GLASNIK MATEMATIČKI
Vol. 41(61)(2006), 115 – 140

CONFIGURATIONS DEFINED ON FINITE RINGS

Andrzej Kozłowski and Krzysztof Prażmowski
University of Białystok, Poland

Abstract. Some configurations defined as structures of orbits under families of linear maps of cyclic rings are introduced and studied. All the admissible families which yield a connected configuration with small lines (of size 3 or 4) over the ring $\mathbb{Z}_{p^n}$ with prime p are found and characterized. The automorphisms of rank 3 configurations of this type are determined.

Introduction

Quite frequently geometrical structures of various types can be defined in terms of some families of transformations. As one of the most important examples we quote the construction of the structure of graphs of a sufficiently transitive transformation group (cf. [2, 10]) which, in particular cases, yields affine planes and Minkowskian planes. Another construction of this kind can be found in [2]: the family of blocks of a chain geometry is the orbit of some "typical" chain under the group of projective transformations of the projective line over a ring; these two constructions were further generalized, e.g. in [4, 8]. Closer to the subject of our paper is the André construction (cf. [1]); here, given a transformation group G of a set X we define blocks to be all orbits $G_{\langle x\rangle}[y]\cup\{x\}$ of elements y of X under point stabilizers $G_{\langle x\rangle}$ $(x\neq y)$, suitably completed.

To obtain an interesting incidence structure the underlying family of transformations need not to be a group. For example, in [7] incidence structures with blocks which are graphs of polynomial functions were successfully studied. Other examples, more important for us, as exactly these are generalized in our paper, are incidence structures determined by difference sets. Recall that given a difference set D in a group G (cf. [3, Chapter VI], [6]) we

2000 *Mathematics Subject Classification.* 51E14, 51E26.
Key words and phrases. Cyclic ring, (quasi) difference set, partial linear space, hank of polygons.

define blocks as all cosets Dg with $g \in G$. Under certain assumptions on D this construction produces linear spaces. Replacing these assumptions with some weaker ones we obtain the notion of a *quasi difference set*, and then the incidence structure determined by a quasi difference set is a partial linear space (see [9] for details). It is evident that blocks Dg can be seen as orbits of elements of G under some family of translations of G.

In the paper we consider incidence structures with blocks which are orbits of elements of a finite commutative ring $\mathfrak{R}$ under some family F of "affine" maps of $\mathfrak{R}$. Clearly, some limitations must be imposed upon this general project. First, it seems reasonable to consider families F of two types only, consisting of maps f of the form $f(x) = ax+b$ with either common coefficient a, or common coefficient b. The first approach yields the structure which is just a substructure of the structure determined by a quasi difference set in the additive group of $\mathfrak{R}$ and thus its geometry can be simply derived from the already known geometry. Consequently, in the paper we concentrate ourselves on families F of the second type and after that we restrict ourselves mainly to the rings $\mathfrak{R} = \mathbb{Z}_{p^n} = \mathbb{Z}/p^nZ$ for a prime number p. It seems that in this case we can obtain the most regular, new, and interesting incidence structures; in particular, some interesting partial linear spaces. Finally, we consider in some details only structures with small blocks (of rank $\boldsymbol{\kappa} = 3$ and $\boldsymbol{\kappa} = 4$). The case $\boldsymbol{\kappa} = 5$ is only mentioned, and $\boldsymbol{\kappa} > 5$ is passed over.

Principal results obtained in the paper can be sketched as follows. Let F be a family of linear maps f of the ring $\mathbb{Z}_{p^n}$ of the form $f(x) = ax$. In Section 2 we give some general necessary (Proposition 2.5) and sufficient (Proposition 2.14) conditions for the set of coefficients of elements of F which assure that the resulting incidence structure is a connected partial linear space of the given size of lines $\boldsymbol{\kappa} = |F|$ and we establish parameters of the obtained structures (Propositions 2.10, 2.9). Explicit formulas which characterize families F determining partial linear spaces of rank $\boldsymbol{\kappa} = 3$ (Theorem 3.3) and of rank $\boldsymbol{\kappa} = 4$ (Theorem 5.4, Lemma 5.1) are given in Sections 3 and 5. In the case $\boldsymbol{\kappa} = 4$ some additional assumptions on p are necessary for the existence of a suitable family F (Propositions 5.2, 5.6). Since the arising incidence structures with $\boldsymbol{\kappa} = 3$ have an interesting fractal-like structure we pay some more attention to them and in Example 3.4 and Section 4 we roughly explain their shape and the structure of their automorphism group. In Section 6 some conditions are found, which are necessary to obtain a connected partial linear space of rank $\boldsymbol{\kappa} = 5$ with the method proposed in the paper (Theorem 6.1, Fact 6.2), and some examples are given, but the problem to characterize all the admissible families F remains open. In the closing Section 7 we discuss again the general case of arbitrary finite $\boldsymbol{\kappa}$ and indicate the way how to decompose the resulting partial linear space into some cyclic subconfigurations.

