

# Constructions of Large Translation Nets with Nonabelian Translation Groups

DIRK HACHENBERGER

*Mathematisches Institut der Justus—Liebig—Universität Giessen Arndtstrasse 2, D—6300 Giessen, F.R. Germany*

Communicated by D. Jungnickel

Received January 18, 1991. Revised February 7, 1991

**Abstract.** In this paper the first infinite series of translation nets with nonabelian translation groups and a *large* number of parallel classes are constructed. For that purpose we investigate partial congruence partitions (PCPs) with at least one normal component.

Two series correspond to partial congruence partitions containing one normal elementary abelian component. The construction results by using some basic facts about the first cohomology group of the translation group  $G$  regarded as an extension of the normal component which itself is a group of central translations.

The other series correspond to partial congruence partitions containing two normal nonabelian components. The constructions are based on the well known automorphism method which leads to so-called splitting translation nets. By investigating the Suzuki groups  $Sz(q)$ , the projective unitary groups  $PSU(3, q^2)$  and the Ree groups  $R(q)$  as doubly transitive permutation groups, we obtain examples of nonabelian groups admitting a large number of pairwise orthogonal fixed-point-free group automorphisms.

## 1. Large Translation Nets—An Introduction

Let  $s > 1$  be an integer and  $G$  a group of order  $s^2$ . Each set  $\mathbf{H} := \{H_1, \dots, H_r\}$  of  $r \geq 3$  subgroups of  $G$  satisfying

$$|H_i| = s \text{ for all } i = 1, \dots, r \text{ and} \quad (1.1)$$

$$H_i H_j = G \text{ for all } i \neq j \quad (1.2)$$

is called a *partial congruence partition* in  $G$  of order  $s$  and degree  $r$  (for short an  $(s, r)$ -PCP in  $G$ ). The members of  $\mathbf{H}$  are called *components*. Because of (1.1) the property (1.2) is equivalent to

$$H_i \cap H_j = 1 \text{ for all } i \neq j. \quad (1.2a)$$

Partial congruence partitions are studied by many authors (see (Bailey and Jungnickel 1990; Frohardt 1987; Gluck 1989; Hachenberger 1991; Hachenberger and Jungnickel 1990; Jungnickel 1981; Jungnickel 1989; Jungnickel 1989a; Sprague 1982)) because of their close relation to *translation nets*.

Given an  $(s, r)$ -PCP  $\mathcal{IH}$  in  $G$  the incidence structure

$$N(\mathcal{IH}) := (G, \{Hg : H \in \mathcal{IH}, g \in G\}, \epsilon) \quad (1.3)$$

is a translation net of order  $s$  and degree  $r \geq 3$ , that is an *affine 1-design*  $N$  with parameters  $s$  and  $r$  together with a *translation group*  $G$  acting sharply transitively on the set of points of  $N$  and fixing each of the  $r$  parallel classes. Conversely every translation net can be constructed in this way—hence the existence of an  $(s, r)$ -PCP in  $G$  is equivalent to the existence of an  $(s, r)$ -translation net with translation group  $G$ . In particular the number of components is equal to the number of parallel classes (the degree) of the corresponding translation net. (All definitions and more details can be found in (Beth, Jungnickel and Lenz 1986) and (Jungnickel 1990). The latter is a survey on Latin squares, their geometries and their groups.)

It is well known that the degree  $r$  of a net is at most  $s + 1$  with equality if and only if the incidence structure is an *affine plane of order*  $s$ . Thus  $(s, s + 1)$ -translation nets are called *translation planes* (see (Lüneburg 1980)) for an extensive treatment of this topic). Since translation planes have elementary abelian translation groups, the order  $s$  is a prime power in this case.

The main problem in the area of partial congruence partitions is the determination of the number

$$T(G) := \max\{r \leq s + 1 : \text{there exists an } (s, r)\text{-PCP in } G\}, \quad (1.4)$$

or to find at least upper or lower bounds for this number. ( $G$  is any group of order  $s^2$ .)

Since any  $(s, r)$ -PCP in  $G$  induces a PCP with the same number  $r$  of components in each Sylow subgroup of  $G$ , a fact which was first proved implicitly by Frohardt (1987), we are mainly interested in the case, where  $G$  is a  $p$ -group for some prime number  $p$ . Note that we have

$$T(G) = p^n + 1, \text{ if } G \text{ is elementary abelian of order } p^{2n}. \quad (1.5)$$

We are now going to summarize recent results on  $p$ -groups which show how far a translation net is from being a translation plane, provided that the translation group is not elementary abelian.

**THEOREM 1.** Let  $G$  be a group of order  $p^{2n}$ . If  $G$  is not elementary abelian, then

$$T(G) < p^{n-1}, \text{ if } n \geq 4; \quad (1.6)$$

$$T(G) \leq p^{n-1} + 1, \text{ if } p \text{ is odd and } n \in \{2, 3\} \text{ or if } p = n = 2; \quad (1.7)$$

$$T(G) \leq 4, \text{ if } G \text{ is of order } 64. \quad (1.8)$$

(1.6) is proved in (Frohardt 1987) and (Hachenberger 1991) where the cases  $p = 2$  and  $p$  odd are handled respectively. (1.7) is proved in (Hachenberger 1991), (1.8) in (Sprague 1982) and (Gluck 1989).

In the present paper, we complement these results by showing that there exist nonabelian  $p$ -groups of order  $p^{2^n}$  which have a *large* number of mutually disjoint subgroups of order  $p^n$ . We will explain the expression *large* in the following:

Some applications of a factorization lemma in (Hachenberger 1991) show that the number  $r$  of components of a partial congruence partition in a group  $G$  is much smaller than the bound in (1.6) provided that some assumptions on the structure of  $G$  or on the components themselves are made. If for example  $G$  is abelian of order  $p^{2^n}$ , but not elementary abelian, we have

$$T(G) \leq p^{\lceil n/2 \rceil} + 1 \quad (\text{where } \lceil n/2 \rceil := \max\{k \in \mathbb{N}: k \leq n/2\}). \quad (1.9)$$

This bound is for example sharp when  $G = Z_{p^2}^m \times Z_{p^2}^m$  and  $n = 2m$ . Therefore  $(Z_{p^2}^m \times Z_{p^2}^m)_{m \in \mathbb{N}}$  is a series of groups containing partial congruence partitions with degree  $p^m + 1 = \sqrt[4]{|G|} + 1$  which is best possible by (1.9). Until now no comparable result is known in the nonabelian case. The only known examples for nonabelian  $p$ -groups with  $T(G) \geq \sqrt[4]{|G|} + 1$  arise from the classification of the groups which satisfy equality in (1.7) and (1.8) (see (Hachenberger 1991) and (Gluck 1989; Sprague 1982) respectively). But these examples are sporadic in the sense that the groups have order at most  $p^6$ —the parameter  $n$  is 2 or 3 and therefore bounded. In Sections 3 and 4 we construct the first *series* of PCPs in nonabelian groups which—comparing degrees—can compete with the abelian example mentioned above. More precisely, we prove

**THEOREM 2.** There exist

$(q^2, q + 1)$ —PCPs with one normal elementary abelian component in a certain nonabelian group of order  $q^4$ , where  $q$  is any odd prime power; (1.10)

$(q^3, q^2 + 1)$ —PCPs with one normal elementary abelian component in a certain nonabelian group of order  $q^6$ , where  $q$  is any odd prime power; (1.11)

$(q^2, (q - 1) \cdot \gcd(q - 1, 2)^{-1} + 2)$ —PCPs containing two normal nonabelian components in a certain nonabelian group of order  $q^4$ , where  $q = p^n$  is a prime power and  $n$  is not a power of 2. (1.12)

$(q^3, q + 1)$ —PCPs containing two normal nonabelian components in a certain nonabelian group of order  $q^6$ , where  $q$  is any prime power. (1.13)

We say that these PCPs have a *large* number of components. The corresponding translation nets and translation groups are as well called *large*.

