UNIVERSITÄT KAISERSLAUTERN

ON A COMBINATORIAL PROBLEM IN GROUP THEORY

Dirk Hachenberger

Preprint No 208

FACHBEREICH MATHEMATIK

ON A COMBINATORIAL PROBLEM IN GROUP THEORY

Dirk Hachenberger

Preprint No 208

UNIVERSITÄT KAISERSLAUTERN
Fachbereich Mathematik
Erwin–Schrödinger–Straße
6750 Kaiserslautern

November 1991

On a Combinatorial Problem in Group Theory

Dirk Hachenberger
Fachbereich Mathematik der Universität Kaiserslautern
Erwin - Schrödinger Straße
D - 6750 Kaiserslautern

Abstract:

In this paper we continue the study of p-groups G of square order p^{2n} and investigate the existence of partial congruence partitions (sets of mutually disjoint subgroups of order p^n) in G. Partial congruence partitions are used to construct translation nets and partial difference sets, two objects studied extensively in finite geometries and combinatorics.

We prove that the maximal number of mutually disjoint subgroups of order p^n in a group G of order p^{2n} cannot be more than $(p^{n-1} - 1)(p-1)^{-1}$ provided that $n \geq 4$ and that G is not elementary abelian. This improves a result in [6] and as we do not distinguish the cases $p = 2$ and p odd in the present paper, we also have a generalization of D. FROHARDT's theorem on 2-groups in [4].

Furthermore we study groups of order p^6. We can show that for each odd prime number, there exist exactly four nonisomorphic groups which contain at least $p+2$ mutually disjoint subgroups of order p^3. Again, as we do not distinguish between the even and the odd case in advance, we in particular obtain D. GLUCK's and A. P. SPRAGUE's classification of groups of order 64 which contain at least 4 mutually disjoint subgroups of order 8 in [5] and [13] respectively.

Acknowledgement:

The results in this paper will form part of the authors doctoral dissertation. He thanks his supervisor Prof. Dr. Dieter Jungnickel for many helpful discussions.

1. Introduction

Let G be a finite group and $\mathbb{H} = \{H_1, \ldots, H_r\}$ a nonempty set of r nontrivial subgroups of G. We say that $\mathbb{H}$ satisfies the **maximality condition**, if

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

The elements of $\mathbb{H}$ are called **components**.

If in addition the order of G is s^2, the number r of components is at least 3 and

(2) $$|H_i| = s \text{ for all } i = 1, \ldots, r,$$

then $\mathbb{H}$ is called a **partial congruence partition of order s and degree r** in G (for short an **(s,r) - PCP** in G).

A direct consequence of the definition of an (s,r) - PCP $\mathbb{H}$ is

(3) $$H_i \cap H_j = 1 \text{ for all } i \neq j \text{ in } \mathbb{H}.$$

Partial congruence partitions are studied extensively by many authors (see e.g. [1, 3, 4, 5, 6, 7, 8, 10, 11, 13]) because of their close relation to translation nets. The reader who is interested in the geometric background is refered to [2, 6, 7, 8, 10, 11, 12, 13]. Further applications of partial congruence partitions in mathematics, e. g. the construction of certain partial difference sets, are discussed in [1, 12], where one can also find a lot of further references.

As in [6, 7, 12] we define

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

It is easy to see that a partial congruence partition of order s in G cannot contain more than s+1 components and it is well known that equality holds if and only if G is elementary abelian, thus in particular the order s is a power of a prime. As $T(G) \leq T(P)$ for any Sylow subgroup P of G (see [4, 6, 11, 12]), we are mainly interested in studying PCPs in p - groups. The elementary abelian case is well known:

If G is elementary abelian of order p^{2n}, then

(5) $$T(G) = p^n + 1.$$

We are therefore going to investigate p - groups which are not elementary abelian and deal with the following problem:

How large can be the degree r of a partial congruence partition in a group G of order p^{2n} provided that G is not elementary abelian ?

The following theorem shows that r will be considerably smaller than in the elementary abelian case.

(1.1) Theorem :

Let $n \geq 4$ and let G be a group of order p^{2n}. Assume that G is not elementary abelian. Then

$$T(G) \leq \frac{p^{n-1} - 1}{p - 1} .$$

Example:

Let G be elementary abelian of order 3^8, then $T(G) = 82$ by (5). Let K be any group of order 3^8 which is not elementary abelian, then $T(K) \leq 13$.

Theorem (1.1) is an improvement of a result on p-groups of odd order in [6]. If $p = 2$, we obtain a known result on 2-groups which was proved by D. FROHARDT in [4]. Similar to [4] our proof of (1.1) proceeds by investigating carefully the interplay between the components of a PCP in G and $\Omega_1(Z(G))$, the largest elementary abelian subgroup of the center of G. However, our proof is not just a generalization of that in [4]: In his proof, D. FROHARDT uses in several steps the fact that a finite 2-group G contains at least $4^{-1} \cdot |G|$ elements of order at least 4 provided that G is not elementary abelian (see [4, Lemma 1]). As the analogue is not true in p-groups of odd order and as we do not distinguish between the cases $p = 2$ and p odd, we have to use other methods and therefore give implicitely a new proof of the special case when $p = 2$.

We will see that p-groups of exponent p are more difficult to handle than other p-groups (this becomes clear in (1.8) below). On the other hand, p-groups of exponent p are also a source for many interesting examples: In [7] some series of so-called large translation nets are constructed with partial congruence partitions in such groups. Furthermore, we will see that all groups G of order p^6 with odd p and $T(G) \geq p+2$ have exponent p. We prove

(1.2) Theorem :

Let G be a group of order p^6 and let $\Omega := \Omega_1(Z(G)) = \langle x \in Z(G) \mid x^p = 1 \rangle$.

If $T(G) \geq p+2 = (p^{3-1} - 1)(p-1)^{-1} + 1$, then $|\Omega| \geq p^3$ and one has one of the following cases:

(1.2.a) G is elementary abelian and $T(G) = p^3 + 1$.

(1.2.b) p is odd, G is isomorphic to $E(p^3) \times EA(p^3)$ and $T(G) = p+2$.

(Here $E(p^3)$ and $EA(p^3)$ denote the extraspecial group of order p^3 and exponent p and the elementary abelian group of order p^3 respectively.)

(1.2.c) p is odd, G is isomorphic to the unique special group of exponent p with center of order p^3 and $T(G) = p^2 + 1$.

(1.2.d) G is isomorphic to $\langle a,b,c,u,v,x \mid$ all generators have order p; $[a,b]=u$, $[b,c]=v$, all other commutators are equal to one $\rangle$ and $T(G) = p+2$.

Again most of the results are new in the odd case while partial congruence partitions in groups of order 64 were studied by D. GLUCK and A. P. SPRAGUE in [5] and [13] respectively. Their result is covered by our investigations.

The particular interest in 2-groups arises from the fact that certain Hadamard Difference sets can be constructed by using $(2^n, 2^{n-1})$- PCPs (see J. DILLON [3], where the problem of classifying all groups G of order 2^{2n} with $T(G) \geq 2^{n-1}$ was posed). We shall therefore summarize the consequences of (1.1) and (1.2) for the particular case p = 2:

Theorem (D. FROHARDT, D. GLUCK, A.P.SPRAGUE):

Let G be a group of order 2^{2n} with $n \geq 3$ and assume that there exists a $(2^n, 2^{n-1})$ - PCP in G. Then G is elementary abelian or G is isomorphic to the group in (1.2.d) (with p = 2).

However, as mentioned in the abstract and above, partial congruence partitions in general are of certain interest in mathematics.

We remark that all groups of order p^4 with at least three mutually disjoint subgroups of order p^2 are classified in [6, section 4].

In the remainder of this introductory section we summarize the basic tools we need to prove (1.1) and (1.2). They are more or less implicite in [6, sections 2 and 3] so that we do not need to prove everything. Beside these results we use only basic facts from the theory of p-groups, which can be found in [9, chap. III].

We start with some upper bounds for the cardinality of sets of subgroups satisfying the maximality condition (1):

(1.3) Proposition:

Let G be a p-group and $\mathbb{H}$ a set of r subgroups of G. Assume that $\mathbb{H}$ satisfies (1). Let $\eta(G)$ be an epimorphic image of G and assume that $\eta(\mathbb{H}) := \{ \eta(H) \mid H \in \mathbb{H} \}$ is a set of nontrivial subgroups of $\eta(G)$.

