PROOF OF THE PRIME POWER CONJECTURE FOR PROJECTIVE PLANES OF ORDER $n$ WITH ABELIAN COLLINEATION GROUPS OF ORDER $n^2$

AART BLOKHUIS, DIETER JUNGNICKEL, AND BERNHARD SCHMIDT

(Communicated by Stephen D. Smith)

Abstract. Let $G$ be an abelian collineation group of order $n^2$ of a projective plane of order $n$. We show that $n$ must be a prime power, and that the $p$-rank of $G$ is at least $b+1$ if $n = p^b$ for an odd prime $p$.

1. Introduction

The purpose of this note is a surprisingly elementary proof of the following result.

Theorem 1.1. Let $G$ be an abelian collineation group of order $n^2$ of a projective plane of order $n$. Then $n$ is a prime power, say $n = p^b$. If $p > 2$, then the $p$-rank of $G$ is at least $b + 1$.

Theorem 1.1 is the most conclusive known result in the context of the prime power conjecture for projective planes. Let us consider some background. Among other things, Dembowski and Piper [3] showed that there are only three possible types of projective planes of order $n$ with abelian collineation groups $G$ of order $n^2$. These are translation planes, dual translation planes and the so-called type (b) planes. By a classical result of André [1], in the case of translation planes and dual translation planes, the collineation group $G$ is always an elementary abelian $p$-group. Following [3], a projective plane of order $n$ is called a type (b) plane if it has an abelian collineation group of order $n^2$ whose orbits on the point set $P$ are $\{p\} \setminus \{p\}$ and $P \setminus L$ where $(p, L)$ is a suitable incident point-line pair. In this case, we call $G$ a group of type (b). Such groups exist for all prime powers $n$, see [2] or [7]. As a consequence of the prime power conjecture for projective planes, it has been conjectured that groups of type (b) only exist for prime powers $n$. Combining the results of André and Dembowski and Piper, we have the following.

Result 1.2 ([1, 3]). Let $\Pi$ be a projective plane of order $n$ with an abelian collineation group $G$ of order $n^2$. Then one of the following holds.

(a) $\Pi$ is a translation plane or its dual, $n$ is a prime power and $G$ is elementary abelian.

(b) $\Pi$ is a plane of type (b).
Groups of type (b) are closely related to planar functions. Let $H$ and $K$ be groups of order $n$. A planar function of degree $n$ is a map $f : H \to K$ such that for every $h \in H \setminus \{1\}$ the induced map $f_h : x \mapsto f(hx)f(x)^{-1}$ is bijective. If a planar function from $H$ to $K$ exists, then $H \times K$ is a group of type (b); see [3, 7]. Thus Theorem 1.1 implies the following.

**Corollary 1.3.** If there is a planar function of degree $n$ between abelian groups, then $n$ is a prime power.

The prime power conjecture for planar functions has been studied in many papers. The best result previous to Corollary 1.3 is due to S.L. Ma [6].

## 2. Proof of the result

A good way to talk about collineation groups of type (b) is to use the group ring. We first introduce the necessary notation. Let $G$ be a multiplicatively written finite group with identity element 1. For $X = \sum a_g g \in \mathbb{Z}[G]$ we write $|X| = \sum a_g$, $X^{(i)} = \sum a_g g^i$ and $[X]_1 = a_1$ (the coefficient of 1 in $X$). For $r \in \mathbb{Z}$ we write $r$ for the group ring element $r \cdot 1$, and for $S \subset G$ we write $S$ instead of $\sum g \in S g$. It is well known [3] that an abelian group $G$ of order $n^2$ is a group of type (b) on a suitable projective plane of order $n$ if and only if there are a subgroup $N$ of order $n$ of $G$ and an $n$-subset $D$ of $G$ such that

$$(1) \quad DD^{(-1)} = n + G - N$$

in $\mathbb{Z}[G]$. The set $D$ is called an $(n, n, n, 1)$ difference set in $G$ relative to $N$.

We prepare the proof of our main result with two lemmas. Let $G$ be a finite abelian group, and let $p$ be a prime. By $r_p(G)$ we denote the $p$-rank of $G$, i.e. the minimum number of generators of the Sylow $p$-subgroup of $G$.

**Lemma 2.1.** Let $G$ be a finite abelian group, let $N$ be a subgroup of $G$, and let $p$ be a prime. Then

$$[G^{(p)}]_1 = p^{r_p(G)}, \quad [G^{(p)}N]_1 = p^{r_p(G/N)}|N|.$$  

*Proof.* Straightforward checking.