1. General construction

Let X be a nonempty set and $F = \{F_1, \dots, F_l\}$ be a finite set of maps defined on X. For $x \in X$ we write

$$F[x] = \{f(x)\colon f \in F\}$$

and then we set

$$\mathcal{F} = F[X] = \{F[x]\colon x \in X\}.$$

Let us recall a standard example of the above construction, frequently used to define finite configurations.

Example 1.1. Let D be a quasi difference set in an abelian group $\mathfrak{G} = \langle G, +, \theta\rangle$ i.e. assume that for every $g \in G$, $g \neq \theta$ there is at most one pair $(d_1, d_2) \in D \times D$ with $g = d_1 - d_2$ (see [9]). To every $g \in G$ we assign the translation τ_g over $\mathfrak{G}$, $\tau_g(x) = x + g$. Set $X = G$ and $F = \{\tau_d\colon d \in D\}$. Then $\langle X, F[X]\rangle =: \mathbf{D}(\mathfrak{G}, D)$ is a partial linear space with lines of the size $\boldsymbol{\kappa} = |D|$. If $\mathfrak{G}$ is a cyclic group, we call $\mathbf{D}(\mathfrak{G}, D)$ *a cyclic configuration.*

In the sequel we shall analyze some particular classes of structures which can be represented in the form $\langle Z_k, \mathcal{F}\rangle$ with $\mathcal{F}$ being a family of linear maps defined over a cyclic ring $\mathbb{Z}_k = \mathbb{Z}/kZ$. Formally, elements of $\mathbb{Z}_k$ are classes $x + kZ$ with $x \in Z$. However, it will be more convenient to us to consider elements of the ring $\mathbb{Z}_k$ as integers in $\{0, 1, \dots, k-1\} =: Z_k$, with addition and multiplication defined modulo k (in particular, consequently, if $k_1 | k_2$ then elements of $\mathbb{Z}_{k_1}$ are simply elements of $\mathbb{Z}_{k_2}$ as well).

We use the symbol $[x]_k$ for the remainder of x modulo k, and $\left(\frac{x}{p}\right)$ stands for the Legendre symbol. By $\mathrm{GCD}(a, b)$ we denote the greatest common divisor of a, b. Let Z_k^* stand for the set of all invertible elements of $\mathbb{Z}_k$; clearly, it is a (multiplicative) group (denoted by $\mathbb{Z}_k^*$). It is seen that

$$\begin{aligned} Z_k^* &= \{x \in Z_k\colon x \neq 0,\ \mathrm{GCD}(x, k) = 1\} \text{ and} \\ Z_k \setminus Z_k^* &= \{x \in Z_k\colon x \cdot y \equiv 0 \mod k \quad \text{for some } y \in Z_k \setminus \{0\}\}. \end{aligned}$$

We write φ for the Euler function; $\varphi(k)$ is the number of integers x such that $x < k$ and $\mathrm{GCD}(k, x) = 1$. In other words, $\varphi(k) = |Z_k^*|$.

The following is a folklore:

Fact 1.2 (see [5]). *Let $a \in Z_k$ be an integer with $\mathrm{GCD}(a, k) = 1$. Then $a^{\varphi(k)} \equiv 1 \mod k$, and thus the the rank r of the cyclic group $\langle a\rangle$ generated by a in Z_k^* divides $\varphi(k)$. In particular, if $k = p^n$ is a prime power, then the group Z_k^* is cyclic.*