If  $G$  is one of the groups in (1.10) (or (1.12) provided that  $q$  is a power of 2) then  $T(G) \geq \sqrt[4]{|G|} + 1$ , the bound in (1.9). If  $G$  is one of the groups in (1.11), we even have  $T(G) \geq \sqrt[3]{|G|} + 1$  which is much better than what is possible in the abelian but not elementary abelian case. In (1.13) we have  $T(G) \geq \sqrt[6]{|G|} + 1$  which is weaker than (1.9) but nevertheless we call  $G$  large.

All these series are constructed by using the fact that we have at least one normal component. In Section 2 we will therefore make some general remarks on PCPs containing at least one normal component. Many of the results in Section 2 are implicit in (Hachenberger and Jungnickel 1990) but for the convenience of the reader and due to the fact that they are crucial for our constructions in Sections 3 and 4 we will summarize them.

## 2. On Central Translations and Partial Congruence Partitions Containing at Least One Normal Component

Let  $\mathcal{IH}$  be an  $(s, r)$ -partial congruence partition ( $r \geq 3$ ) in a group  $G$  of order  $s^2$  and let  $A \in \mathcal{IH}$  be a normal subgroup of  $G$ . We say that  $A$  is a *normal component* in  $\mathcal{IH}$ . Consider the parallel class  $P_A = \{Ag \mid g \in G\}$  corresponding to the component  $A$  in the net  $N(\mathcal{IH})$  (see (1.3)). Then  $A$  fixes as a collineation group of  $N(\mathcal{IH})$  every line of  $P_A$  and acts regularly on the points of each line in  $P_A$ . Hence  $A$  consists of *central translations* of  $P_A$ . Therefore  $N(\mathcal{IH})$  is called  *$P_A$ -transitive*. In (Hachenberger and Jungnickel 1990) such types of translation nets, called *semi-splitting translation nets*, are studied under a geometric point of view and in relation to *difference matrices*. (All definitions above can be found in (Hachenberger and Jungnickel 1990), but we will not use them here.)

If  $H$  is any component different from  $A$  in  $\mathcal{IH}$ , then  $G$  is isomorphic to a semidirect product  $S(A, H, \pi)$ , where  $\pi : H \rightarrow \text{Aut}(A)$  denotes the corresponding representation of  $H$  as an automorphism group of  $A$  ( $\pi(h)$  can be viewed as conjugation of  $A$  by  $h$ ). For any component  $U$  in  $\mathcal{IH} - \{A, H\}$ , we define  $\varphi_U : H \rightarrow A$  in the following way: Let  $\varphi_U(h)$  be the unique element in  $A$  such that  $h \in U\varphi_U(h)^{-1}$ . By (1.2.a)  $A$  is a complete class of representatives of right cosets of  $U$  in  $G$ . Furthermore, each  $h$  in  $H$  lies in exactly one coset of  $U$ . Hence  $\varphi_U$  is well-defined and a bijection between  $H$  and  $A$ . Moreover we have  $U = \{h\varphi_U(h) \mid h \in H\}$ . Because of the normality of  $A$  in  $G$  and the fact that different components have only trivial intersection, the set  $\Phi := \{\varphi_U \mid U \in \mathcal{IH} - \{A, H\}\}$  has the following properties:

$$\vartheta(U, V) : H \rightarrow A, h \mapsto \varphi_U(h)^{-1} \varphi_V(h) \text{ is bijective if and only if } U \neq V, \quad (2.1)$$

$$\varphi_U(h_1 h_2) = \varphi_U(h_1)^{\pi(h_2)} \varphi_U(h_2) \quad \text{for all } h_1, h_2 \text{ in } H. \quad (2.2)$$

In (Hachenberger and Jungnickel 1990)  $\Phi$  is called a *system of pairwise orthogonal semi-isomorphisms from  $H$  onto  $A$* . (In contrast to (Hachenberger and Jungnickel 1990) all groups are written multiplicatively here.) Furthermore, it is proved there (see theorem 4.10) that the converse as well is true, hence:

$$\begin{aligned} &\text{Let } H \text{ and } A \text{ be groups of order } s \text{ and } \pi : H \rightarrow \text{Aut}(A) \text{ a representation of} \\ &H \text{ as an automorphism group of } A. \text{ The existence of a system } \Phi \text{ of pairwise} \\ &\text{orthogonal semi-isomorphisms from } H \text{ onto } A \text{ is equivalent to the existence} \\ &\text{of an } (|H|, |\Phi| + 2)\text{-PCP in the semidirect product } G = S(A, H, \pi) \text{ contain-} \\ &\text{ing the subgroups } H \text{ and } A \text{ as components.} \end{aligned} \quad (2.3)$$

If  $A$  is an abelian group, then mappings satisfying condition (2.2) are of certain interest in algebra. They are called *cocycles* in this case and (2.2) is known as *cocycle-condition* (see (Aschbacher 1986; Huppert 1967; Huppert and Blackburn 1982; Huppert and Blackburn 1983) as references for the results from group theory we use here). Cocycles are very important by studying the *first cohomology group*  $H^1(A, H)$  of the extension  $G$  of  $A$  by  $H$  with respect to  $\pi$ . In Section 3 we use some basic facts about the cohomology of groups when among other things we are going to discuss how partial congruence partitions containing an abelian normal component  $A$  can be represented in terms of certain automorphisms of  $G = S(A, H, \pi)$ .

If  $H$  as well is a normal subgroup of  $G$ , then  $\pi$  is the trivial representation of  $H$  on  $\text{Aut}(A)$ . Since  $r \geq 3$  it is not difficult to see that  $H$  is isomorphic to  $A$  and therefore  $G$  is isomorphic to  $A \times A$ . The set  $\Phi$  of semi-isomorphisms then is a set of automorphisms of  $A$ . Assume that besides  $A \times 1$  and  $1 \times A$  the diagonal  $\{(a, a) : a \in A\}$  as well is a member of  $\text{IH}$ , which is equivalent to the fact that the identity is in  $\Phi$ , then  $\Phi$  becomes a set of *pairwise orthogonal fixed-point-free group automorphisms of  $A$* . (Note that two fixed-point-free automorphisms  $\varphi$  and  $\eta$  of  $A$  are called orthogonal, if  $\varphi^{-1}\eta$  is also fixed-point-free. We consider the identity as well as fixed-point-free.) As in (Bailey and Jungnickel 1990) we define

$$f(A) := \text{maximal number of pairwise orthogonal fixed-point-free group automorphisms of } A \text{ containing the identity.} \quad (2.4)$$

Translation nets constructed with this automorphism method are called *splitting translation nets* in (Bailey and Jungnickel 1990). By (2.3) it is clear that

$$T(A \times A) \geq f(A) + 2. \quad (2.5)$$

We mention that we do not know any example where equality does *not* hold in (2.5). However, if  $\text{IH}$  contains at least three normal components, it is not difficult to show that  $G$  is abelian (see (Sprague 1982)), hence all components are normal and we have always equality in (2.5). The abelian case is completely solved by Bailey and Jungnickel (1990):

**THEOREM 3.** Let  $A$  be an abelian  $p$ -group of the form  $Z_{p^{m_a}} \times \dots \times Z_{p^{m_1}}$ , where  $m_a \neq 0$ . Then  $f(A) + 2 = T(A \times A) = p^m + 1$ , where  $m = \min\{m_i | i = 1, \dots, a, m_i \neq 0\}$ .

If  $A$  is as in Theorem 3 then a maximal set of mutually orthogonal fixed-point-free automorphisms of  $A$  can directly be constructed by using a method developed by Jungnickel (1989a) together with a direct product construction, a basic recursive method (see for example (Jungnickel 1990)).

As the abelian case is completely solved, we give examples of nonabelian groups with a large number of pairwise orthogonal fixed-point-free group automorphisms in Section 4 and prove (1.12) and (1.13). The series in (1.12) with  $q$  even and (1.13) are examples, where  $f(A)$  is indeed as large as possible—there exists always a characteristic subgroup  $C$  of  $A$  of order  $f(A) + 1$ . (It is easy to see that  $f(A) \leq |S| - 1$ , where  $S$  is any characteristic section of  $A$ —see again (Bailey and Jungnickel 1990).)