Then $\eta(\mathbb{H})$ satisfies as well the maximality condition and

$$\left|\eta(G)/\Phi(\eta(G))\right| \geq r(p-1)+1.$$

(As usual, $\Phi(X)$ denotes the Frattini subgroup of a p-group X.)

Proof:

The first assertion is clear as $\eta(\mathbb{H})$ by assumption is a set of nontrivial subgroups of G and as $\eta(H)\eta(K) = \eta(HK) = \eta(G)$ for any two different components H and K in $\mathbb{H}$. By (1) different components of $\eta(\mathbb{H})$ lie in different maximal subgroups of $\eta(G)$, hence, by assumption, $\eta(G)$ contains at least r different maximal subgroups. The Frattini subgroup $\Phi(\eta(G))$ of $\eta(G)$ is by definition the intersection of all maximal subgroups in $\eta(G)$, whence the maximal subgroups of the factor group $V := \eta(G)/\Phi(\eta(G))$ are in one-to-one correspondence to the maximal subgroups of $\eta(G)$. As V is elementary abelian, the number of maximal subgroups of $\eta(G)$ is by duality equal to the number of one-dimensional subspaces of V (regarded as vector space over the Galois field GF(p) of order p). The above inequality follows now immediately from the fact that V contains $(|V|-1)(p-1)^{-1}$ different one-dimensional subspaces. □

(1.4) Corollary:

Let $\mathbb{H}$ and G be as in (1.3) and let X be a proper normal subgroup of G. Assume that HX/X is a nontrivial subgroup of G/X for all H in $\mathbb{H}$. Then

$$\frac{|G|\,|\Phi(G)\cap X|}{|X|\,|\Phi(G)|} \geq r(p-1)+1.$$

Proof:

By [9, chap. III, 3.14] we have $\Phi(G/X) = \Phi(G)X/X$, which is isomorphic to $\Phi(G)/\Phi(G)\cap X$. Hence $\left|\Phi(G/X)\right| = |\Phi(G)|\cdot|\Phi(G)\cap X|^{-1}$. Now apply (1.3) with the natural epimorphism $\eta : G \longrightarrow G/X$. □

Sets of subgroups of p-groups satisfying the maximality condition were first studied by D. JUNGNICKEL in [10,11]. There such sets are called generalized partial congruence partitions with parameter t provided that there exists a component of order p^t and that this is the maximal order a component can have. The situations where Theorem 4.9 of [10], a result on the maximal size of generalized partial congruence partitions, is used in [6] can indeed be handled with variations of (1.4). In the present paper we will use (1.4) instead of the deeper result in [10].

We continue with a factorization lemma of [6]. Its applications (1.6), (1.7) and (1.8) below are indispensable in studying PCPs. They were for example very useful in determining all groups G of order p^4 with $T(G) \geq 3$. Proofs, further applications and generalizations of (1.5) can be found in [6, section 3].

(1.5) Factorization lemma :

Let G be a group of order s^2, X a nontrivial normal subgroup of G and $\mathbb{H}$ an (s,r) - PCP in G (with $r \geq 3$ by definition). Assume the validity of

(6) $X = (H \cap X)(K \cap X)$ for each pair of subgroups H, K $(H \neq K)$ in $\mathbb{H}$.

Then the order of X is a square, say $|X| = n^2$ and the order of the factor group G/X is $(s/n)^2$. Furthermore $\{H \cap X : H \in \mathbb{H}\}$ and $\{HX/X : H \in \mathbb{H}\}$ are (n,r) - and $(s/n, r)$ - PCPs in X and G/X, respectively.

In particular, $r \leq \min\{T(X), T(G/X)\}$.

(1.6) Application:

Let G be a p - group of order p^{2n} and $\mathbb{H}$ a (p^n, r) - PCP $(r \geq 3)$ in G consisting only of abelian components. Then (6) holds with $X = Z(G)$ and $X = \Omega_1(Z(G))$.

Furthermore, if one of these groups is nontrivial then

$$r \leq p^{[n/2]} + 1.$$

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

(1.7) Remarks :

Let G be a p - group of order p^{2n} and $\mathbb{H}$ an (p^n, r) - PCP in G.

(i) If Z(G) or $\Omega_1(Z(G))$ is not of square order, then $\mathbb{H}$ contains at most two abelian components by the previous lemma.

(ii) Let $X \in \{Z(G), \Omega_1(Z(G))\}$. If $\mathbb{H}$ contains exactly two abelian components, say H and K, then H and K still factorize X that means $X = (H \cap X)(K \cap X)$ remains valid. But $H \cap X$ and $K \cap X$ do not need to have equal order and likewise X does not need to have square order.

(1.8) Application :

Let p be an odd prime number and let G be a group of order p^{2n}. Assume that the class of G is 2 and that the derived subgroup G' of G is elementary abelian. Let $\mathbb{H}$ be any (p^n, r) - PCP in G. Then (6) holds with $X = \Omega_1(G)$.

Moreover, if $r > p^{[n/2]} + 1$, then G has exponent p.

We close the introduction with a very useful argument (see [4, Lemma 2]). For any nonempty subset X of a group G we denote by $X^G := \{x^g \mid x \in X, g \in G\}$ the union of the conjugacy classes of elements in X.

(1.9) Lemma :

Let G be a group of order s^2 and let $\mathbb{H}$ be an (s,r) - PCP in G.
Then $|H^G \cap K^G| = 1$ for any two different components H and K in $\mathbb{H}$.

2. The proofs of Theorems (1.1) and (1.2)

The proofs of (1.1) and (1.2) proceed in several steps. We use the notation $\Omega := \Omega_1(Z(G))$. Note that $\Omega \neq 1$ for all nontrivial p-groups.

General assumptions :

Let G be a group of order p^{2n} which is not elementary abelian. Assume that $n \geq 3$ and that G contains a (p^n, r)-PCP $\mathbb{H}$ with $r > (p^{n-1}-1)(p-1)^{-1}$.

In particular, we have $r \geq 4$.

(2.1) $\quad |\Phi(G)| \leq p^n$.

Proof :

If we use (1.4) with $X = 1$, then, by our general assumption on the number r of components, we obtain immediately that

$$|\Phi(G)| \leq |G| \cdot \left(r(p-1)+1\right)^{-1} < p^{n+1}.$$

Since $|\Phi(G)|$ is a power of p, we have the desired result. □

(2.2) $\quad$ G is nonabelian.

Proof :

Assume that G is abelian, then each component of $\mathbb{H}$ is abelian. As G is not elementary abelian by assumption, Ω is a proper subgroup of G. We may therefore apply (1.6) with $X := \Omega$ which is equal to $\Omega_1(G)$ in this case and obtain $T(G) \leq p^{[n/2]} + 1$. But this is a contradiction to $T(G) \geq r > (p^{n-1}-1)(p-1)^{-1}$ and $n \geq 3$. □

(2.3) $\quad$ If $|Z(G)| > p^n$ then $n = 3$, p is odd, G is isomorphic to $E(p^3) \times EA(p^3)$ and $T(G) = p+2$ (this is case (1.2.b)).

Proof :

We assume first that $\mathbb{H}(Z(G)) := \{HZ(G)/Z(G) \mid H \in \mathbb{H}\}$ is a set of nontrivial subgroups of $G/Z(G)$. An application of (1.4) with $X := Z(G)$ shows

(7) $\quad |Z(G)| \leq p^{2n} \cdot |\Phi(G) \cap Z(G)| \cdot |\Phi(G)|^{-1} \cdot \left(r(p-1)+1\right)^{-1}$.

As trivially $|\Phi(G) \cap Z(G)| \cdot |\Phi(G)|^{-1} \leq 1$ and $r > (p^{n-1}-1)(p-1)^{-1}$ by assumption, we obtain $|Z(G)| < p^{n+1}$ from (7), thus $|Z(G)| \leq p^n$, a contradiction.

Therefore there exists a component N in $\mathbb{H}$ satisfying $NZ(G) = G$. Thus N is a normal subgroup of G. The factor group G/N is isomorphic to a factor group of Z(G) and therefore abelian. Thus the derived subgroup G' of G is contained in N. As $Y' \leq G'$ for every subgroup Y of G, we obtain by (3) in particular that H is abelian for all H in $\mathbb{H}-\{N\}$.