Since most of our results concern incidence structures defined over the ring $\mathbb{Z}_{p^n}$ where $p \neq 2$ is a prime number we briefly recall some representation of elements of $\mathbb{Z}_{p^n}$, which will be useful in the sequel. Namely, for every $x \in Z_{p^n}$ there are (uniquely determined) $x_0, \dots, x_{n-1} \in Z_p$ such that

$$x = x_{n-1}p^{n-1} + \dots x_1 p + x_0. \tag{1.1}$$

Indeed, $x_0 = [x]_p$, $x_1 p + x_0 = [x]_{p^2}$, and so on. It is seen that if x has form (1.1), then $x \in Z^*_{p^n}$ iff $x_0 \neq 0$ (this observation simply justifies that $|Z^*_{p^n}| = p^{n-1}(p-1)$). Generally, if $1 \leq m < n$, then $p^m \mid x$ iff $x_0 = \ldots = x_{m-1} = 0$ (and $x_m, \ldots, x_{n-1}$ are arbitrary). Consequently,

$$|\{x \in Z_{p^n} : p^m \mid x\}| = p^{n-m}. \tag{1.2}$$

We write $\mathcal{Z}^{(m)}_{p^n} = \{p^m d \in Z_{p^n} : d \in Z^*_{p^n}\}$ with $m = 0, \ldots, n$. Clearly, $\mathcal{Z}^{(0)}_{p^n} = Z^*_{p^n}$ and $\mathcal{Z}^{(n)}_{p^n} = \{0\}$. It is seen that elements of $\mathcal{Z}^{(m)}_{p^n}$ $(m < n)$ can be characterized as those $x \in Z_{p^n}$ which satisfy $p^m \mid x$, $p^{m+1} \nmid x$. Evidently,

$$|\mathcal{Z}^{(m)}_{p^n}| = p^{n-m-1}(p-1). \tag{1.3}$$

2. "Quasi difference sets" in the multiplicative structure of a ring

Let $\mathcal{A} = \{a_1, \ldots, a_l\} \subseteq Z_k \setminus \{0\}$. We define functions F_i by the formula $F_i(x) = a_i \cdot x$ and we put $F = \{F_i : i = 1 \ldots, l\}$. Then we consider the family of blocks

$$\mathcal{F} = F[Z_k \setminus \{0\}] = \{F[x] : x \in Z_k,\ x \neq 0\}$$

and, finally, we set

$$\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A}) := \langle Z_k, \mathcal{F} \rangle.$$

To avoid the trivial case when F is a set of affine maps of a field, in the sequel we assume that $\mathbb{Z}_k$ *is not a field* (i.e. k is not a prime number).

In this section we first establish properties of the set $\mathcal{A}$ which assure that the incidence structure $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ satisfies certain natural geometrical conditions: namely, to be a connected structure without isolated points with the constant rank of its blocks. (Recall that a point q of an incidence structure $\mathfrak{M}$ is isolated if no block passes through q, and the structure $\mathfrak{M}$ is connected if any two its points can be joined by a polygonal path i.e. by a sequence of blocks such that any two consecutive blocks in this sequence share a point.)

Lemma 2.1. *The following conditions are equivalent:*

(i) $|F[x]| = l$ *for every* $x \in Z_k \setminus \{0\}$;

(ii) $(a_i - a_j) \in Z^*_k$ *for every* $i, j = 1, \ldots, l$ *with* $i \neq j$.

Proof. Evidently, $|F[x]| < l$ for some $x \neq 0$ is equivalent to $a_i x = a_j x$ for some i, j, i.e. to $(a_i - a_j)x = 0$ for some $i \neq j$ and some $x \neq 0$. □

Lemma 2.2. *The structure* $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ *has isolated points iff* $\mathcal{A} \cap Z^*_k = \emptyset$. *If* $a \in \mathcal{A} \cap Z^*_k$ *then* $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A}) \cong \mathbf{D}^*(\mathbb{Z}_k, a^{-1} \cdot \mathcal{A})$ *and, clearly,* $1 \in a^{-1} \cdot \mathcal{A}$.

Proof. Let $\mathcal{A} \cap Z^*_k = \emptyset$; then $F[x] \cap Z^*_k = \emptyset$ for every $x \in Z_k$ so, points in Z^*_k are isolated.

If $a \in \mathcal{A} \cap Z^*_k$ then the map $x \longmapsto a^{-1}x$ is an isomorphism of $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ onto $\mathbf{D}^*(\mathbb{Z}_k, a^{-1} \cdot \mathcal{A})$, and evidently, the latter has no isolated points. □

In view of Lemma 2.2, in the sequel we shall assume that $a_1 = 1 \in \mathcal{A}$.