### 3. Partial Congruence Partitions Containing One Normal Abelian Component

In this section we summarize some basic facts about the cohomology of groups (see (Aschbacher 1986, § 17)) and use them later to show how partial congruence partitions in a group  $G$  containing one normal abelian component  $A$  can be described in terms of certain sets of automorphisms of  $G$  which fix  $A$  and  $G/A$  elementwise.

Let  $A$  be a finite abelian group and let  $\pi : H \rightarrow \text{Aut}(A)$  be a representation of the finite group  $H$  as an automorphism group of  $A$ . Again let  $G := S(A, H, \pi)$  be the corresponding semidirect product of  $A$  by  $H$  with respect to  $\pi$ . We write  $G$  multiplicatively and as usually assume that  $A$  and  $H$  are subgroups of  $G$  and that  $\pi$  is the conjugation of  $A$  by elements of  $H$ . Let  $\Gamma(H, A)$  be the set of cocycles from  $H$  into  $A$ , that is (as in (2.2)) the set of mappings  $\gamma : H \rightarrow A$  satisfying the cocycle condition

$$\gamma(h_1 h_2) = \gamma(h_1)^{h_2} \gamma(h_2) \quad \text{for all } h_1, h_2 \text{ in } H. \quad (3.1)$$

$$\begin{aligned} \Gamma(H, A) \text{ is an abelian group with respect to pointwise multiplication:} \\ (\delta\gamma)(h) := \delta(h) \gamma(h), \text{ for all } \delta, \gamma \in \Gamma(H, A) \text{ and all } h \in H. \end{aligned} \quad (3.2)$$

$$\begin{aligned} \text{There is a one-to-one correspondence between } \Gamma(H, A) \text{ and the set } C \text{ of} \\ \text{complements of } A \text{ in } G; \\ C = \{S_\gamma : \gamma \in \Gamma(H, A)\}, \text{ where } S_\gamma := \{h\gamma(h) : h \in H\}. \end{aligned} \quad (3.3)$$

The mapping

$$\begin{aligned} \Delta : \Gamma(H, A) &\rightarrow \text{Aut}(G) \\ \gamma &\mapsto \Delta_\gamma : G \rightarrow G, ha \mapsto h\gamma(h)a \end{aligned} \quad (3.4)$$

is a monomorphism from  $\Gamma(H, A)$  into  $\text{Aut}(G)$  (note that every element  $g$  in  $G$  can uniquely be written as  $ha$  with  $h \in H$  and  $a \in A$ ). Moreover the image of  $\Gamma(H, A)$  under  $\Delta$  consists exactly of the automorphisms of  $G$  which fix  $A$  and  $G/A$  elementwise:

$$\begin{aligned} U(H, A) := \Delta(\Gamma(H, A)) &= \{\varphi \in \text{Aut}(G) : \varphi(a) = a \text{ for all } a \text{ in } A, \\ &\varphi(hA) = hA \text{ for all } h \text{ in } H\}. \end{aligned} \quad (3.5)$$

$$\begin{aligned} \text{Because of (3.3) } U(H, A) \text{ acts regularly on the set of complements of } A \text{ in} \\ G \text{—each complement of } A \text{ in } G \text{ is of the form } \varphi(H) \text{ where } \varphi \in U(H, A). \end{aligned} \quad (3.6)$$

Since  $\varphi(hA) = hA$  for all  $h \in H$  and all  $\varphi \in U(H, A)$ , we see that  $\varphi(h) = ha$  for some  $a$  in  $A$ . Therefore  $\varphi(h) = ha \in H \cap \varphi(H)$  if and only if  $\varphi(h) = h$ . We have:

$$\begin{aligned} \text{For every } \varphi \in U(H, A) \text{ the intersection } \varphi(H) \cap H \text{ is exactly the set of} \\ \text{elements in } H \text{ fixed by } \varphi. \end{aligned} \quad (3.7)$$

By applying these results to partial congruence partitions, observing that  $|\varphi(H) \cap \eta(H)| = |\eta^{-1}\varphi(H) \cap H|$  for all automorphisms  $\varphi$  and  $\eta$  of  $G$  and using (2.3) we obtain the following correspondence:

Let  $G$  be a group of order  $s^2$ ,  $A$  a normal abelian subgroup of  $G$  of order  $s$  and  $H$  a complement of  $A$  in  $G$ . An  $(s, r)$ -PCP  $\text{IH}$  in  $G$  containing  $H$  and  $A$  as components exists if and only if there exists a subset  $\Phi$  of  $U(H, A)$  of cardinality  $r - 1$  satisfying the following properties: (3.8)

The identity of  $G$  is an element of  $\Phi$ ; (3.8.a)

$\eta^{-1}\varphi(H) \cap H = 1$  for any two different automorphisms  $\varphi$  and  $\eta$  in  $\Phi$ . (3.8.b)

The PCP corresponding to  $\Phi$  is the set  $\text{IH}(\Phi) := \{\varphi(H) : \varphi \in \Phi\} \cup \{A\}$ .

Note that (3.8.b) is equivalent to

$\varphi(H) \cap \eta(H) = 1$  for any two different automorphisms  $\varphi$  and  $\eta$  in  $\Phi$ .) (3.8.c)

Before discussing some examples and proving (1.10) and (1.11), we mention that if  $c : A \rightarrow \text{Aut}(G)$  is the conjugation of  $G$  by elements of  $A$ , then  $c(A)$  is a subgroup of  $U(H, A)$  (note that  $A$  is assumed to be abelian). The first cohomology group  $H^1(H, A)$  of the extension  $G$  of  $A$  by  $H$  with respect to  $\pi$  is defined as the factor group  $U(A, H)/_{c(A)}$ . There is a one-to-one correspondence between  $H^1(H, A)$  and the set of conjugacy classes of complements of  $A$  in  $G$  (see again (Aschbacher 1986, § 17)).

**CONSTRUCTION 1.**  $(q^2, q + 1)$ -PCPs in certain nonabelian groups of order  $q^4$ , where  $q$  is any odd prime power.

Let  $q$  be an odd prime power and let  $GF(q)$  denote the Galois field of order  $q$  with characteristic  $p$ . We define a multiplication on the set  $G$  of 4-tuples over  $GF(q)$ :

$$(a_1, b_1, c_1, d_1)(a_2, b_2, c_2, d_2) := (a_1 + a_2, b_1 + b_2, c_1 + c_2 - a_2b_1, d_1 + d_2). \quad (3.9)$$

It is not difficult to show that  $G$  together with this multiplication becomes a group. Furthermore

$$(a, b, c, d)^{-1} = (-a, -b, -c - ab, -d) \quad \text{and} \quad (3.10)$$

$$[(a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2)] = (0, 0, a_1b_2 - a_2b_1, 0). \quad (3.11)$$

(As usually  $[x, y]$  denotes the commutator of  $x$  and  $y$ .)

We summarize some facts about the structure of  $G$  and skip the details since they all can easily be verified by using (3.9), (3.10) and (3.11).

$G$  is nonabelian of order  $q^4$  and exponent  $p$ . The center and the derived subgroup of  $G$  are  $Z(G) = \{(0, 0, c, d) : c, d \in GF(q)\}$  and  $G' = \{(0, 0, c, 0) : c \in GF(q)\}$  respectively. Since  $G' \leq Z(G)$ ,  $G$  is nilpotent of class two.