Furthermore, it is clear that HZ(G) is a proper subgroup of G for any other component H in $\mathbb{H}-\{N\}$. Otherwise we would have $G' \leq N \cap H = 1$, thus G is abelian. But this is a contradiction to (2.2).

An application of (1.6) with $X := Z(G)$ and the partial congruence partition $\mathbb{H}-\{N\}$ of order p^n and degree $r-1$ yields

$$(8) \qquad (p^{n-1}-1)(p-1)^{-1} \leq r-1 \leq p^{[n/2]}+1.$$

(Observe that $r-1 \geq 3$ and that $1 \neq Z(G)$ by (2.2) is a proper subgroup of G.)

Now (8) implies $n=3$, hence G is a group of order p^6. Since the left hand and the right hand side are equal in (8), we see that $r=p+2$. As the order of Z(G) by (1.6) is a square, G is nonabelian and $|Z(G)| > p^n = p^3$ by assumption, we obtain that $|Z(G)| = p^4$.

Now $\mathbb{H}-\{N\}$ is an $(p^3, p+1)$ - PCP consisting only of abelian components. Applying once more (1.6) we see that Ω is of square order, hence $|\Omega| \in \{p^2, p^4\}$. Moreover, $N \cap \Omega$ is nontrivial as N is normal in G. Thus all components have nontrivial intersection with Ω, so that we obtain $|\Omega| \geq (p+2)(p-1) + 1 = p^2 + p - 1 > p^2$, hence Ω is of order p^4 and $\Omega = Z(G)$.

In particular, we see that G is isomorphic to $N \times EA(p^3)$. As G is nonabelian by (2.2), the component N has to be nonabelian. Moreover, as G/N is elementary abelian, the Frattini subgroup $\Phi(G)$ of G is contained in N. Now for any subgroup X of G we have $\Phi(X) \leq \Phi(G)$ by [9, chap. III, 3.14]. Hence, again by (3), $\Phi(H) = 1$ and H is elementary abelian for all H in $\mathbb{H}-\{N\}$.

Now $\mathbb{H}(\Omega) := \{H\Omega \mid H \in \mathbb{H}-\{N\}\}$ is exactly the set of maximal subgroups in G containing Ω (note that $|H \cap \Omega| = p^2$ for all $H \in \mathbb{H}-\{N\}$ by (1.5) and (1.6)). As $X \cap Y = \Omega$ for different members X and Y in $\mathbb{H}(\Omega)$, an easy counting argument shows

$$(9) \qquad \Big| \bigcup_{H \in \mathbb{H}-\{N\}} H\Omega \Big| = (p+1)(p^5 - p^4) + p^4 = p^6 = |G|.$$

Since $H\Omega$ is elementary abelian of order p^5 for all H in $\mathbb{H} - \{N\}$, equation (9) implies that G is of exponent p. In particular N is a nonabelian group of order p^3 and exponent p. Thus p is odd and N is isomorphic to $E(p^3)$, the extraspecial group of order p^3 and exponent p.

It remains to show that $G := E(p^3) \times EA(p^3)$ indeed contains $p+2$ mutually disjoint subgroups of order p^3:

In generators and relations G can be written as

$\langle a,b,u,v,x,y \mid$ all generators have order p; $[a,b] = y$, all other commutators are equal to 1 $\rangle$.

As p is odd and G has class 2, we can use that the commutator mapping $[.,.]: G \times G \longrightarrow G'$ is bilinear and skew - symmetric with respect to the Galois field GF(p) of order p, that is

(10) $[g,h] = [h,g]^{-1}$ and $[g^\lambda,h] = [g,h]^\lambda$ for all g,h in G and all $\lambda \in GF(p)$.

Furthermore,

(11) $(gh)^\lambda = g^\lambda h^\lambda [g,h]^{-\binom{\lambda}{2}}$ for all g,h in G and all λ in GF(p)
(here $\binom{\lambda}{2} = 2^{-1}\lambda(\lambda-1)$).

It is easy to show that any element in G can uniquely be written in the form $a^\alpha b^\beta u^\mu v^\nu x^\xi y^\eta$ with $\alpha,\beta,\mu,\nu,\xi,\eta \in GF(p)$. We refer to this as the standard presentation.

(12) Define $H_i := \langle ab^i, xy^i, uv^i \rangle$ for i in GF(p),
$H_\infty := \langle bx, v, uy \rangle$ and
$N := \langle av, b, y \rangle$.

We claim that $\mathbb{H} := \{N, H_\infty\} \cup \{H_i \mid i \in GF(p)\}$ is an $(p^3, p+2)$-PCP in G:

Using the presentation of G, it is easy to see that N is isomorphic to $E(p^3)$ and that all other subgroups are elementary abelian of order p^3. We use now (10) and (11) to write elements of H_i ($i \in GF(p)$), H_∞ and N in standard presentation and obtain:

$$H_i = \{(ab^i)^\alpha (xy^i)^\beta (uv^i)^\gamma \mid \alpha,\beta,\gamma \in GF(p)\}$$
$$= \{a^\alpha b^{i\alpha} u^\gamma v^{i\gamma} x^\beta y^{i\beta - i\binom{\alpha}{2}} \mid \alpha,\beta,\gamma \in GF(p)\},$$

$$H_\infty = \{b^\alpha u^\gamma v^\beta x^\alpha y^\gamma \mid \alpha,\beta,\gamma \in GF(p)\},$$

$$N = \{a^\alpha b^\beta v^\alpha y^\gamma \mid \alpha,\beta,\gamma \in GF(p)\}.$$

Now is not difficult to verify that $\mathbb{H}$ satisfies (3), which proves (2.3). We skip the easy calculations. □

From now on we assume that $|Z(G)| \leq p^n$. In (2.4), (2.5) and (2.6) we therefore deal with the cases $|\Omega| = p^n$, $|\Omega| = p^{n-1}$ and $|\Omega| \leq p^{n-2}$ respectively.

(2.4) If $|\Omega| = p^n$, then $n = 3$ and, depending on whether $|\Phi(G)| = p^3$ or $|\Phi(G)| = p^2$, we have one of the following cases :

(i) p is odd, G is a special group of exponent p with center of order p^3 and therefore isomorphic to

$\langle a,b,c,x,y,z \mid$ all generators have order p; $[a,b]=x$, $[a,c]=y$, $[b,c]=z$, all other commutators are equal to one $\rangle$.

Furthermore $T(G) = p^2+1$. (This is case (1.2.c).)

(ii) p is any prime number, G is isomorphic to

$\langle a,b,c,u,v,x \mid$ all generators have order p; $[a,c]=u$, $[b,c]=v$, all other commutators are equal to one $\rangle$.

Furthermore $T(G) = p+2$. (This is case (1.2.d).)

Proof :

Assume that $|\Omega| = p^n$ (note that then $\Omega = Z(G)$). As in the proof of (2.3) any subgroup X of G satisfying $X\Omega = G$ is normal in G and has therefore nontrivial intersection with Ω. As $|\Omega| = p^n$ and $|G| = p^{2n}$, X cannot have order p^n. In particular each component H in $\mathbb{H}$ intersects Ω nontrivially. Hence $\{H\Omega/\Omega \mid H \in \mathbb{H}\}$ is a set of nontrivial subgroups of G/Ω. An application of (1.4) with $X := \Omega$ shows

$$1 \leq |\Phi(G)| \cdot |\Phi(G) \cap \Omega|^{-1} = |\Phi(G) : \Phi(G) \cap \Omega| \leq p^{2n} \cdot |\Omega|^{-1} \cdot \left(r(p-1)+1\right)^{-1} < p.$$

Therefore $\Phi(G) \cap \Omega = \Phi(G)$, hence $\Phi(G) \leq \Omega$. As furthermore G is nonabelian by (2.2), this shows that G is nilpotent of class 2.

Before going on, we give a short outline of the further proof of (2.4):

By counting nonabelian components of $\mathbb{H}$ we can deduce a lower bound for the order of the derived subgroup G' of G. As $G' \leq \Phi(G)$, we therefore obtain likewise a lower bound for $|\Phi(G)|$; more precisely we prove that $|G'|, |\Phi(G)| \in \{p^{n-1}, p^n\}$ (see (2.4.a)). After having handled the case $|G'| = p^{n-1}$ in (2.4.b), we can assume that G is a special group, that is $\Phi(G) = G' = Z(G)$ (see (2.4.c)) and may apply some ideas of [6, section 5].

