementary abelian.*

5.11. COROLLARY. *Let p be a prime number and*

$$T^*(p^n) := \max\{T(G)\colon\ G \text{ a group of order } p^{2n},\ G \text{ not elementary abelian}\}.$$

Then

(i) $T^*(p^2) = p+1$,

(ii) $T^*(p^3) \leqslant p^2+1$, *if p is odd.*

(iii) $T^*(64) = 4$.

(iv) $T^*(p^n) < p^{n-1}$ *for $n \geqslant 4$.*

As a consequence of Theorem (6.4) below we see that $T^*(p^3) = p^2+1$ for all odd prime numbers p.

6. (p^3, p^2+1)-TRANSLATION NETS WITH NONABELIAN TRANSLATION GROUPS

In this section we examine the group

$$\langle a, b, c, x, y, z \mid \text{ all generators have order } p;\ [a, b] = x,\ [a, c] = y,\ [b, c] = z; \text{ all further commutators are equal to } 1\rangle$$

more carefully.

As in Section 5, p is an odd prime number. G is the special group of order p^6 with exponent p and a center of order p^3. We have proved that $T(G) \leqslant p^2+1$. In this section, we show that this bound is indeed sharp for all odd prime numbers p. Note that G is of class 2. Beside the commutator formulas in (3.7) we need the following lemma:

6.1. LEMMA. *Every element g in G can uniquely be written as*

$$g = a^\alpha b^\beta c^\gamma x^\xi y^\eta z^\zeta,$$

where $\alpha, \beta, \gamma, \xi, \eta, \zeta$ are elements of the finite field $GF(p)$ of order p.

Proof. Assume $a^{\alpha_1} b^{\beta_1} c^{\gamma_1} x^{\xi_1} y^{\eta_1} z^{\zeta_1} = a^{\alpha_2} b^{\beta_2} c^{\gamma_2} x^{\xi_2} y^{\eta_2} z^{\zeta_2}$. By (3.7) and the presentation of G we obtain

$$a^{\alpha_1-\alpha_2} = b^{\beta_2-\beta_1} c^{\gamma_2-\gamma_1} x^{\xi_2-\xi_1} y^{\eta_2-\eta_1} z^{\zeta_2-\zeta_1+\beta_1(\gamma_2-\gamma_1)}.$$

If $\alpha_1 \neq \alpha_2$ then a lies in $\langle b, c, \Phi(G)\rangle$ and therefore we obtain $G = \langle b, c, \Phi(G)\rangle = \langle b, c\rangle$, a contradiction. If $\beta_1 \neq \beta_2$ then $b \in U := \langle c, x, y, z\rangle$.

But U is elementary abelian of order p^4 which contradicts $[b, c] = z \neq 1$. As c is not an element of $Z(G)$ we obtain $\gamma_1 = \gamma_2$ and as (x, y, z) is a basis of $Z(G)$ we obtain as well $\xi_1 = \xi_2$, $\eta_1 = \eta_2$ and $\zeta_1 = \zeta_2$. ▌

Let $A, C \in GF(p)^*$ and $B \in GF(p)$. For all i, j in $GF(p)$ we define

$$H_{ij}(A, B, C) := \langle ac^{-j}z^{Ai+Bj}, bc^iy^{Cj}, xy^iz^j \rangle.$$

An easy commutator calculation (see (3.7)(iii)) shows

$$[ac^{-j}z^{Ai+Bj}, bc^iy^{Cj}] = xy^iz^j.$$

Furthermore $H_{ij}(A, B, C)$ is isomorphic to the extraspecial group $E(p^3)$ of order p^3 and exponent p. Similar to the proof of (6.1) one can show that each element g of $H_{ij}(A, B, C)$ can uniquely be written as

$$g = (ac^{-j}z^{Ai+Bj})^\alpha \, (bc^iy^{Cj})^\beta \, (xy^iz^j)^\gamma$$

with α, β, and $\gamma \in GF(p)$.