We define a multiplication of elements of  $G$  by elements of  $GF(q)$ :

$$\begin{aligned} * : GF(q) \times G &\rightarrow G, \\ (\lambda, (a, b, c, d)) &\mapsto [\lambda a, \lambda b, \lambda c - \binom{\lambda}{2} ab, \lambda d], \\ \text{where } \binom{\lambda}{2} &:= 2^{-1}\lambda(\lambda - 1). \end{aligned} \quad (3.12)$$

For the sake of simplicity we write  $\lambda(a, b, c, d)$  instead of  $*(\lambda, (a, b, c, d))$ . As  $G$  is of class 2, the commutator mapping

$$[\cdot, \cdot] : G \times G \rightarrow G', (x, y) \mapsto [x, y] = x^{-1} y^{-1} xy$$

is “bilinear” and skew-symmetric with respect to  $*$ , that is

$$\begin{aligned} [(\lambda x)(\mu z), y] &= (\lambda[x, y])(\mu[z, y]), \\ [x, (\lambda y)(\mu z)] &= (\lambda[x, y])(\mu[x, z]) \quad \text{and} \\ [y, x] &= (-1)[x, y] = [x, y]^{-1} \text{ hold for all } x, y, z \text{ in } G \text{ and all } \lambda, \mu \text{ in } GF(q). \end{aligned} \quad (3.13)$$

Let  $E_1 := (1, 0, 0, 0)$ ,  $E_2 := (0, 1, 0, 0)$ ,  $E_3 := (0, 0, 1, 0)$  and  $E_4 := (0, 0, 0, 1)$ . Then

$$(a, b, c, d) = (aE_1)(bE_2)(cE_3)(dE_4). \quad (3.14)$$

Hence, similar to the 4-dimensional vector space  $V(4, q)$  over  $GF(q)$ , we can think of  $G$  as a group consisting of all “linear combinations” of  $E_1, E_2, E_3$  and  $E_4$ , though  $*$  does of course not satisfy the axioms of a scalar multiplication.

Now let  $A := \{(a, 0, c, 0) : a, c \in GF(q)\} = \{(aE_1)(cE_3) : a, c \in GF(q)\}$  and  $H := \{(0, b, 0, d) : b, d \in GF(q)\} = \{(bE_2)(dE_4) : b, d \in GF(q)\}$ . Both  $A$  and  $H$  are elementary abelian subgroups of  $G$  which additionally are invariant under the multiplication with elements of  $GF(q)$ . They have order  $q^2$  and trivial intersection. Since  $G' \leq A$  we see that  $A$  is a normal subgroup of  $G$  and  $G$  is isomorphic to a semidirect product of  $H$  with  $A$ . As above let  $U(H, A)$  be the group of automorphisms of  $G$  fixing  $A$  and  $G/A$  elementwise.

We are now going to construct a subgroup of  $U(H, A)$ :

If  $\tau \in U(H, A)$ , then  $E_1^\tau = E_1$ ,  $E_3^\tau = E_3$  and  $E_2^\tau, E_4^\tau$  are of the form  $(\alpha E_1)E_2(\gamma_1 E_3) = (\alpha, 1, \gamma_1, 0)$  and  $(\gamma_2 E_3)E_4 = (0, 0, \gamma_2, 1)$  respectively for some  $\alpha, \gamma_1, \gamma_2 \in GF(q)$ . The restriction that  $E_4^\tau$  has no  $E_1$ -coordinate follows from the observation that  $E_4$  lies in  $H \cap Z(G)$  and that therefore  $E_4^{-1}E_4^\tau$  has to be an element of  $A \cap Z(G) = G'$ .

We choose therefore  $\alpha, \gamma_1$  and  $\gamma_2$  in  $GF(q)$  arbitrarily, define  $\tau := \tau(\alpha, \gamma_1, \gamma_2)$  on the set  $\{E_1, E_2, E_3, E_4\}$  in the above manner and extend  $\tau$  to an automorphism in  $U(H, A)$  by defining



$$(a, b, c, d)^\tau := (aE_1^\tau)(bE_2^\tau)(cE_3^\tau)(dE_4^\tau). \quad (3.15)$$

More precisely, we obtain:

Let  $\alpha, \gamma_1, \gamma_2 \in GF(q)$ . The mapping

$$\tau(\alpha, \gamma_1, \gamma_2) : G \mapsto G,$$

$$(a, b, c, d) \mapsto \left[ a + \alpha b, b, \gamma_1 b - \alpha \begin{pmatrix} b \\ 2 \end{pmatrix} + c + \gamma_2 d, d \right]$$

$$\text{is an element of } U(H, A). \quad (3.16)$$

Moreover,

$T := \{ \tau(\alpha, \gamma_1, \gamma_2) : \alpha, \gamma_1, \gamma_2 \in GF(q) \}$  is an elementary abelian subgroup of order  $q^3$  of  $U(H, A)$  with respect to  $\tau(\alpha, \gamma_1, \gamma_2) \tau(\beta, \delta_1, \delta_2) := \tau(\alpha + \beta, \gamma_1 + \delta_1, \gamma_2 + \delta_2)$ . Furthermore every  $\tau$  in  $T$  respects multiplication by scalars, i.e.,  $(\lambda g)^\tau = \lambda(g^\tau)$  for all  $g \in G$  and all  $\lambda \in GF(q)$ . (3.17)

In view of (3.8) we want to find a subset  $\Phi$  of  $T$ , as large as possible satisfying (3.8.a) and (3.8.b). We therefore have to examine when  $\tau \in T$  has a fixed point in  $H$ . The equation  $(0, b, 0, d)^{\tau(\alpha, \gamma_1, \gamma_2)} = (0, b, 0, d)$  leads to the system

$$\alpha b = 0,$$

$$-\alpha \begin{pmatrix} b \\ 2 \end{pmatrix} + \gamma_1 b + \gamma_2 d = 0. \quad (3.18)$$

If we choose now for example

$$\Phi := \{ \tau(\lambda, 0, \lambda) : \lambda \in GF(q) \}, \quad (3.19)$$

then  $\tau(\lambda, 0, \lambda)$  has a nontrivial fixed-point in  $H$  if and only if  $\lambda = 0$ . As  $\Phi$  is a subgroup of  $T$  the conditions (3.8.a) and (3.8.b) are satisfied automatically and we obtain:

$$\{ H^{\tau(\lambda, 0, \lambda)} : \lambda \in GF(q) \} \cup \{ A \} \text{ is a } (q^2, q + 1)\text{-PCP in } G. \quad (3.20)$$

This proves (1.10).

We finally show that no PCP IH in  $G$  containing  $A$  can have more than  $q + 1$  components and that therefore the choice of  $\Phi$  above is best possible:

Every other component in  $\text{IH} - \{A\}$  is isomorphic to  $G/A$ , hence elementary abelian of order  $q^2$  (since  $G' \leq A$  and  $\exp(G) = p$ ). An application of a factorization lemma in (Hachenberger 1991) now shows that each component of  $\text{IH}$  meets  $Z(G)$  in a subgroup of order  $q$  and since  $Z(G)$  has order  $q^2$  these intersections build a PCP in  $Z(G)$  with the same number of components. As  $Z(G)$  is elementary abelian we have  $T(Z(G)) = q + 1$  by (1.5), hence  $|\text{IH}| \leq q + 1$ .

CONSTRUCTION 2.  $(q^3, q^2 + 1)$ -PCPs in certain nonabelian groups of order  $q^6$ , where  $q$  is any odd prime power.

Again let  $q$  be an odd prime power and let  $GF(q)$  denote the Galois field of order  $q$  with characteristic  $p$ . Now we define a multiplication on the set  $G$  of 6-tupels over  $GF(q)$  and proceed in a similar way as in Construction 1.

$$\begin{aligned} (a_1, b_1, c_1, x_1, y_1, z_1)(a_2, b_2, c_2, x_2, y_2, z_2) := \\ (a_1 + a_2, b_1 + b_2, c_1 + c_2, x_1 + x_2 - a_2b_1, \\ y_1 + y_2 - a_2c_1, z_1 + z_2 - b_2c_1). \end{aligned} \quad (3.21)$$

Again, together with this multiplication  $G$  becomes a group.

$$(a, b, c, x, y, z)^{-1} = (-a, -b, -c, -x - ab, -y - ac, -z - bc). \quad (3.22)$$

$$\begin{aligned} [(a_1, b_1, c_1, x_1, y_1, z_1), (a_2, b_2, c_2, x_2, y_2, z_2)] = \\ (0, 0, 0, a_1b_2 - a_2b_1, a_1c_2 - a_2c_1, b_1c_2 - b_2c_1). \end{aligned} \quad (3.23)$$

Some facts about  $G$ :  $G$  is nonabelian of order  $q^6$ , exponent  $p$  and class 2.  $G$  is a special group with  $Z(G) = G' = \Phi(G) = \{(0, 0, 0, x, y, z) : x, y, z \in GF(q)\}$  (as usually  $\Phi(G)$  denotes the Frattini subgroup of  $G$ ).