(2.4.a) $|G'|, |\Phi(G)| \in \{p^{n-1}, p^n\}$.

If n is odd, then $|\Omega|$ is not a square and remark (1.7)(i) shows that $\mathbb{H}$ cannot contain more than 2 abelian components. Therefore H' is nontrivial for at least r - 2 components. We obtain

(13) $$|G'| \geq (r-2)(p-1) + 1 \geq p^{n-1} - p + 1$$

and therefore $|G'| \geq p^{n-1}$ as $|G'|$ is a power of p and as $n \geq 3$.

If n is even, for instance $n = 2k$, then the number of abelian components in $\mathbb{H}$ is at most $p^k + 1$ by (1.6). Therefore the number of nonabelian components in $\mathbb{H}$ is at least $r - p^k - 1$, we have

(13') $$|G'| \geq (r-1-p^k)(p-1) + 1 \geq p^{n-1} - p^{k+1} + p^k.$$

If $k > 2$, then $n - 1 = 2k - 1 > k + 1$ and we have $|G'| \geq p^{n-1}$ as before.

Finally assume that $k = 2$ and $n = 4$. If $\mathbb{H}$ would contain $p^2 + 1$ abelian components, then $\{H \cap \Omega \mid H \in \mathbb{H}, H' = 1\}$ would be a (complete) congruence partiton of Ω, that is

$$\Omega = \bigcup_{\substack{H \in \mathbb{H}, \\ H \text{ abelian}}} (H \cap \Omega).$$

By (3) any other component would intersect Ω trivially, thus, as $H \cap \Omega > 1$ for all H in $\mathbb{H}$, there do not exist any nonabelian components in $\mathbb{H}$ and therefore $r = p^2 + 1$. But this is a contradiction to $r > p^2 + p + 1$. The PCP $\mathbb{H}$ can therefore contain at most p^2 abelian components and after counting again, we see

(13'') $$|G'| \geq (r - p^2)(p-1) + 1 > p^2$$

and therefore $|G'| \geq p^3$, if $n = 4$.

Altogether we have $|G'| \geq p^{n-1}$ for all $n \geq 3$. As G' is a subgroup of $\Phi(G)$, we obtain now $|G'|, |\Phi(G)| \in \{p^{n-1}, p^n\}$ by (2.1), hence (2.4.a).

(2.4.b) If $|G'| = p^{n-1}$, then $n = 3$, $\Phi(G) = G'$ and G is isomorphic to the group in (2.4)(ii) above. Furthermore $T(G) = p + 2$.

Assume that $|G'| = p^{n-1}$. As $r(p-1) + 1 > p^{n-1}$, there exists a component N in $\mathbb{H}$ which intersects G' trivially. As a consequence, N is abelian and $N\Omega$ is an abelian maximal subgroup of G (observe that G' is a maximal subgroup of Ω and that $N \cap \Omega$ is nontrivial, whence $|N \cap \Omega| = p$).

Let H be any other component of $\mathbb{H} - \{N\}$ and $H_N := H \cap N\Omega$. By using (1) and the fact that $N\Omega$ is abelian and maximal in G, we obtain that H_N is an abelian maximal subgroup of H. Hence H_N is normal in H and in $N\Omega$ and as $HN\Omega = G$, we see that H_N is a normal subgroup of G. Thus we may apply (1.4) with $X := H_N$:

$\{ KH_N/H_N \mid K \in \mathbb{H} \}$ is a set of nontrivial subgroups of G/H_N and

(14) $$|\Phi(G) : \Phi(G) \cap H_N| \leq p^{2n} \cdot |H_N|^{-1} \cdot \left(r(p-1)+1\right)^{-1} < p^2.$$

(Observe that H_N has order p^{n-1}.) We have that $|\Phi(G) : \Phi(G) \cap H_N| \in \{1, p\}$.

If $\Phi(G) \leq H_N \leq H$, then any component different from H intersects $\Phi(G)$ trivially and is therefore elementary abelian. Using (1.6) and the fact that the abelian component N intersects Ω in a subgroup of order p, we obtain, that $|\Omega| = p^2$, hence $n = 2$, a contradiction.

We conclude that $H_N \cap \Phi(G)$ is a maximal subgroup of $\Phi(G)$. Since H has been choosen arbitrarily in $\mathbb{H} - \{N\}$ this holds for all components different from N. Thus, again with (3), we have $|\Phi(G)| \leq p^2$. By using (2.4.a) and $n \geq 3$, we see that $|\Phi(G)| \geq p^{n-1} \geq p^2$. Thus equality holds everywhere and we obtain $|\Phi(G)| = p^2$, $\Phi(G) = G'$ and $n = 3$.

Furthermore, as N intersects $\Phi(G) = G'$ trivially, we see that $\Phi(N) = 1$, thus N is elementary abelian. Also $N\Omega$, which is equal to $N\Phi(G)$, is elementary abelian.

All components different from N intersect $\Phi(G)$ nontrivially. (This is clear, if H is nonabelian. If H is abelian, then $|H \cap \Omega| = p^2$ by (1.7)(ii) and the facts that $|\Omega| = p^3$ and $|N \cap \Omega| = p$. Hence $H \cap \Omega$ and $\Phi(G)$ both are maximal subgroups of Ω and have therefore nontrivial intersection.) Thus $r \leq T(\Phi(G)) + 1 = p + 2$. By our general assumption we have equality.

Since $|\Omega| = p^3$ is not a square, $\mathbb{H}$ can contain at most 2 abelian components by (1.7)(i). Hence there exists a nonabelian component in $\mathbb{H} - \{N\}$. Furthermore $H \cap N\Omega$ is elementary abelian of order p^2 for all H in $\mathbb{H} - \{N\}$. Therefore, if $p = 2$, then any nonabelian component in $\mathbb{H} - \{N\}$ contains at least 3 elements of order 2. Thus the nonabelian components are dihedral groups of order 8. Since each of them contains exactly 5 elements of order 2, we find an element c of order 2 in H which does not lie in $N\Omega$. If p is odd then we can apply (1.8) and obtain that G is of exponent p.

Altogether, we can choose an element c of order p in $G - N\Omega$ and therefore $\langle c, N\Omega \rangle = G$. Let (a, b, x) be a basis of N where $\langle x \rangle = N \cap \Omega$ and (u, v) a basis of $\Phi(G)$ (regarded as vector spaces over GF(p)). The element c induces by conjugation a linear mapping on $N\Phi(G)$. If $w \in N$ then $w^c = w[w, c] \in wG' = w\Phi(G)$. As $N \cap \Phi(G) = 1$, we see that $w^c \in N$ if and only if c centralizes w, hence if and only if $w \in N \cap \Omega = \langle x \rangle$. Without loss of generality we can assume that $a^c = au$ and $b^c = bv$ (note that $a^{-1}a^c = [a, c]$ and $b^{-1}b^c = [b, c]$ have to be linearly independent in $\Phi(G)$ since $G' = \Phi(G)$).

Thus G is isomorphic to

$$\langle a, b, c, u, v, x \mid \text{all generators have order p; } [a, c] = u,\ [b, c] = v, \text{ all other commutators are equal to one} \rangle.$$

In order to conclude the proof of (2.4.b) it remains to show that $T(G) = p + 2$:

First let $p = 2$. Then the subgroups $N := \langle a, b, x \rangle$, $H_1 := \langle av, c, u \rangle$, $H_2 := \langle bu, cx, v \rangle$ and $H_3 := \langle abc, ux \rangle$ form an $(8,4)$-PCP in G (this example is due to A. P. SPRAGUE [13]). We remark that H_1 and H_2 are dihedral groups of order 8, N is elementary abelian and H_3 is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

If p is odd, we may again use (10) and (11) as G has class 2. Again any element in G can uniquely be written as $a^\alpha b^\beta c^\gamma u^\mu v^\nu x^\xi$ with $\alpha,\beta,\gamma,\mu,\nu,\xi$ in $GF(p)$. Let $\mathbb{H}$ be the following set of subgroups of G:

$$H_i := \langle ab^i v, cx^i v, uv^i \rangle = \{ a^\alpha b^{i\alpha} c^\beta u^\gamma v^{\alpha+\beta+i\gamma} x^{i\beta} \mid \alpha,\beta,\gamma \in GF(p) \},\ i \in GF(p);$$

$$H_\infty := \langle bc, ux, v \rangle = \{ b^\alpha c^\alpha u^\beta v^{\gamma - \binom{\alpha}{2}} x^\beta \mid \alpha,\beta,\gamma \in GF(p) \} \text{ and}$$

$$N := \langle a, b, x \rangle = \{ a^\alpha b^\beta x^\gamma \mid \alpha,\beta,\gamma \in GF(p) \}.$$

Using the standard presentation of G, it is not difficult to show that $\mathbb{H}$ is a $(p^3, p+2)$-PCP in G (we skip again the details). This proves (2.4.b).