LEMMA 2.3. *Let $\mathcal{A} \subseteq Z_k^*$. Then $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ is not connected.*

PROOF. Assume that $\mathcal{A} \subseteq Z_k^*$. Then, for every $x \in Z_k$, $x \neq 0$ either $x \in Z_k^*$, and then $F[x] \subseteq Z_k^*$, or $x \in Z_k \setminus Z_k^*$, and then $F[x] \cap Z_k^* = \emptyset$. Consequently, if $x \in Z_k^*$ and $y \notin Z_k^*$, then x and y cannot be connected by a polygonal path. □

The following observation appears useful in the sequel.

FACT 2.4. *Let $a_1, a_2 \in \mathcal{A}$, $a_1 \neq a_2$, and $a_1, a_2 \notin Z_{p^n}^*$. Then $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is not a partial linear space with all lines of the same size.*

PROOF. From assumptions, $a_i = p^{k_i} t_i$ for $i = 1, 2$ and $t_i \in Z_{p^n}^*$, $k_i \in \mathbb{N} \setminus \{0\}$. Then $p \mid p(p^{k_1 - 1} t_1 - p^{k_2 - 1} t_2) = a_1 - a_2$, which contradicts Lemma 2.1. □

Therefore, if we want $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ to be a connected partial linear space with constant line rank we must assume that $\mathcal{A}$ has *exactly one* element $a \in Z_{p^n} \setminus Z_{p^n}^*$, $a \neq 0$.

For every $\mathcal{A} \subseteq Z_k$ we set $\mathcal{A}^* = \mathcal{A} \cap Z_k^*$. Since $\mathbb{Z}_k^*$ is a multiplicative group we can consider the incidence structure $\mathbf{D}(\mathbb{Z}_k^*, \mathcal{A}^*)$, which is a substructure of $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ – blocks of $\mathbf{D}(\mathbb{Z}_k^*, \mathcal{A}^*)$ are parts of some blocks of $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$.

If $\mathbf{D}^*(\mathbb{Z}_k, \mathcal{A})$ is a partial linear space, then $\mathbf{D}(\mathbb{Z}_k^*, \mathcal{A}^*)$ must be a partial linear space as well. To this aim $\mathcal{A}^*$ must be a quasi difference set in the multiplicative group $\mathbb{Z}_k^*$, which means that the following must hold:

$$c_1' c_1''^{-1} = c_2' c_2''^{-1} \quad \text{yields that} \quad c_1' = c_2',\ c_1'' = c_2'',\ \text{or } c_1' = c_1'',\ c_2' = c_2'', \quad \text{for all } c_1', c_2', c_1'', c_2'' \in \mathcal{A}^*. \tag{2.1}$$

Note that the assumptions of (2.1) can be written, equivalently, in the form $c_1' c_2'' = c_2' c_1''$. Note also (cf. Fact 1.2) that $\mathbf{D}(\mathbb{Z}_{p^n}^*, \mathcal{A}^*)$ is, in fact, a cyclic configuration defined on the cyclic group $C_{(p-1)p^{n-1}}$.

In the sequel we shall analyze some types of incidence structures of the form $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ defined over the ring $\mathbb{Z}_{p^n}$, where $p > 2$ is a prime number and n a positive integer. Not necessarily all of them will be partial linear spaces. Nevertheless, we believe that all of them are of some interest. In view of Lemmas 2.1, 2.2, 2.3, and Fact 2.4 to obtain geometrically reasonable structures we always assume that the set $\mathcal{A} \subset Z_{p^n} \setminus \{0\}$ fulfills the following conditions:

$$\mathcal{A} = \{c_0, c_1, \ldots, c_{l+1}\} \quad \text{with } c_0 = 1,\ c_i \in Z_{p^n}^* \text{ for } i = 1, \ldots, l, \text{ and } c_{l+1} \notin Z_{p^n}^*; \tag{2.2}$$

$$c_i - c_j \in Z_{p^n}^* \quad \text{for all } 0 \leq i < j \leq l + 1. \tag{2.3}$$

Our *main* goal is to construct (and investigate) some *partial linear spaces* which can be presented in the form $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$. Let us start with some more properties of $\mathcal{A}$ that are necessary to this aim.