We again define a multiplication of elements of  $G$  by elements of  $GF(q)$ :

$$\begin{aligned} \lambda(a, b, c, x, y, z) := \\ [\lambda a, \lambda b, \lambda c, \lambda x - \binom{\lambda}{2} ab, \lambda y - \binom{\lambda}{2} ac, \lambda z - \binom{\lambda}{2} bc]. \end{aligned} \quad (3.24)$$

Again,  $[\cdot, \cdot] : G \times G \rightarrow G', (x, y) \mapsto [x, y]$  is “bilinear” and skew—symmetric with respect to (3.24)

Let  $E_1 := (1, 0, 0, 0, 0, 0), \dots, E_6 := (0, 0, 0, 0, 0, 1)$ , then

$$(a, b, c, x, y, z) = (aE_1)(bE_2)(cE_3)(xE_4)(yE_5)(zE_6). \quad (3.25)$$

Let  $H := \{(a, b, 0, x, 0, 0) : a, b, x \in GF(q)\} = \{(aE_1)(bE_2)(xE_4) : a, b, x \in GF(q)\}$  and  $A := \{(0, 0, c, 0, y, z) : c, y, z \in GF(q)\} = \{(cE_3)(yE_5)(zE_6) : c, y, z \in GF(q)\}$ .

By using the commutator-formula (3.23) we see that  $A$  is elementary abelian of order  $q^3$  and normal in  $G$ .  $H$  is special of order  $q^3$  with  $Z(H) = H \cap Z(G) = \{(0, 0, 0, x, 0, 0) : x \in GF(q)\}$ . Furthermore,  $A$  and  $H$  are invariant under multiplication with scalars from  $GF(q)$  and have trivial intersection.

We are now going to determine a subgroup of  $U(H, A)$  as in Construction 1.

If  $\tau \in U(H, A)$ , then  $E_1^\tau, E_2^\tau$  are of the form  $E_1(\gamma_1 E_3)(\eta_1 E_5)(\zeta_1 E_6) = (1, 0, \gamma_1, 0, \eta_1, \zeta_1)$  and  $E_2(\gamma_2 E_3)(\eta_2 E_5)(\zeta_2 E_6) = (0, 1, \gamma_2, 0, \eta_2, \zeta_2)$  respectively. Since  $E_4$  is the commutator of  $E_1$  and  $E_2$ ,  $E_4^\tau = [E_1^\tau, E_2^\tau] = (0, 0, 0, 1, \gamma_2, -\gamma_1)$ .  $E_3, E_5$  and  $E_6$  are elements of  $A$  and therefore fixed by  $\tau$ .

Choosing  $\gamma_1, \eta_1, \zeta_1, \gamma_2, \eta_2, \zeta_2$  arbitrarily in  $GF(q)$  and defining  $\tau := \tau(\gamma_1, \eta_1, \zeta_1, \gamma_2, \eta_2, \zeta_2)$  on  $\{E_1, \dots, E_6\}$  as above, we extend  $\tau$  to an automorphism in  $U(H, A)$ :

$$\begin{aligned} (a, b, c, x, y, z)^\tau &= (aE_1^\tau)(bE_2^\tau)(cE_3^\tau)(xE_4^\tau)(yE_5^\tau)(zE_6^\tau) \\ &= [a, b, c + \gamma_1 a + \gamma_2 b, x, y + \eta_1 a + \eta_2 b - \gamma_1 \begin{pmatrix} a \\ 2 \end{pmatrix} + \gamma_2 x, \\ &\quad z + \zeta_1 a + \zeta_2 b - \gamma_2 \begin{pmatrix} b \\ 2 \end{pmatrix} - \gamma_1 x - \gamma_1 ab]. \end{aligned} \quad (3.26)$$

Moreover, similar to (3.17)

$$T := \{\tau(\gamma_1, \eta_1, \zeta_1, \gamma_2, \eta_2, \zeta_2) : \gamma_1, \eta_1, \zeta_1, \gamma_2, \eta_2, \zeta_2 \in GF(q)\} \text{ is an elementary abelian subgroup of order } q^6 \text{ of } U(H, A) \text{ and each } \tau \text{ in } T \text{ respects scalar multiplication.} \quad (3.27)$$

Here the determination of a large subset  $\Phi$  of  $T$  satisfying (3.8.a) and (3.8.b) is more involved. Let  $\tau \in T$ . The condition  $(a, b, 0, x, 0, 0)^\tau = (a, b, 0, x, 0, 0)$  leads to a system of equations which is more difficult to solve. This is due to the fact that  $H$  is nonabelian.

$$\begin{aligned} \gamma_1 a + \gamma_2 b &= 0 \\ -\gamma_1 \begin{pmatrix} a \\ 2 \end{pmatrix} + \gamma_2 x + \eta_1 a + \eta_2 b &= 0 \\ -\gamma_1(x + ab) - \gamma_2 \begin{pmatrix} b \\ 2 \end{pmatrix} + \zeta_1 a + \zeta_2 b &= 0. \end{aligned} \quad (3.28)$$

As  $E_4^\tau$  depends only on the parameters  $\gamma_1$  and  $\gamma_2$ , the largest subset  $\Phi$  of  $T$  satisfying (3.8.a) and (3.8.b) can have cardinality at most  $q^2$ . Therefore each  $(q^3, r)$ -PCP in  $G$  containing  $A$  can have at most  $q^2 + 1$  components. We will show that such a choice of  $\Phi$  is indeed possible for every odd prime power  $q$ :

Let  $q$  be fixed now. We choose  $d \in GF(q)$  such that the polynomial  $t^3 - t - d$  is irreducible in the ring  $GF(q)[t]$  of polynomials over  $GF(q)$  (observe that such a  $d$  does always exist since  $t \mapsto t^3 - t$  is not surjective on  $GF(q)$ ).

Define  $\Phi_d := \{\tau_{i,j} \in T : i, j \in GF(q)\}$ , where

$$\tau_{i,j} := \tau(-j, 0, -2^{-1}(i + j), i, -2^{-1}dj, 0). \quad (3.29)$$

Then  $\Phi_d$  is a subgroup of order  $q^2$  of  $T$ . In order to prove that  $\Phi_d$  satisfies (3.8.a) and (3.8.b) it suffices to show that (3.28) has only the trivial solution  $(a, b, x) = (0, 0, 0)$  for all  $\tau_{i,j}$  different from  $\tau_{0,0}$ . Let therefore  $(i, j)$  be different from  $(0, 0)$ . Then (3.28) has the form

$$\begin{aligned} ib - ja &= 0 \\ ix - j \left[ -\begin{pmatrix} a \\ 2 \end{pmatrix} + 2^{-1}db \right] &= 0 \\ i \left[ -\begin{pmatrix} b \\ 2 \end{pmatrix} - 2^{-1}a \right] + j(x + ab - 2^{-1}a) &= 0. \end{aligned} \quad (3.30)$$

It is easy to see, that (3.30) has only the trivial solution, if  $i = 0$  or  $j = 0$ . Let therefore  $i$  and  $j$  be different from 0 and set  $t := i/j$ . We obtain

$$\begin{aligned} tb - a &= 0 \\ tx + \begin{pmatrix} a \\ 2 \end{pmatrix} - 2^{-1}db &= 0 \\ t \left[ -\begin{pmatrix} b \\ 2 \end{pmatrix} - 2^{-1}a \right] + x + ab - 2^{-1}a &= 0. \end{aligned} \quad (3.31)$$

Using the first two equations, the parameters  $a$  and  $x$  can be expressed in terms of  $b$  and  $t$  only. After some simplifications the third equation then yields

$$b(t^3 - t - d) = 0. \quad (3.32)$$

As  $t^3 - t - d$  is assumed to be irreducible in  $GF(q)[t]$  we obtain  $b = 0$  and therefore  $a = x = 0$  by (3.31).