We remark that N and H_∞ are elementary abelian and all H_i are extraspecial of exponent p.

(2.4.c) If G is special with center of order p^n, then $n = 3$, p is odd and G is isomorphic to the group in (2.4)(i). Furthermore $T(G) = p^2 + 1$.

In order to prove that $n = 3$, it is sufficient to show that $\mathbb{H}$ cannot contain two components H and K with $|H \cap \Omega| = |K \cap \Omega| = p$ provided that $n \geq 4$: Because then we obtain

$$p^n = |\Omega| \geq (r-1)(p^2-1) + p \geq (p^{n-1} - 1)(p+1) + p = p^n + p^{n-1} - 1,$$

which gives the desired contradiction.

We proceed now as in [6, section 5]. For the sake of completeness and as only the odd case is dealt with in [6], we include the proof:

Let H be a component in $\mathbb{H}$ satisfying $|H \cap \Omega| = p$, say $H \cap \Omega = \langle h \rangle$. We choose $h_1, \ldots, h_{n-1}$ in H such that $\langle h_1, \ldots, h_{n-1}, h \rangle = H$. Let $x \in G - H\Omega$. As $H\Omega$ is a maximal subgroup of G, we have $G = \langle x, H\Omega \rangle$.

If H would be abelian, then we would have $G' = Z(G) = \langle [x,h_1], \ldots, [x,h_{n-1}] \rangle$ and therefore $|G'| \leq p^{n-1}$. This is a contradiction. (Observe, that a special group has elementary abelian center and class 2 so that we again may use the bilinearity of the commutator mapping).

Thus H is nonabelian and we obtain $1 \neq \Phi(H) = H' = H \cap \Omega = \langle h \rangle$. By Burnside's basis theorem (see e.g. [9, chap. III, 3.15]) the set $\{h_1, \ldots, h_{n-1}\}$ above is a minimal system of generators of H. Without loss of generality let $[h_1, h_2] = h$.

Assume that K is a further component in $\mathbb{H}-\{H\}$ satisfying $|K\cap\Omega| = p$. By (1) there exists an element b in $K\cap (G-H\Omega)$. As above $G = \langle b, H\Omega\rangle$ and therefore $G' = \langle [b,h_1], \ldots, [b,h_{n-1}], [h_1,h_2]\rangle$. Furthermore, as G' is elementary abelian of order p^n, the n-tupel $([b,h_1], \ldots, [b,h_{n-1}], [h_1,h_2])$ is a basis of G'.

Now it is not difficult to see that $C_G(b)$, the centralizer of b in G, is $\langle b,\Omega\rangle$ and therefore abelian of order p^{n+1}. If we denote by k a generator of $\Phi(K) = K\cap Z(G)$, we obtain $C_G(b)\cap K = \langle b,k\rangle$. This group has order p^2. By using once more Burnside's basis theorem, we can choose a minimal set of generators of K containing b, e.g. let K be generated by $b, k_2, \ldots, k_{n-1}$ where $[b,k_2] = k$.

If $n \geq 4$, then the generator k_3 exists. Furthermore $k_3 \in K-\langle b,k_2\rangle$ and therefore k_3 does not centralize b. Since $K' = \langle k\rangle$ we may also assume that $[b,k_3] = k$ and obtain $[b,k_2k_3^{-1}] = [b,k_2]\,[b,k_3]^{-1} = 1$. (Here we have again used that $[\cdot,\cdot] : G\times G \longrightarrow G'$ is bilinear.) Thus $k_2k_3^{-1} \in C_G(b)\cap K = \langle b,k\rangle$ and we obtain $k_3 \in \langle b,k_2,k\rangle = \langle b,k_2\rangle$, a contradiction to the fact that k_3 together with b and k_2 belongs to a minimal set of generators of K. This gives the desired contradiction. Hence we indeed have $n = 3$.

If p is odd, then we can use (1.8) to show that $\exp(G) = p$ and it is then clear that G is isomorphic to

(15) $\langle a,b,c,x,y,z \mid$ all generators have order p; $[a,b]=x$, $[a,c]=y$, $[b,c]=z$; all other commutators are equal to one $\rangle$.

This group is investigated extencively in [6, section 6]. It is proved there that $T(G) = p^2+1$ for all odd prime numbers p.

It remains therefore to investigate the case $p = 2$. By assumption we have that $\Omega = Z(G) = G' = \Phi(G)$ is elementary abelian of order 8 and that $\mathbb{H}$ is an $(8,r)$-PCP in G with $r \geq 4$. We use an argument of A.P. SPRAGUE in [13] which leads to a contradiction and shall include a proof as this particular case is neither pointed out explicitely in [13] nor in [5].

The factor group G/Ω is elementary abelian of order 8, thus we can think of the lattice of subgroups of G/Ω as the Fano plane over GF(2). Using the same notation as in (15), let $G/\Omega := \langle a\Omega, b\Omega, c\Omega\rangle$, $[a,b] = x$, $[a,c] = y$ and $[b,c] = z$, where $\langle x,y,z\rangle = \Omega$. As at most one component meets Ω in a 2-dimensional subspace, we have at least 3 components which meet Ω in a one-dimensional subspace and see that $\mathbb{H}(\Omega) := \{H\Omega/\Omega \mid H\in\mathbb{H}\}$ contains at least 3 lines of G/Ω.

As $r \geq 4$, we even have that $\mathbb{H}(\Omega)$ contains three lines which form a triangle of G/Ω. (If $\mathbb{H}(\Omega)$ contains no triangle, then we have only three lines in $\mathbb{H}(\Omega)$ and they meet in one point of G/Ω and any other component corresponds to a point in G/Ω. But as all points are covered by these lines and as $r \geq 4$, we obtain $K\Omega \leq H\Omega$ for some different components K and H in $\mathbb{H}$, which is a contradiction to (1).)

Thus without loss of generality we can choose a coordinatization of G/Ω and H_1, H_2, H_3 in $\mathbb{H}$ such that $H_1\Omega = \langle a\Omega, b\Omega\rangle$, $H_2 = \langle a\Omega, c\Omega\rangle$ and $H_3 = \langle b\Omega, c\Omega\rangle$. Now have a look at $H_1\Omega \cap H_2\Omega = \langle a, \Omega\rangle$. As $a^2 \in H_1 \cap H_2 = 1$, we see that a has order 2. The same argument shows that likewise b and c have order 2. We can therefore present G as in (15) (with $p = 2$).

Let H_4 be a fourth component of $\mathbb{H}$. If H_4 as well would correspond to a line in G/Ω, then $H_4\Omega$ would meet at least one line of our triangle, e.g. without loss of generality $H_4\Omega \cap H_1\Omega = \langle ab, \Omega\rangle$. But as $(abw)^2 = [b,a] = [a,b] = x$ for any w in Ω, the components H_1 and H_4 would have $\langle x\rangle$ in common, a contradiction to (3).

Thus $\mathbb{H}(\Omega)$ contains no further lines of G/Ω, hence any component H_4 in $\mathbb{H}$ different from H_1, H_2 and H_3 leads to a point in G/Ω. As the point $H_4\Omega$ is not incident with the triangle by (1) and as $H_1\Omega, H_2\Omega$ and $H_3\Omega$ cover all but the point $\langle abc, \Omega\rangle$, we see that $r = 4$ and $H_4\Omega = \langle abc, \Omega\rangle$.

The definition of the commutators shows now that $H_1 \cap \Omega = \langle x\rangle$, $H_2 \cap \Omega = \langle y\rangle$ and $H_3 \cap \Omega = \langle z\rangle$. Furthermore $H_4 \cap \Omega$ has order 4 and is a subset of $\{1, xy, xz, yz, xyz\}$ because of (3). Thus $H_4 \cap \Omega = \{1, xy, xz, yz\}$. But this is a contradiction to $(H_4\Omega)^2 = \langle xyz\rangle \in H_4 \cap \Omega$ (note that $abcw \in H_4$ for some w in Ω and that $(abcw)^2 = xyz$ by using the presentation of G).