PROPOSITION 2.5. *Let $\mathcal{A}$ have form (2.2), where $c_{l+1} = bp^m$ with $b \in Z^*_{p^n}$ for some $1 \leq m < n$. Assume that (2.3) holds and set $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$. Moreover, assume that $\mathfrak{M}$ is a partial linear space.*

(i) For every $i = 1, \ldots, l$ there is a permutation α_i of the set $L := \{0, \ldots, l\}$ such that

$$\alpha_i(i) = 0 \text{ and } c_j \equiv c_i c_{\alpha_i(j)} \mod p^m \tag{2.4}$$

for every $j \in L$.

(ii) If $c_i = c_j c_t + p^\mu d$ for some $d \in Z^*_{p^n}$ and $j, t \neq 0$, then $\mu \leq m$.

(iii) Consequently, we can write $c_i = c_j c_{\alpha_i(j)} + p^m d_{i,j}$ for some $d_{i,j} \in Z^*_{p^n}$.

PROOF. (i) Let $x = p^{n-m}$ and $y = c_i p^{n-m}$ for $i \in \{1, \ldots, l\}$. Consider the lines $F[x]$ and $F[y]$ of $\mathfrak{M}$. It is seen that $0 = c_{l+1}x = c_{l+1}y$ and $c_i p^{n-m} = c_i x = c_0 y$ are their common points so, $F[x] = F[y]$. In particular, for every $j \in L$, $c_j x \in F[y]$, i.e. $c_j x = c_i c_{\alpha_i(j)} x$ for some (unique) $\alpha_i(j)$. This yields $p^{n-(n-m)} \mid (c_j - c_i c_{\alpha_i(j)})$, as required.

(ii) Suppose that $c_i \equiv c_j c_t \mod p^\mu$ for some $\mu > m$. Then $c_i p^{n-\mu} \equiv c_j c_t p^{n-\mu} \mod p^n$ so, the lines $F[p^{n-\mu}]$ and $F[c_t p^{n-\mu}]$ of $\mathfrak{M}$ have two points $c_i p^{n-\mu}$ and $c_t p^{n-\mu}$ in common. Therefore, $F[p^{n-\mu}] = F[c_t p^{n-\mu}]$; in particular $\{bp^{n-\mu+m}\} = F[p^{n-\mu}] \cap \mathcal{Z}^{(n-\mu+m)}_{p^n} = F[c_t p^{n-\mu}] \cap \mathcal{Z}^{(n-\mu+m)}_{p^n} = \{c_t bp^{n-\mu+m}\}$. This gives, however, $p^{\mu-m} \mid b(c_t - 1)$, which is impossible.

(iii) is an immediate consequence of (i) and (ii). □

The condition 2.5(i) can be expressed in a less elementary, but much more elegant way as follows:

COROLLARY 2.6. *Under assumptions of Proposition 2.5 the set $\mathcal{A}^*$ yields a subgroup $\mathcal{A}^* / p^m Z_{p^n} = \{1, [a_1]_{p^m}, \ldots, [a_l]_{p^m}\}$ of $\mathbb{Z}^*_{p^m}$.*

Let $\mathcal{A}$ have form (2.2), $c_{l+1} = bp^m$, and $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ be a partial linear space with rank $\boldsymbol{\kappa} = l + 2$. Then, in particular, (2.3) holds. After Proposition 2.5 some fundamental parameters of $\mathfrak{M}$ can be computed.

LEMMA 2.7. *Let $x \in Z_{p^n} \setminus \{0\}$. Then $0 \in F[x]$ iff $x = tp^{n-m}$ for some t, i.e. iff $p^{n-m} \mid x$.*

PROOF. Assume that $0 \in F[x]$. Then: $c_i x = 0$ for some $i = 0, \ldots, l$, or $bp^m x = 0$. Since $x \in Z_{p^n} \setminus \{0\}$, we have $c_i x \neq 0$ as well, and thus $0 \in F[x]$ yields $bp^m x = 0$, i.e. $x = tp^{n-m}$ for some t.