We have proved that  $\Phi_d$  satisfies (3.8.a) and (3.8.b) and therefore (1.11):

$$\{\tau(H) : \tau \in \Phi_d\} \cup \{A\} \text{ is a } (q^3, q^2 + 1)\text{-PCP in } G. \quad (3.33)$$

We close this section with some remarks. As above let  $p$  be an odd prime number. In (Hachenberger 1991) it is proved that the only nonabelian  $p$ -groups of odd order satisfying equality in (1.7) are  $G_1 := \langle a, b \mid a^{p^2} = b^{p^2} = 1, [a, b] = a^p \rangle$ ,  $G_2 := \langle a, b, x, y \mid \exp(G_2) = p, Z(G_2) := \langle x, y \rangle, [a, b] = x \rangle$  and the (unique) special group of order  $p^6$ , exponent  $p$  with center of order  $p^3$  which we denote by  $G_3$ . Furthermore PCPs with the largest possible number of components are given for each of these groups in (Hachenberger 1991). If  $q = p$  in Constructions 1 and 2, we obtain groups isomorphic to  $G_2$  and  $G_3$  respectively. Therefore our series above are generalizations of these two particular examples. If one also wants to generalize the metacyclic example  $G_1$ , one has to examine the groups

$$G(n) := \langle a, b \mid a^{p^{2n}} = b^{p^{2n}} = 1, [a, b] = a^{p^n} \rangle, n \geq 1.$$

Since  $\Phi(G(n))$  is of order  $p^{2n-2}$ ,  $G(n)$  has exactly  $p + 1$  maximal subgroups. By (1.2) different components lie in different maximal subgroups. Therefore we have  $T(G(n)) \leq p + 1$ . Hence a generalization of the metacyclic example does not lead to a series of large translation nets. Using a construction based on the ideas outlined in this section, one can show that indeed  $T(G(n)) = p + 1$  for all integers  $n \geq 1$ .

In particular our constructions show that there exist nonabelian groups of order  $p^8$  and  $p^{12}$  containing  $(p^4, p^2 + 1)$ - and  $(p^6, p^4 + 1)$ -PCPs respectively. Furthermore in most of the known examples the sizes of maximal PCPs (that are PCPs which cannot be enlarged by adding a further component) are of the form  $p^k + 1$ . The bound (1.6) is therefore reasonably good in these smaller cases. It would be nice to know whether there exist nonabelian groups of order  $p^{10}$  containing  $(p^5, p^3 + 1)$ -PCPs. However, Construction 2 shows that the required calculations can become very involved.

Of course the methods explained in this section can be used for constructions of PCPs in 2-groups, too. But as nonabelian 2-groups have exponent at least 4 it is not clear how to build series from small examples. We remark that the pair  $(H, A) = (EA(4), EA(4))$  does not give  $(4, 3)$ -PCPs and  $(D_4, EA(8))$  and  $(Q_8, EA(8))$  do not lead to PCPs with more than 3 components (the latter follows also from results on groups of 64 in (Gluck 1989 and Sprague 1982)). (Here  $D_4$  and  $Q_8$  denote the dihedral and the quaternion group of order 8 respectively.) In view of our results nonabelian  $p$ -groups of class 2 and exponent  $p$  seem to be very interesting (note that necessarily  $p$  is odd then).

If  $A$  is nonabelian the set  $\Gamma(H, A)$  of semi-isomorphisms from  $H$  to  $A$  is no longer a group. Hence one does not have such a nice characterization of  $\Gamma(H, A)$  as in (3.5). The direct construction of semi-isomorphisms as well as the search for systems of pairwise orthogonal semi-isomorphisms therefore seems to be more difficult (observe that in our examples the orthogonality could be proved very easily as the corresponding sets of automorphisms formed subgroups of  $U(H, A)$ ).

#### 4. Nonabelian Groups with a Large Number of Pairwise Orthogonal Fixed-Point-Free Group Automorphisms

In this section we give among other things examples of nonabelian  $p$ -groups  $A$  which admit as many pairwise orthogonal fixed-point-free group automorphisms as possible. As mentioned in Section 2 this leads to so-called splitting translation nets with translation group  $A \times A$ , where the number  $r$  of parallel classes is equal to  $f(A) + 2$  (see (2.4) for the definition of  $f(A)$ ).

We first discuss examples of nonabelian  $p$ -groups where  $f(A) = \sqrt{|A|} - 1$  and  $f(A) = \sqrt[3]{|A|} - 1$ . In order to give an idea, where one can find examples of groups with a large number of pairwise orthogonal fixed-point-free automorphisms, we start with some remarks on permutation groups. All results from group theory we need in this section can be found in (Huppert 1967; Huppert and Blackburn 1982; Huppert and Blackburn 1983).

Let  $G$  be a finite group acting as a permutation group on a finite set  $\Omega$ . If  $G$  has a normal subgroup  $A$  which acts sharply transitively on  $\Omega$ , then  $G$  is isomorphic to a semidirect product of  $G_\omega$  with  $A$ , where  $G_\omega$  denotes a stabilizer of a point  $\omega$  of  $\Omega$ . Moreover the action

of  $G_\omega$  as an automorphism group on  $A$  (the conjugation of  $A$  by elements of  $G_\omega$ ) is equivalent to the action of  $G_\omega$  on  $\Omega$  (see (Huppert 1967, Chap. II, 2.2)).

We are interested in the following situation:

Assume that  $G_\omega$  has a proper subgroup  $U$  which contains all automorphisms which fix an element of  $A - \{1\}$ . Then each set of representatives of left cosets of  $U$  in  $G_\omega$  containing 1 is a set of pairwise orthogonal fixed-point-free group automorphisms of  $A$ . In particular, by (2.5), we obtain

$$T(A \times A) \geq f(A) + 2 \geq |G_\omega : U| + 2. \quad (4.1)$$

An investigation of the Suzuki groups  $Sz(q)$ , the projective unitary groups  $PSU(3, q^2)$  and the Ree groups  $R(q)$  as doubly transitive permutation groups leads to examples where the above situation occurs and where  $A$  is always a nonabelian  $p$ -group.

*Example 1.*  $(2^{2n}, 2^n + 1)$ —splitting translation nets with nonabelian translation groups of order  $2^{4n}$ , where  $n \geq 3$  is any odd integer.

Let  $m > 0$  be an integer,  $q := 2^{2m+1}$  and  $K := GF(q)$  the Galois field of order  $q$ . Let  $\pi : K \rightarrow K, x \mapsto x^{2^{m+1}}$  be the unique automorphism of  $K$  satisfying  $x^{\pi^2} = x^2$  for every  $x$  in  $K$ . Consider the set

$$\begin{aligned} Q := \{p_\infty\} \cup \{p_{x,y} : x, y \in K\} \text{ of points of the 3-dimensional projec-} \\ \text{tive space } \mathbb{IP}(3, K) \text{ over } K, \text{ where } p_{x,y} := \langle (xy + x^\pi x^2 + y^\pi, y, x, 1) \rangle \\ \text{and } p_\infty := \langle (1, 0, 0, 0) \rangle. \end{aligned} \quad (4.2)$$

The subgroup  $G := Sz(q)$  of  $GL(4, K)$  which induces the group of collineations of  $\mathbb{IP}(3, K)$  leaving  $Q$  invariant is called the *Suzuki group over  $GF(q)$* .  $(Sz(2^{2m+1}))_{m \geq 1}$  is a series of finite simple groups discovered by Suzuki (1962). We list some well known properties of  $G$  (see (Huppert and Blackburn 1983, Chap. IX, § 3) for details; we refer the reader as well to (Lüneburg 1965; 1980), where the geometry of the Suzuki groups is studied extensively).