Altogether, we have proved that $T(G) \leq 3$ provided that G is a special 2-group of order 64 with center of order 8. The proof of (2.4) is now complete. □

(2.5) $\qquad |\Omega| \neq p^{n-1}$.

Proof:

Assume that $|\Omega| = p^{n-1}$. As $r(p-1)+1 > p^{n-1}$ there exists a component N in $\mathbb{H}$ which intersects Ω trivially. Thus $N\Omega$ is a maximal subgroup of G and therefore normal in G. As $N\Omega$ is isomorphic to $N \times \Omega$ we see that $\Phi(N\Omega) = \Phi(N)$. As $\Phi(N)$ is a characteristic subgroup of $N\Omega$ we see furthermore that $\Phi(N)$ is a normal subgroup of G. As nontrivial normal subgroups of G have nontrivial intersection with Ω we obtain that $\Phi(N) = 1$, thus N is elementary abelian.

We proceed now similar as in the beginning of the proof of (2.4.b):

$N\Omega$ is an elementary abelian maximal subgroup of G. Let H be any component of $\mathbb{H}-\{N\}$, then $H_N := H \cap N\Omega$ is a normal subgroup of G of order p^{n-1}. The set $\{ KH_N/H_N \mid K \in \mathbb{H} \}$ consists of nontrivial subgroups of G/H_N and as in (14), (1.4) yields $|\Phi(G) : \Phi(G) \cap H_N| \leq p^{2n} \cdot |H_N|^{-1} \cdot \big(r(p-1)+1\big)^{-1} < p^2$. An application of (1.5) and (1.6) together with remark (1.7)(ii) shows that any component H which is different from N is nonabelian. (Let $H \in \mathbb{H}-\{N\}$ and assume that H is abelian. Then $\Omega \leq H$ by (1.7)(ii) and the facts that N is abelian and $N \cap \Omega = 1$. Hence, by (3), we have $K \cap \Omega = 1$ for all K in $\mathbb{H}-\{H\}$. The argument of the beginning of the proof shows then that K is elementary abelian. Hence $\mathbb{H}$ consists only of abelian components whence $|X \cap \Omega|$ is constant for all X in $\mathbb{H}$ by (1.5) and (1.6), this is a contradiction.) Therefore $1 \neq \Phi(H)$ for all H in $\mathbb{H}-\{N\}$ and $H_N \cap \Phi(G)$ is a maximal subgroup of $\Phi(G)$. We obtain that $|\Phi(G)| = p^2$ and $r-1 \leq T(\Phi(G)) \leq p+1$. Thus $r \leq p+2$ and therefore $n=3$. By our general assumption we have $r = p+2$. In particular $\Phi(G)$ is elementary abelian.

The component N intersects $\Phi(G)$ trivially as $\Phi(G) = \bigcup_{H \in \mathbb{H}-\{N\}} H \cap \Phi(G)$. Hence $N\Omega = N\Phi(G)$.

Now fix a component H in $\mathbb{H}-\{N\}$. Let $h \in H \cap (G - N\Phi(G))$, then $\langle h, N\Phi(G) \rangle = G$. Let x be an element of N. If $x^h \in N$, then $x^{-1}x^h = [x,h] \in N \cap G' = 1$, hence h centralizes x and as $N\Omega$ is abelian this shows that $x \in N \cap \Omega = 1$. Thus no nonidentity element of N is centralized by h. As $N\Phi(G)$ is elementary abelian of order p^5 the conjugation of $N\Phi(G)$ by h is a linear mapping with respect to GF(p). Let n_1, n_2, n_3 and v_1, v_2 be bases of N and $\Phi(G)$ respectively and combine them to a basis of $N\Omega$. As a matrix with respect to this basis, the conjugation by h on $N\Phi(G)$ has the form $\begin{pmatrix} E_3 & * \\ O & E_2 \end{pmatrix}$, where $*$ is a (3×2)-matrix over GF(p) and E_3 and E_2 are the identity matrices of order 3 and 2 respectively. As the rank of $*$ is at most 2 it is not difficult to see that there exists an $x \neq 1$ in N which is fixed by h. But this leads by the argument above to a contradiction, which proves (2.5). □

In order to complete the proofs of (1.1) and (1.2), we finally show

(2.6) $\quad |\Omega| > p^{n-2}$.

Proof:

Assume that $|\Omega| \leq p^{n-2}$. Similarly to [4] we study the sets

$$\mathcal{A} := \{ H \in \mathbb{H} \mid H \cap \Omega = 1 \} \text{ and } \mathcal{A}' := \{ H \in \mathcal{A} \mid H' \neq 1 \}.$$

Since at most $(|\Omega| - 1)(p-1)^{-1}$ components of $\mathbb{H}$ intersect Ω nontrivially, we obtain

(16) $$a := |\mathcal{A}| \geq r - (|\Omega| - 1)(p-1)^{-1} .$$

By remark (1.7)(ii) and the definition, $\mathcal{A}$ can contain at most one abelian component (see also [4, step 4 and the subsequent remark]), whence

(17) $$a' := |\mathcal{A}'| \geq a - 1 \geq r - 1 - (|\Omega| - 1)(p-1)^{-1}.$$

We are now going to determine the orders of G' and $\Phi(G)$:

Let X be any subgroup of G. Since G' is a normal subgroup of G, we have that $X'^G = \{x^g \mid x \in X', g \in G\}$, the union of the conjugacy classes of elements in X' is a subset of $X^G \cap G'$.

Now let $H \in \mathcal{A}'$. Then H' is a nontrivial noncentral subgroup of G', hence $|h^G| \geq p$ for all $1 \neq h$ in $H \cap G'$. If $H \cap G'$ is of order p, say $H \cap G' = \langle h \rangle$, then $|H'^G - \{1\}| \geq (p-1)p$ (observe that $h^g \in \langle h \rangle$ if and only if $h^g = h$). The same lower bound for $|H'^G - \{1\}|$ holds trivially, if $H \cap G'$ has order at least p^2. Using (17), (1.9) and $r > (p^{n-1} - 1)(p-1)^{-1}$ we obtain therefore

$$|G'| \geq (p-1)p\,a' + |\Omega \cap G'| \geq p^n - p^{n-1} + |\Omega \cap G'|.$$

As G' is a subgroup of $\Phi(G)$ and $|\Phi(G)| \leq p^n$ by (2.1), we thus have

(2.6.a) $G' = \Phi(G)$ is of order p^n.

Next we show

(2.6.b) $\Omega \leq \Phi(G)$.

The set $\left\{ H\Omega/\Omega \mid H \in \mathbb{H} \right\}$ consists of nontrivial subgroups of G/Ω and satisfies the maximality condition (1). Hence (1.4) yields with $X := \Omega$ the following inequality

$$|\Omega : \Phi(G) \cap \Omega| \leq p^{2n} \cdot |\Phi(G)|^{-1} \cdot \left(r(p-1) + 1 \right)^{-1} < p$$

and (2.6.b) follows immediately.

We are now going to count the cardinality of $S(H) := H^G \cap \Phi(G) - \{1\} = H^G \cap G' - \{1\}$ for H in $\mathcal{A}$ a bit more carefully. As $|\Phi(G)| = p^n$, every component H intersects $\Phi(G)$ nontrivially (otherwise we would have $H\Phi(G) = G$ and therefore $H = G$). We are therefore able to use the same argument as above to show that $|S(H)| \geq p(p-1)$ for all H in $\mathcal{A}$ (here we use $S(H)$ instead of $H'^G - \{1\}$ as we now know that $S(H)$ is nonempty even if H would be abelian). We follow [4] and define

(18) $$\mathcal{B} := \{ H \in \mathcal{A} \mid |H^G \cap \Phi(G) - \{1\}| = p^2 - p \} \text{ and } b := |\mathcal{B}|.$$

As mentioned above, $\mathbb{B}$ consists exactly of the components H of $\mathcal{A}$, where $|S(H)|$ is minimal. In order to obtain some information about the cardinality b of $\mathbb{B}$, we are going to deduce lower bounds for $|S(H)|$ if $H \in \mathcal{A} - \mathbb{B}$:

Let $H \in \mathcal{A} - \mathbb{B}$ and let $X := H \cap \Phi(G)$. If X is of order p, say $X = \langle h \rangle$, then $|S(H)| \geq p^2(p-1)$ since $|h^G| = |(h^i)^G|$ for $i = 1, \ldots, p-1$ and by the definition of $\mathbb{B}$. If X has order at least p^2 and $g \in G$ does not normalize X (such an element exists as $X \leq H$ and H intersects Ω trivially by the definition of $\mathcal{A}$), then $|\{ X^y \mid y \in \langle g \rangle \}| \geq p$ and therefore

$$\Big| \bigcup_{y \in \langle g \rangle} X^y \Big| \geq \big(|X| - p^{-1}|X| \big) p + p^{-1}|X| \geq p^2(p-1) + p,$$

whence trivially $|S(H)| \geq p^2(p-1)$.