If we write $g \in H_{ij}(A\ B, C)$ in "standard" presentation of G we obtain

$$g = a^\alpha b^\beta c^{i\beta - j\alpha} x^\gamma y^{j\binom{\alpha}{2} + Cj\beta + i\gamma} z^{-i\binom{\beta}{2} + Ai\alpha + Bj\alpha + j\gamma + j\alpha\beta}. \tag{1}$$

6.2. PROPOSITION. *For every odd prime number p there exist $A, C \in GF(p)^*$ and $B \in GF(p)$ such that $\{H_{ij}(A, B, C)$: $i, j \in GF(p)\}$ is a (p^3, p^2)-PCP in G.*

Proof. Let i, j, k, and l be elements of $GF(p)$ and assume that $(i, j) \neq (k, l)$. Let g be an element of $H_{ij}(A, B, C) \cap H_{kl}(A, B, C)$. Then there exist elements α, β, γ, λ, μ, τ in $GF(p)$ such that

$$\begin{aligned} &a^\alpha b^\beta c^{i\beta - j\alpha} x^\gamma y^{j\binom{\alpha}{2} + Cj\beta + i\gamma} z^{-i\binom{\beta}{2} + Ai\alpha + Bj\alpha + j\gamma + j\alpha\beta} \\ &\quad = a^\lambda b^\mu c^{k\mu - l\lambda} x^\tau y^{l\binom{\lambda}{2} + Cl\mu + k\tau} z^{-k\binom{\mu}{2} + Ak\lambda + Bl\lambda + l\tau + l\lambda\mu}. \end{aligned} \tag{2}$$

By using (6.1) we obtain the following system of equations:

$$\alpha = \lambda \tag{3}$$

$$\beta = \mu \tag{4}$$

$$i\beta - j\alpha = k\mu - l\lambda \tag{5}$$

$$\gamma = \tau \tag{6}$$

$$j\binom{\alpha}{2} + Cj\beta + i\gamma = l\binom{\lambda}{2} + Cl\mu + k\tau \tag{7}$$

$$-i\binom{\beta}{2} + Ai\alpha + Bj\alpha + j\gamma + j\alpha\beta = -k\binom{\mu}{2} + Ak\lambda + Bl\lambda + l\tau + l\lambda\mu \tag{8}$$

By using (3), (4), and (6) we obtain

$$(i-k)\,\beta=(j-l)\,\alpha \tag{9}$$

$$(i-k)\,\gamma=(l-j)\left[\binom{\alpha}{2}+C\beta\right] \tag{10}$$

$$(i-k)\left[A\alpha-\binom{\beta}{2}\right]=(l-j)\;[\gamma+B\alpha+\alpha\beta] \tag{11}$$

from (5), (7), and (8).

Now define $s:=i-k$ and $t:=j-l$.

If $s=0$, then $t\neq 0$ because of the assumption $(i, j)\neq(k, l)$ and therefore we obtain $\alpha=0$, $\beta=0$, and $\gamma=0$ by (9), (10), (11), and the choice of A, B, and C. Hence $g=1$. Similarly, we obtain $g=1$, if $t=0$.

We are now going to study the case where $t\neq 0$ and $s\neq 0$. Let $r:=s/t$, then the equalities (9), (10), and (11) imply

$$\alpha=r\beta \tag{12}$$

$$-r\gamma=\binom{\alpha}{2}+C\beta \tag{13}$$

$$-r\left[A\alpha-\binom{\beta}{2}\right]=\gamma+B\alpha+\alpha\beta. \tag{14}$$

Now (12) in (13) yields

$$\gamma=-r^{-1}\binom{r\beta}{2}-r^{-1}C\beta \tag{15}$$

and (12) and (15) in (14) imply

$$-r\left[Ar\beta-\binom{\beta}{2}\right]=-r^{-1}\binom{r\beta}{2}-r^{-1}C\beta+Br\beta+r\beta^2. \tag{16}$$

After some simplifications, using that $r\neq 0$, we obtain that (16) is equivalent to

$$\left(r^3+\frac{1+2B}{2A}r^2+\frac{1}{2A}r-\frac{C}{A}\right)\beta=0. \tag{17}$$

If

$$f_{A,B,C}(\omega)=\omega^3+\frac{1+2B}{2A}\omega^2+\frac{1}{2A}\omega-\frac{C}{A}$$

is irreducible in $GF(p)[\omega]$, we obtain $\beta=0$ from (17) and therefore $\alpha=0$ and $\gamma=0$ from (12) and (13), respectively. This shows that $H_{ij}(A, B, C) \cap H_{kl}(A, B, C)=1$ for (i, j), (k, l) in $GF(p)^2$ whenever $(i, j) \neq (k, l)$.