$G$  acts as a *Zassenhaus group* on  $Q$ , hence  $G$  is doubly transitive, has no regular normal subgroup and only the identity fixes more than 2 elements of  $Q$ . Therefore the stabilizer  $G_\infty$  of the point  $p_\infty$  is a *Frobenius group* on  $\Omega := Q - \{p_\infty\}$  (see (Huppert 1967, Chap. V, § 8) for the definitions and more details about Frobenius groups). The Frobenius kernel  $A$  of  $G_\infty$  consists of the following collineations of  $\mathbb{IP}(3, K)$  (represented as matrices over  $K$ ):

$$A := \{s(a, b) : a, b \in K\}, \text{ where}$$

$$s(a, b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a^\pi & 1 & 0 \\ a^2 a^\pi + ab + b^\pi & aa^\pi + b & a & 1 \end{pmatrix}, \quad (4.3)$$

The group  $H$  of diagonal matrices of the form

$$h(\lambda) := \text{diag}(\lambda^{1+2^m}, \lambda^{2^m}, \lambda^{-2^m}, \lambda^{-1-2^m}) \text{ for } \lambda \in K^* \quad (4.4)$$

is a Frobenius complement of  $A$  in  $G_\infty$ . Hence the whole group  $H$  acts fixed-point-freely on  $A$  and we obtain

$$T(A \times A) \geq |H| + 2 = q + 1. \quad (4.5)$$

$A$  is a nonabelian special group of order  $q^2 = 2^{4m+2}$  with center of order  $q$ . Since  $f(A) \leq f(Z(A)) \leq q - 1$  the set  $H$  of pairwise orthogonal fixed-point-free group automorphisms above is as large as possible. Therefore  $f(A) = q - 1$  and we obtain a series of  $(q^2, q + 1)$ -PCPs in nonabelian groups of order  $q^4$  where  $q \geq 8$  is any odd power of 2.

*Example 2.*  $(q^3, q + 1)$ -splitting translation nets with nonabelian translation groups of order  $q^6$ .

Let  $p$  be a prime and  $q := p^m$  any power of  $p$ ,  $m \geq 1$ . Let  $K := GF(q^2)$  and  $K_0 := GF(q)$  be the Galois fields of order  $q^2$  and  $q$  respectively. Let  $\tau : K \rightarrow K$ ,  $x \mapsto x^q$  be the unique involution in the automorphism group of  $K$  and let  $\text{IP}(2, K)$  be the classical projective plane over  $K$ . Then  $\tau$  induces a polarity on  $\text{IP}(2, K)$  and the set  $Q$  of absolute points in  $\text{IP}(2, K)$  with respect to  $\tau$  has cardinality  $q^3 + 1$ . The *projective unitary group*  $G := \text{PSU}(3, q^2)$  acts as a permutation group on  $Q$  and has the following properties (see (Huppert 1967, Chap. II, § 8) for details).

If  $q > 2$ , then  $G$  is a simple group. In all cases  $G$  acts doubly transitively on  $Q$ . The point stabilizer  $G_\omega$  of a point  $\omega$  in  $Q$  has a regular normal subgroup  $A$  (of order  $q^3$ ). As a matrix group  $A$  has the form

$$A := \{u(a, b) : a, b \in K, b + b^\tau + aa^\tau = 0\},$$

$$\text{where } u(a, b) := \begin{pmatrix} 1 & a & b \\ 0 & 1 & -a^\tau \\ 0 & 0 & 1 \end{pmatrix}. \quad (4.6)$$

$$H := \{h(\lambda) : \lambda \in K^*\}, \text{ where } h(\lambda) = \text{diag}(\lambda^{-\tau}, \lambda^{\tau^{-1}}, \lambda) \quad (4.7)$$

is cyclic of order  $q^2 - 1$  and acts as an automorphism group on  $A$ .

The action of  $H$  on  $A$  can be described by

$$h(\lambda)^{-1}u(a, b)h(\lambda) = u(\lambda^{2q-1}a, \lambda^{q+1}b). \quad (4.8)$$

Assume that  $h(\lambda)$  fixes an element  $u(a, b)$  different from  $u(0, 0)$  in  $A$ . Then  $\lambda^{2q-1}a = a$  and  $\lambda^{q+1}b = b$ . If  $b = 0$  then  $a \neq 0$  hence  $\lambda^{2q-1} = 1$ . Therefore the order of  $\lambda$  divides  $\text{gcd}(q^2 - 1, 2q - 1) = \text{gcd}(q + 1, 2q - 1)$ . If  $b \neq 0$  then  $\lambda^{q+1} = 1$  and the order of

$\lambda$  divides  $q + 1$ , too. Therefore  $\lambda$  lies in any case in the unique subgroup  $U$  of order  $q + 1$  of  $H$ . Conversely it is clear that  $h(\lambda)$  fixes a nonidentity element of  $A$  if  $\lambda$  is a  $(q + 1)$ st root of unity in  $K$ . As mentioned in (4.1), each set of representatives of left cosets of  $U$  in  $H$  containing  $h(1)$  is a set of pairwise orthogonal fixed-point-free group automorphisms of  $A$ . We therefore have

$$T(A \times A) \geq f(A) + 2 \geq |H : U| + 2 = q + 1$$

and obtain a  $(q^3, q + 1)$ -PCP in  $A \times A$  by using the automorphism method.

This proves (1.13) since  $A$  is nonabelian. We remark that  $A$  is a special group with center of order  $q$ . As in Example 1, we have  $f(A) = f(Z(A)) = q - 1$ , hence the sets of pairwise orthogonal fixed-point-free group automorphisms above are again as large as possible.

If  $q$  is odd, then  $A$  is of exponent  $p$ . If  $q$  is even, then  $Z(A) = \{u(0, 0)\}$  is exactly the set of involutions of  $A$  and  $H$  permutes this set cyclically. If in addition  $q > 2$  then  $A$  has more than one involution and satisfies therefore the properties of a so-called *Suzuki 2-group* (see (Higman 1963; Huppert and Blackburn 1982, Chap. VII, § 6, 7) for more details about Suzuki 2-groups). We mention that the groups  $A$  in Example 1 are likewise Suzuki 2-groups. Suzuki 2-groups are special 2-groups and their centers consist exactly of the elements of order at most 2. They are classified by Higman (1963). There exist four families, three of which contain nonabelian groups of order  $t^3$  with center of order  $t$ , where  $t$  are certain powers of 2 (see (Higman 1963) for details). All such groups lead to  $(t^3, t + 1)$ -PCPs by using the automorphism method. In the next example, which proves (1.12), we are going to study a family of matrix groups which are a generalization of the fourth family of Suzuki 2-groups in (Higman 1963) (we also consider matrices over fields of odd characteristic).

*Example 3.*  $(q^2, (q - 1) \cdot \gcd(q - 1, 2)^{-1} + 2)$ —splitting translation nets with nonabelian translation groups of order  $q^4$  where  $q = p^n$  is a prime power and  $n$  is not a power of 2.

Let  $p$  be a prime and  $n > 1$  an integer which is not a power of 2. Let  $F := GF(q)$  be the Galois field of order  $q := p^n$  and  $\tau \neq id$  any automorphism of  $F$  of odd order.

Let  $k$  denote the order of  $\tau$ . Assume that  $x\tau^k = 1$  for some  $x$  in  $F^*$ . Then  $x = x^{\tau^k} = x^{(-1)^k} = x^{-1}$  and therefore  $x^2 = 1$ , hence  $x \in \{1, -1\}$ .

$$A(n, \tau) := \{u(a, b) : a, b \in F\}, \text{ where } u(a, b) := \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\tau \\ 0 & 0 & 1 \end{pmatrix} \quad (4.9)$$

is a group of order  $q^2$  and center  $Z(A(n, \tau)) = \{u(0, b) : b \in F\}$  of order  $q$ .