We have therefore $|S(H)| \geq p^2(p-1)$ for all H in $\mathcal{A} - \mathbb{B}$.

Using (1.9), (2.6.b) and (17) we now obtain

$$\begin{aligned} p^n = |\Phi(G)| &\geq \sum_{H \in \mathcal{A}} |S(H)| + |\Omega| \\ &\geq p^2(p-1)(a-b) + p(p-1)b + |\Omega| \\ &\geq p^2(p-1)\left(r - 1 - (|\Omega| - 1)\cdot(p-1)^{-1} \right) + p^2(p-1) - p(p-1)^2 b + |\Omega| \\ &\geq p^2(p^{n-1} - |\Omega|) - p(p-1)^2 b + p^2(p-1) + |\Omega| \end{aligned}$$

and therefore a lower bound for b:

$$p(p-1)b \geq p^n + p^2 - (p+1)|\Omega|. \tag{19}$$

If H and K are two different components of $\mathbb{B}$ with $\langle h \rangle = H \cap \Phi(G)$ and $\langle k \rangle = K \cap \Phi(G)$, then h and k are elements of order p and lie in $Z(H)$ and $Z(K)$ respectively (note that $H' = H \cap \Phi(G) = \langle h \rangle$, if H is nonabelian, whence $H' \leq Z(H)$ as H' is normal in H and thus intersects $Z(H)$ nontrivially). Now $h\Omega \neq k\Omega$. (Otherwise $h^{-1}k \in \Omega$ and therefore h and $(h^{-1}k)$ centralize H, whence $k = h(h^{-1}k)$ also centralizes H. Since $k \in Z(K)$ this yields that $k \in \Omega$ by (1), a contradiction to the choice of K.) We therefore have that $\Phi(G)/\Omega$ contains at least b different subgroups of order p. Therefore $|\Phi(G)| \cdot |\Omega|^{-1} \geq b(p-1) + 1$ and this gives a lower bound for b:

$$p(p-1)b \leq p^{n+1}|\Omega|^{-1} - p. \tag{20}$$

Comparing (19) and (20) we obtain

$$0 \geq -p^{n+1}|\Omega|^{-1} + p + p^n + p^2 - (p+1)|\Omega|.$$

With $|\Omega| := p^m$ and $i := n - m$, after some simplifications, we see

$$0 \geq (p^m - p)(p^i - p - 1).$$

By assumption $i \geq 2$, hence $p^i - p - 1 > 0$. It follows therefore that $p^m - p \leq 0$, hence $m = 1$.

We have proved

(2.6.c) $\qquad |\Omega| = p.$

Furthermore, by (19) and (20), we obtain

(21) $\qquad b = (p^{n-1} - 1)(p-1)^{-1}.$

Moreover, we can show

(2.6.d) $\qquad r = b + 1 = (p^{n-1} - 1)(p-1)^{-1} + 1.$

By (21) and the definition of $\mathbb{B}$ we have $\left| \bigcup_{H \in \mathbb{B}} \left(H^G \cap \Phi(G) - \{1\} \right) \right| = p^n - p$ and thus, with (2.6.c):

(22) $$\Phi(G) = \bigcup_{H \in \mathbb{B}} \left(H^G \cap \Phi(G) \right) \cup \Omega.$$

Hence there exists at most one component N in $\mathbb{H} - \mathbb{B}$, in which case the intersection of N with $\Phi(G)$ is Ω. Our assumption $r > (p^{n-1} - 1)(p-1)^{-1}$ and (22) now imply (2.6.d).

To conclude the proof of (2.6), we finally have to show that this situation cannot occur. We are therefore going to continue the study of the structure of G.

(2.6.e) $\qquad \Phi(G)$ is elementary abelian.

Let H be a component in $\mathbb{B}$ and let $1 \neq x$ be an element of $H^G \cap \Phi(G)$. Then x has order p and $C_G(x)$, the centralizer of x in G is a maximal subgroup of G and therefore contains $\Phi(G)$. Hence $x \in \Omega_1(Z(\Phi(G)))$. As $\{ H^G \cap \Phi(G) - \{1\} \mid H \in \mathbb{B} \} \cup \{\Omega\}$ by (22) is a partition of $\Phi(G)$, we obtain that $\Phi(G)$ is elementary abelian.

(2.6.f) $\qquad [G', G] = \Omega.$

Let $\langle h \rangle := H \cap \Phi(G)$ and $g \in G - C_G(h)$ for some component H in $\mathbb{B}$. Then $\langle h, h^g \rangle$ is elementary abelian of order p^2, normal in G and therefore contains Ω. Hence $\langle h, h^g \rangle / Z(G)$ is normal in $G/Z(G)$ and of order p whence $\langle h, h^g \rangle \leq Z_2(G)$ (where $Z_2(G)/Z(G) := Z\left(G/Z(G)\right)$). With (22) we see that $\Phi(G) \leq Z_2(G)$, hence $G/Z_2(G)$ is elementary abelian. As G' is not contained in Ω, we can now deduce that G is nilpotent of class 3. Thus $1 \neq [G', G] \leq \Phi(G) \cap Z(G) = \Omega$ and the assertion follows now from the fact that Ω has order p (see (2.6.c)).

We are now going to study the action π of G on $\Phi(G)$ by conjugation:

As $\Phi(G)$ is an n-dimensional vector space over GF(p), the action π of G on $\Phi(G)$ is a linear representation of G. The kernel C of π is the centralizer of $\Phi(G)$ in G. Let $B := (v_1, v_2, \ldots, v_n)$ be a basis of $\Phi(G)$ and $\langle v_n \rangle = \Omega$. By (2.6.f) we have $v^g = v[v,g] \in v\Omega$ for all v in $\Phi(G)$ and all g in G. Thus, in the matrix representation with respect to B, $\pi(G)$ consists of $(n \times n)$-matrices of the form $\begin{pmatrix} E_{n-1} & u \\ 0 & 1 \end{pmatrix}$, where $u \in GF(p)^{n-1}$ and E_{n-1} is the $((n-1)\times(n-1))$-identity matrix over GF(p).

In particular we obtain

(23) $$|\pi(G)| \leq p^{n-1} \text{ and } |C| \geq p^{n+1}.$$

Now $HC \neq G$ holds for every H in $\mathbb{B}$, otherwise $\langle h \rangle = H \cap \Phi(G)$ is centralized by H and C and therefore $\langle h \rangle \leq \Omega$, a contradiction. Thus we have that $\{HC/C \mid H \in \mathbb{B}\}$ satisfies the maximality condition (1) and (1.4) together with (21) yield

$$|C| \leq p^{2n} |\Phi(G) \cap C| |\Phi(G)|^{-1} \left(b(p-1)+1\right)^{-1} = p^{n+1}.$$

(Observe that $\Phi(G) \leq C$ as $\Phi(G)$ is abelian.)

Using (23) we obtain

(24) $$|\pi(G)| = p^{n-1} \text{ and } |C| = p^{n+1}.$$

Furthermore, by the definition of C and the fact that $\Phi(G)$ is an abelian maximal subgroup of C, we see that C also is abelian. As $|H \cap \Phi(G)| = p$ and $HC \neq G$ for all H in $\mathbb{B}$ we have that $H \cap C$ has order p^2 for every H in $\mathbb{B}$. Thus $\{HC \mid H \in \mathbb{B}\}$ is exactly the set of maximal subgroups of G containing C.