If the polynomial $f_{A,B,C}$ is not irreducible, then it has a root in $GF(p)^*$. One can find therefore a nontrivial triple (α, β, γ) with arbitrarily chosen β in $GF(p)^*$ which solves our equalities (3) to (8) where $(i-k)/(j-l)$ is a root of $f_{A,B,C}$.

It remains to show that we can find $A, C \in GF(p)^*$ and $B \in GF(p)$ for a given odd prime number p such that $f_{A,B,C}$ is irreducible in $GF(p)$:

Since the mapping $\mu: GF(p) \rightarrow GF(p)$, $\omega \rightarrow \omega^3-\omega$ is not bijective, we always find an element $D(p)$ in $GF(p)^*$ such that $g_{D(p)}(\omega)=\omega^3-\omega-D(p)$ is irreducible in $GF(p)[\omega]$. If we choose $(A, B, C)=(-2^{-1}, -2^{-1}, -2^{-1}D(p))$, we obtain that $f_{A,B,C}=g_{D(p)}$ is irreducible. This completes the proof of (6.2). ▌

6.3. Proposition. *Define* $H_\infty := \langle c, y, z\rangle$. *Then* $H_\infty \cap H_{ij}(A, B, C)=1$ *for all* (i, j) *in* $GF(p)$ *for all choices of* A, B, *and* C *as in* (6.2).

Proof. Let $(i, j) \in GF(p)^2$, $A, C \in GF(p)^*$, $B \in GF(p)$, and $g \in H_\infty \cap H_{ij}(A, B, C)$. Using (1) we find $\alpha, \beta, \gamma, \lambda, \mu, \tau$ in $GF(p)$ such that

$$\begin{aligned} &a^\alpha b^\beta c^{i\beta-j\alpha} x^\gamma y^{j\binom{\alpha}{2}+Cj\beta+i\gamma} z^{-i\binom{\beta}{2}+Ai\alpha+Bj\alpha+j\gamma+j\alpha\beta} \\ &\quad = c^\lambda y^\mu z^\tau. \end{aligned}$$

Using (6.1) one obtains $\alpha=\beta=\gamma=0$ and therefore $g=1$. ▌

A direct consequence of (6.2), (6.3), and (5.3) is

6.4. Theorem. *Let p be an odd prime number, G the special group of order p^6, of exponent p and center of order p^3. Then there exists a (p^3, p^2+1)-PCP in G. Furthermore $T(G)=p^2+1$.*

References

1. M. Aschbacher, "Finite Group Theory," Cambridge Univ. Press, Cambridge, 1986.
2. R. A. Bailey and D. Jungnickel, Translation nets and fixed-point-free group automorphisms, *J. Combin. Theory Ser. A* **55** (1990), 1–13.
3. J. Dillon, Elementary Hadamard difference sets, *in* "Proceedings, 6th Southeastern Conference on Combinatorics, Graph Theory and Computing," pp. 237–249, Utilitas Math., Winnipeg, 1975.
4. D. Frohardt, Groups with a large number of large disjoint subgroups, *J. Algebra* **107** (1987), 153–159.
5. D. Gluck, Hadamard difference sets in groups of order 64, *J. Combin. Theory Ser. A* **51** (1989), 138–141.

6. D. HACHENBERGER AND D. JUNGNICKEL, Bruck nets with a transitive direction, *Geom. Dedicata* **36** (1990), 287–313.
7. B. HUPPERT, "Endliche Gruppen I," Springer, Berlin–Heidelberg–New York, 1967.
8. D. JUNGNICKEL, Existence results for translation nets, *in* "Finite Geometries and Designs," London Math. Soc. Lecture Notes, Vol. 49, pp. 172–196, Cambridge Univ. Press, 1981.
9. D. JUNGNICKEL, Existence results for translation nets II, *J. Algebra* **122** (1989), 288–298.
10. D. JUNGNICKEL, Latin squares, their geometries and their groups. A survey, *in* "Coding Theory and Design Theory II" (D. K. Ray-Chaudhuri, Ed.), pp. 166–225, Springer, Berlin/New York, 1990.
11. A. P. SPRAGUE, Translation nets, *Mitt. Math. Sem. Giessen* **157** (1982), 46–68.
12. M. SUZUKI, "Group Theory I/II," Springer, New York–Berlin–Heidelberg–Tokyo, 1980/86.