**Lemma 2.2.** Let $G$ be an abelian group, let $D \in \mathbb{Z}[G]$ with $|D| = k$ and

$$DD^{(-1)} = k + X, \quad DX = aG$$

for some integer $a$ and $X \in \mathbb{Z}[G]$. Furthermore, let $p \geq 3$ be a prime dividing $k$. Then

$$(p - 1)k^2 \leq k|X + X^{(p)}|_1 + [XX^{(p)}]_1$$

with equality if and only if $D^{(-1)}D^{(p)}$ has coefficients 0 and $p$ only.

*Proof.* Write $A := D^{(-1)}D^{(p)} = \sum a_g g$. Then $\sum a_g = k^2$. Since $G$ is abelian, we have $D^{(p)} = D^p$ in $\mathbb{Z}_p[G]$. As $k$ is divisible by $p$, we get

$$A = (k + X)D^{p - 1} = XD^{p - 1} = aGD^{p - 2} = akGD^{p - 3} = 0$$
in \( Z_p[G] \). Hence all \( a_g \) are divisible by \( p \), and thus
\[
\sum a_g^2 \geq p \sum a_g = pk^2
\]
with equality if and only if \( a_g \in \{0, p\} \) for all \( g \). On the other hand, we have
\[
AA^{(-1)} = (k + X)(k + X^{(p)}) = k^2 + k(X + X^{(p)}) + XX^{(p)}
\]
and thus
\[
\sum a_g^2 = [AA^{(-1)}]_1 = k^2 + k[X + X^{(p)}]_1 + [XX^{(p)}]_1.
\]
This proves the lemma.

Now we are ready to prove our main result.

**Theorem 2.3.** Let \( D \) be the relative difference set satisfying (1), and let \( p \geq 3 \) be a prime divisor of \( n \). Then
\[
(p - 2)n \leq p^{r_p(G)} - p^{r_p(N)} - p^{r_p(G/N)}.
\]

**Proof.** Since \(|D| = n\), (1) implies that \( D \) contains exactly one element of each coset of \( N \) in \( G \), i.e.
\[
DN = G.
\]
Because of (1) and (2), we can apply Lemma 2.2 with \( X = G - N \) and \( k = n \). Note that \([X + X^{(p)}]_1 = p^{r_p(G)} - p^{r_p(N)}\), using Lemma 2.1. Furthermore, \([XX^{(p)}]_1 = [(n^2 - n)G - G^{(p)} N + nN]_1 = n^2 - np^{r_p(G/N)}\), again using Lemma 2.1. Thus Lemma 2.2 gives us
\[
(p - 1)n^2 \leq n(p^{r_p(G)} - p^{r_p(N)}) + n^2 - np^{r_p(G/N)}.
\]
Subtracting \( n^2 \) and dividing by \( n \) gives the assertion.

**Proof of Theorem 1.1.** In view of Result 1.2, we can assume that \( G \) is a group of type (b). It is shown in [4] that \( n \) must be a power of 2 if \( n \) is even. Thus we can assume that \( n \) is odd. If \( n \) is not a prime power, then there is a prime divisor \( p \geq 3 \) of \( n \) such that the Sylow \( p \)-subgroup \( S \) of \( G \) has order less than \( n \). But then \( p^{r_p(G)} \leq |S| < n \), contradicting Theorem 2.3. Thus \( n \) is a prime power, say \( n = p^b \) where \( p \) is an odd prime. Theorem 2.3 shows \( p^{r_p(G)} > n \), and so \( G \) must have rank at least \( b + 1 \).

**References**


DEPARTMENT OF MATHEMATICS AND COMPUTING SCIENCE, EINDHOVEN UNIVERSITY OF TECHNOLOGY, DEN DOLECH 2, P.O. BOX 513, 5600 MB EINDHOVEN, NETHERLANDS
E-mail address: aart@win.tue.nl

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT AUGSBURG, UNIVERSITÄTSSTRASSE 14, 86135 AUGSBURG, GERMANY
E-mail address: jungnickel@math.uni-augsburg.de

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT AUGSBURG, UNIVERSITÄTSSTRASSE 14, 86135 AUGSBURG, GERMANY
E-mail address: schmidt@math.uni-augsburg.de