Conversely, let $x = tp^{n-m}$ for some t. Then $0 = bp^m tp^{n-m} \in F[tp^{n-m}] = F[x]$, as required. □

LEMMA 2.8. *Let $x, y \in Z_{p^n} \setminus \{0\}$. Then $F[x] = F[y]$ iff $x = tp^{n-m}$ for some t and $y = c_i x$ for some $i = 0, \ldots, l$.*

PROOF. Suppose that $F[x] = F[y]$. Considering the sets $F[x] \cap \mathcal{Z}_{p^n}^{(j)}$ and $F[y] \cap \mathcal{Z}_{p^n}^{(j)}$ we get that there is j_0 with $x, y \in \mathcal{Z}_{p^n}^{(j_0)}$. Since $y \in F[x]$, we have $y = c_{i_0} x$ for some $i_0 \in \{0, \ldots, l\}$ and thus we can write $F[x] = F[c_{i_0} x]$. In particular, this yields that for every i there is i' with $c_{i'} c_{i_0} x = c_i x$. From this we deduce $p^{n-j_0} \mid (c_{i'} c_{i_0} - c_i)$ and then from Proposition 2.5(ii) we come to $n - j_0 \leq m$. Consequently, $j_0 \geq n - m$ i.e. $p^{n-m} \mid x$.

Conversely, a straightforward computation gives that if (2.4) holds and $x = tp^{n-m}$, then $F[x] = F[c_i x]$ for every $i = 0, \ldots, l$. □

From Lemma 2.8 we get the number of lines of $\mathfrak{M}$.

PROPOSITION 2.9. *Under assumptions of Proposition 2.5, the partial linear space $\mathfrak{M}$ has $p^n - 1 - l \cdot \frac{p^m - 1}{l+1}$ lines.*

PROOF. From definition, for every $x \in Z_{p^n} \setminus \{0\}$ we obtain some line $F[x]$, so we have $|\mathbb{Z}_{p^n} \setminus \{0\}| = p^n - 1$ symbols of the form $F[x]$. However, in Lemma 2.8 we showed that ν of them can be grouped into $(l+1)$-element families which denote the same set, where $\nu = |\{y \in Z_{p^n} : y \neq 0,\ p^{n-m} \mid y\}|$. Therefore $\mathfrak{M}$ has $p^n - 1 - \nu + \frac{1}{l+1}\nu$ lines. From (1.2), $\nu = p^m - 1$; substituting we obtain the desired formula. □

Now, we can count how many lines pass through a point of $\mathfrak{M}$.

PROPOSITION 2.10. *Let $y \in Z_{p^n} \setminus \{0\}$, and $\boldsymbol{r}$ be the rank of y.*

(i) If $y \in Z_{p^n}^*$, then $\boldsymbol{r} = l + 1$.

(ii) Let $y = ep^i$, where $e \in Z_{p^n}^*$ and $i \geq 1$. Then

$$\boldsymbol{r} = \begin{cases} p^m + 1 & \text{if } n - m \leq i, \\ p^m + l + 1 & \text{if } n - m > i, \\ & \text{for } m \leq i < n, \end{cases} \quad \text{and} \quad \boldsymbol{r} = \begin{cases} 1 & \text{if } n - m \leq i, \\ l + 1 & \text{if } n - m > i, \\ & \text{for } 1 \leq i < m. \end{cases}$$

(iii) Point 0 is on $\frac{p^m - 1}{l+1}$ lines.

(iv) If $y \in \mathcal{Z}_{p^n}^{(i)}$, then the points collinear with y are in $\mathcal{Z}_{p^n}^{(i)} \cup \mathcal{Z}_{p^n}^{(i+m)} \cup \mathcal{Z}_{p^n}^{(i-m)}$.

PROOF. Let $x \in Z_{p^n} \setminus \{0\}$. From definition, $y \in F[x]$ iff one of the following holds:

(a) $y = c_i x$, for some $i = 0, \ldots, l$, or

(b) $y = bp^m x$.

For every $y \in Z_{p^n} \setminus \{0\}$ every equation of (a) always has one (unique) solution.

(i) Since equation (b) has no solution for $y \in Z_{p^n}^*$, the rank of a point y in this case is $l + 1$.

(ii) Now, let $y \notin Z^*_{p^n}$. Then $y = ep^i$ for some $e \in Z^*_{p^n}$ and $1 \leq i \leq n-1$. We can write equation (b) in $\mathbb{Z}_{p^n}$ in the form $p^m x \equiv b^{-1}ep^i \mod p^n$, where b^{-1} is the inverse of b in $\mathbb{Z}_{p^n}$.