It is easy to see that C is elementary abelian, otherwise $\Phi(G) = \Omega_1(C)$ and $H \cap C$ is cyclic for all H in $\mathbb{B}$ and therefore all H in $\mathbb{B}$ contain $\langle x^p \mid x \in C \rangle$, which is a group of order p. But this is a contradiction to (3).

Together with the following observation we will be able to conclude the proof of (2.6):

For each K in $\mathbb{B}$ let $X_K := K \cap C$. As C is normal in G, the subgroup X_K is normal in K. Since C is abelian, we obtain that both K and C are subgroups of $N_G(X_K)$, the normalizer of X_K in G. As X_K is not normal in G and as KC is a maximal subgroup in G, we indeed have equality :

(25) $$N_G(K \cap C) = KC \text{ for all } K \text{ in } \mathbb{B}.$$

Hence $S(X_K) := \{ X_K^g \mid g \in G \}$, the set of subgroups in G which are conjugate to X_K, has cardinality p. It is clear that $S(X_K)$ consists of subgroups of C.

Assume that all members of $S(X_K)$ are mutually disjoint for all K in $\mathbb{B}$. By using (1.9), we then obtain

$$p^{n+1} - 1 = |C| - 1 \geq \sum_{K \in \mathbb{B}} \sum_{X \in S(X_K)} \left(|X| - 1 \right) = bp(p^2 - 1)$$
$$= (p^{n-1} - 1)p(p+1) = p^{n+1} + p^n - p^2 - p,$$

which is a contradiction to $n \geq 3$.

Therefore there exists a component H in $\mathbb{B}$ such that $S(X_H)$ is a set of subgroups of C which are not mutually disjoint. Moreover, all members of $S(X_H)$ have a one-dimensional subspace in common.

We choose such a component H in $\mathbb{B}$ and a basis $(v_0, v_1, v_2, \ldots, v_n)$ of C such that $\langle v_0, v_1 \rangle = H \cap C$, $\langle v_n \rangle = \Omega$ and $\langle v_1, v_2, \ldots, v_n \rangle = \Phi(G)$ (in particular $\langle v_1 \rangle = H \cap \Phi(G)$). Let $g \in G - HC$. The one-dimensional subspace of $X_H = H \cap C$ which is fixed by the conjugation with g is of course not $\langle v_1 \rangle$ (note that $HC = H\Phi(G)$ is exactly the centralizer of $\langle v_1 \rangle$ in G). Without loss of generality we may therefore assume that v_0 commutes with g. Furthermore, by (2.6.f) and the fact that $\Omega = \langle v_n \rangle$, we may assume that $v_1^g = v_1 v_n$.

Next we show that v_0 lies in the center of H:

Let τ denote the action of G on C by conjugation. As C is abelian, C lies in the kernel of τ. Since $\Phi(G) \leq C$, we have that kernel$(\tau) \leq$ kernel$(\pi) = C$, hence kernel$(\tau) = C$. The image $\tau(G)$ is therefore isomorphic to G/C, hence elementary abelian of order p^{n-1}. Now for any h in H we have

$$v_0^{\tau(h)} = v_0^h = v_0 [v_0, h] \in v_0 \left(H \cap G' \right) = v_0 \langle v_1 \rangle.$$

If $v_0^h = v_0 v_1$ for some h in H, then, with g as above, $v_0^{\tau(h)\tau(g)} = v_0^{hg} = (v_0 v_1)^g = v_0 v_1 v_n$. But $\tau(G)$ is abelian, whence also $v_0^{\tau(h)\tau(g)} = v_0^{\tau(g)\tau(h)} = v_0^{gh} = v_0^h = v_0 v_1$. This is a contradiction and therefore v_0 is indeed an element of the center of H.

This finally leads to a contradiction which proves (2.6):

As also g and C centralize v_0, we see that $G = \langle g, HC \rangle \leq C_G(v_0)$ and therefore $v_0 \in Z(G)$. But this not possible by the choice of H. □

Theorems (1.1) and (1.2) are now completely proved.

3. Concluding remarks

We conclude this paper with some remarks:

A partial congruence partition is called maximal, if it cannot be enlarged by adding a further component. Most of the known examples of maximal PCPs contain at least one normal component (see [6, 7]). Partial congruence partitions with at least one normal component are very interesting objects which are studied from a geometric and a group theoretic point of view in [8] and [7] respectively (the reader is refered to [8], where the connection of such PCPs to translation nets with transitive directions is discussed). This situation occurs also in our examples which prove (1.2.b) and (1.2.c):

The proof of (2.3) shows, that each PCP in $E(p^3) \times EA(p^3)$ (the group in (1.2.b)) of maximal possible degree $p+2$ contains a normal component which is isomorphic to $E(p^3)$ (see e.g. the concrete example in (12)). The partial congruence partitions in the special group of order p^6, exponent p and center of order p^3 (see (1.2.c)) constructed in [6, section 6] likewise contain one normal component.

The group G in (1.2.d) is the only example known to the author where the PCPs of largest possible degree do not contain any normal component. (This can easily be shown by using (1.7) and the fact that there exists an elementary abelian component intersecting $\Phi(G)$ trivially. We do not want to go into further detail here.)

The group $G = E(p^3) \times EA(p^3)$ in (1.2.b) is also quite interesting because of the following reason: As far as the author knows it is the first example of a maximal PCP containing a normal component which has degree not of the form $p^k + 1$ (for a suitable positive integer k). All maximal PCPs constructed in [7] have a degree of this form.

We finally want to mention that we do not know any example of a group G of order p^{2n} with $n \geq 4$ satisfying $T(G) = (p^{n-1}-1)(p-1)^{-1}$ (equality in the statement of Theorem (1.1)). Starting with $r = (p^{n-1}-1)(p-1)^{-1}$, the proof of (1.1) shows that a lot of further cases would have to be investigated. It seems therefore to be suggestive to look for examples in groups of order p^8 (the case $n = 4$) first.

The constructions in [7] show, that for small n there exist examples of groups G of odd order where T(G) comes quite close to the bound in (1.1):

- For any odd prime number p there exists a nonabelian group X of order p^8 satisfying $T(X) \geq p^2 + 1$. (Note that $T(X) \leq p^2 + p + 1$ by (1.1)).
- For any odd prime number p there exists a nonabelian group Y of order p^{12} satisfying $T(Y) \geq p^4 + 1$. (Note that $T(Y) \leq p^4 + p^3 + p^2 + p + 1$ by (1.1)).

If $p = 2$, then again by a construction in [7], there exists a nonabelian group Z of order 2^{12} satisfying $T(Z) \geq 9$. (By (1.1) we have $T(Z) \leq 31$.)

References :

1. R. A. BAILEY and D. JUNGNICKEL,
Translation nets and fixed - point - free group automorphisms,
J. Comb. Th. Ser. A 55 (1990), 1 - 13.

2. T. BETH, D. JUNGNICKEL and H. LENZ,
"Design Theory",
Cambridge Univ. Press, Cambridge, 1986.

3. J. DILLON,
Elementary Hadamard difference sets,
in "Proc. 6th Southeastern Conference on Combinatorics, Graph Theory and Computing", Utilitas Math., Winnipeg, 1975, 237 - 249.

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. Comb. Th. Ser. A 51 (1989), 138 - 141.

6. D. HACHENBERGER,
On the existence of translation nets,
(1991) to appear in J. Algebra.

7. D. HACHENBERGER,
Constructions of large translation nets with nonabelian translation groups,
(1991) to appear in Designs, Codes and Cryptography.

8. D. HACHENBERGER and D. JUNGNICKEL,
Bruck Nets with a transitive direction,
Geometriae Dedicata 36 (1990), 287 - 313.

9. B. HUPPERT,
"Endliche Gruppen I",
Springer, Berlin - Heidelberg - New York, 1967.

10. D. JUNGNICKEL,
Existence results for translation nets,
in "Finite geometries and designs",
London Math. Soc. Lecture Notes 49 (1981),
Cambridge University Press, 172 - 196.

11. D. JUNGNICKEL,
Existence results for translation nets II,
J. Algebra 122 (1989), 288 - 298.

12. D. JUNGNICKEL,
Latin squares, their geometries and their groups. A Survey,
in "Coding Theory and Design Theory II " (ed. D.K. Ray - Chaudhuri),
166 - 225, Springer, 1990.

13. A.P. SPRAGUE,
Translation nets,
Mitt. Math. Sem. Gießen 157 (1982), 46 - 68.