Let  $H := \{h(\lambda) : \lambda \in F^*\}$  where  $h(\lambda) := \text{diag}(1, \lambda, \lambda\lambda^\tau)$ . Then  $H$  acts as an automorphism group on  $A(n, \tau)$ :

$$u(a, b)^{h(\lambda)} := h(\lambda)^{-1}u(a, b)h(\lambda) = u(\lambda a, \lambda\lambda^\tau b). \quad (4.10)$$



If  $h(\lambda)$  has a fixed point  $u(a, b)$  different from  $u(0, 0)$  in  $A(n, \tau)$ , then  $\lambda a = a$  and  $\lambda\lambda^\tau b = b$ . If  $b = 0$  then  $a \neq 0$  and  $\lambda = 1$ ; if  $b \neq 0$  then  $\lambda\lambda^\tau = 1$  and  $\lambda \in \langle -1 \rangle$  by the remark above. As  $H$  is isomorphic to  $F^*$ , a further application of (4.1) shows

$$T(A(n, \tau) \times A(n, \tau)) \geq f(A(n, \tau)) + 2 \geq (q - 1) \cdot \gcd(2, q - 1)^{-1} + 2$$

and this proves (1.12).

Note that  $f(A(n, \tau)) = q - 1$ , if  $q$  is even. Furthermore in this case  $A(n, \tau)$  is one of the Suzuki 2-groups of the fourth family in (Higman 1963) and the number of mutually orthogonal fixed-point-free group automorphisms again is as large as possible.

We are now giving a final example for situation (4.1). The Ree groups, a further series of finite simple groups (discovered by Ree in (1961)), as well lead to splitting translation nets with a remarkably large number of parallel classes.

*Example 4.*  $(q^3, \frac{1}{2}(q + 3))$ —splitting translation nets with nonabelian translation groups of order  $q^6$ , where  $q > 3$  is any odd power of 3.

Let  $n \geq 1$  be an integer and  $q = 3^{2n+1}$ . The *Ree group*  $R(q)$  is a simple group of order  $(q^3 + 1)q^3(q - 1)$  which is doubly transitively of degree  $q^3 + 1$  (see (Huppert and Blackburn 1983, Chap. XI, § 13) for details). The stabilizer of a point has a regular normal subgroup  $A$  which is isomorphic to the group of all triples  $(x, y, z)$  over  $GF(q)$  with multiplication

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2 + x_1x_2^\tau, z_1 + z_2 - x_1y_2 + y_1x_2 - x_1x_1^\tau x_2), \quad (4.11)$$

where  $\tau : GF(q) \rightarrow GF(q)$ ,  $x \mapsto x^{3^{n+1}}$ . The subgroup  $A$  is nonabelian of order  $q^3$  with center of order  $q$ . Let  $H$  be the stabilizer of two points.  $H$  is cyclic of order  $q - 1$ . If  $H := \{h(\lambda) : \lambda \in GF(q)^*\}$ , the action of  $H$  on  $A$  can be described by

$$(x, y, z)^{h(\lambda)} = (\lambda x, \lambda^{1+3^{n+1}} y, \lambda^{2+3^{n+1}} z). \quad (4.12)$$

Assume that  $h(\lambda)$  has a fixed point  $(x, y, z)$  different from  $(0, 0, 0)$ . If  $z \neq 0$  then the order of  $\lambda$  divides  $\gcd(2 + 3^{n+1}, 3^{2n+1} - 1) = 1$ , hence  $\lambda = 1$ . (Observe that  $1 = (-3^{n+1} + 2)(3^{n+1} + 2) + 3(3^{2n+1} - 1)$ .) If  $y \neq 0$  then the order of  $\lambda$  divides  $\gcd(3^{n+1} + 1, 3^{2n+1} - 1) = 2$ , hence  $\lambda = 1$  or  $\lambda = -1$  (observe that  $\{(0, y, 0) : y \in GF(q)\}$  is fixed if  $\lambda = -1$ ). If  $x \neq 0$  then  $\lambda = 1$ . Therefore any automorphism in  $H$  fixing a nontrivial element of  $A$  lies in  $\{h(1), h(-1)\}$ , the unique subgroup of order 2 in  $H$ . Using once more (4.1), we obtain

$$T(A \times A) \geq f(A) + 2 \geq |H : \langle h(-1) \rangle| + 2 = \frac{1}{2}(q + 3)$$

and therefore the desired series of  $(q^3, \frac{1}{2}(q + 3))$ -splitting translation nets with nonabelian translation groups of order  $q^6$ . The best known upper bound for  $f(A)$  which is  $|Z(A)| - 1 = q - 1$  is not met in this example.

We finally remark that similar to the Suzuki groups and the projective unitary groups in Example 1 and 2 the geometry of the Ree groups was studied extensively (see for example (Lüneburg 1966) and (Tits 1960)). (Lüneburg 1967) is a survey about group theoretic methods in geometry in general.

## Acknowledgment

The results of this paper will form part of the author's doctoral dissertation. He thanks his supervisor Prof. Dr. Dieter Jungnickel as well as Prof. Dr. Thomas Meixner for many helpful discussions.

## References

- Aschbacher, M. 1986. Finite group theory. Cambridge: Cambridge University Press.
- Bailey, R.A. and Jungnickel, D. 1990. Translation nets and fixed-point-free group automorphisms. *J. Comb. Th. Ser. A* 55: 1–13.
- Beth, T., Jungnickel, D. and Lenz, H. 1986. Design Theory. Cambridge: Cambridge University Press.
- Frohardt, D. 1987. Groups with a large number of large disjoint subgroups. *J. Algebra* 107: 153–159.
- Gluck, D. 1989. Hadamard difference sets in groups of order 64. *J. Comb. Th. Ser. A* 51: 138–141.
- Hachenberger, D. (forthcoming 1991) On the existence of translation nets. *J. Algebra*.
- Hachenberger, D. and Jungnickel, D. 1990. Bruck nets with a transitive direction. *Geometriae Dedicata* 36: 287–313.
- Higman, G. 1963. Suzuki 2-groups. *Illinois J. Math.* 7: 79–96.
- Huppert, B. 1967. *Endliche Gruppen I*. Berlin-Heidelberg-New York: Springer.
- Huppert, B. and Blackburn, N. 1982. *Finite Groups II*. Berlin-Heidelberg-New York: Springer.
- Huppert, B. and Blackburn, N. 1983. *Finite Groups III*. Berlin-Heidelberg-New York: Springer.
- Jungnickel, D. 1981. Existence results for translation nets. In *Finite geometries and designs, London Math. Soc. Lecture Notes* 49, (Eds. P.J. Cameron, J.W.P. Hirschfeld and D.R. Hughes), Cambridge: Cambridge University Press, 172–196.
- Jungnickel, D. 1989. Existence results for translation nets II. *J. Algebra* 122: 288–298.
- Jungnickel, D. 1989a. Partial spreads over  $Z_q$ . *Linear Algebra Appl.* 114: 95–102.
- Jungnickel, D. 1990. Latin squares, their geometries and their groups. A Survey. In *Coding Theory and Design Theory II* (Ed. D.K. Ray-Chaudhuri), Berlin-Heidelberg-New York: Springer, 166–225.
- Lüneburg, H. 1965. *Die Suzukigruppen und ihre Geometrien*. Lecture Notes in Mathematics 10, Berlin-Heidelberg-New York: Springer.
- Lüneburg, H. 1966. Some remarks concerning Ree groups of type  $(G_2)$ . *J. Algebra* 3: 256–259.
- Lüneburg, H. 1967. Gruppentheoretische Methoden in der Geometrie. Ein Bericht. In: *Jahresbericht der DMV*, Bd. 70: 16–51.
- Lüneburg, H. 1980. Translation planes. Berlin-Heidelberg-New York: Springer.
- Ree, R., 1961. A family of simple groups associated with the simple Lie algebra of type  $(G_2)$ . *Amer. J. Math.* 83: 432–462.
- Sprague, A.P. 1982. Translation nets. *Mitt. Math. Sem. Giessen* 157: 46–68.
- Suzuki, M. 1962. On a class of doubly transitive groups. *Annals of Mathematics* 75: 105–145.
- Tits, J. 1960. Les groupes simples de Suzuki et de Ree. *Sem. Bourbaki, décembre*.