First, suppose that $i \geq m$. Then we have to solve the congruence $x \equiv b^{-1}ep^{i-m} \mod p^{n-m}$, which has p^m solutions in $\mathbb{Z}_{p^n}$ (we use equation (1.2) here) of the form $x = b^{-1}ep^{i-m} + t$, where $t \in Z_{p^n}$ and $p^{n-m} \mid t$. Since $p^{n-m} \not| x$ ($n - m \leq i - m$ is impossible), from Lemma 2.8 we get that the obtained lines $F[x]$ are pairwise distinct. However, if $p^{n-m} \mid y$ i.e. $n - m \leq i$, the solutions of the equations of (a) yield the same line $F[y]$.

Next, suppose that $i < m$. There is no solution of the congruence $xp^{m-i} \equiv b^{-1}e \mod p^{n-i}$. Consequently, only solutions of (a) are admissible and thus we obtain either a single line through y (if $p^{n-m} \mid y$), or $l+1$ distinct lines.

(iii) From Lemma 2.7 we know, that $0 \in F[x]$ holds iff $x = ep^{n-m}$ for some e i.e. iff $p^{n-m} \mid x$. But Lemma 2.8 gives $F[ep^{n-m}] = F[c_i ep^{n-m}]$ for every i. Therefore, using formula (1.2) we obtain that 0 is on $\frac{p^m-1}{l+1}$ lines.

(iv) Let $y = p^i e$, where $e \in Z^*_{p^n}$, and z be a point collinear with y. If z is on a line $F[x]$, where x is a solution of (a), then z is one of the following: $y, c_i y, c_i^{-1} y \in \mathcal{Z}^{(i)}_{p^n}$, or $p^{m+i}eb, p^{m+i}c_i^{-1}eb \in \mathcal{Z}^{(i+m)}_{p^n}$. If x is a solution of (b) (to this aim $i \geq m$ is necessary), then z is one of the following: $b^{-1}ep^i \in \mathcal{Z}^{(i)}_{p^n}$, or $b^{-1}ep^{i-m} + p^{n-m}t, b^{-1}ec_i p^{i-m} + p^{n-m}c_i t \in \mathcal{Z}^{(i-m)}_{p^n}$. □

As we see in Proposition 2.10 the structure $\mathfrak{M}$ may contain points with distinct ranks. But, in some sense, these ranks characterize corresponding points:

FACT 2.11. *The four possible values of ranks of points in $Z_{p^n} \setminus (Z^*_{p_n} \cup \{0\})$ are pairwise distinct.*

The structure $\mathfrak{M}$ has points from $y \in Z_{p^n} \setminus (Z^*_{p^n} \cup \{0\})$ of rank:

(i) $p^m + l + 1$ *iff* $2m > n$,

(ii) 1 *iff* $m > 1$ *and* $2m > n$, *and*

(iii) $l + 1$ *iff* $m > 1$ *and* $n > m + 1$.

(iv) $\mathfrak{M}$ *always has points of rank* $p^m + 1$.

Point 0 *has rank:*

(a) 1 *iff* $p^m = l + 2 = \boldsymbol{\kappa}$,

(b) $l + 1$ *iff* $p^m = (l+1)^2 + 1 = (\boldsymbol{\kappa} - 1)^2 + 1$.

Point 0 *never has rank* $p^m + 1$ *or* $p^m + l + 1$.

PROOF. The first statement is evident, since the numbers p^m+1, 1, $l+1$, and $p^m + l + 1$ are pairwise distinct (note that $p^m = l$ gives a contradiction: $(l+1)|(l-1)$). The statements (i)–(iv) are evident, as to get $y \in \mathcal{Z}^{(i)}_{p^n}$ with a desired rank, in accordance with Proposition 2.10, we must find i in suitable intervals in Z. From Proposition 2.10, point 0 has rank $\frac{p^m-1}{l+1}$. Then (a) and (b) are evident. To prove the last statement assume that the point 0 has rank

$p^m + l + 1$. Then $\frac{p^m-1}{l+1} = p^m + l + 1$, so $lp^m + (l+1)^2 + 1 = 0$, which is impossible. Analogously, $\frac{p^m-1}{l+1} = p^m + 1$ gives, inconsistently, $lp^m + l + 2 = 0$. □

As a corollary to Proposition 2.10(iv) we obtain

COROLLARY 2.12. *If $y \in \mathcal{Z}_{p^n}^{(i)}$, $y \neq 0$, then the distance between y and 0 (i.e. the minimal length of a polygonal path joining y and 0) is*

$$\min\{k\colon n - m \leq i + km\} + 1.$$

Finally, from Proposition 2.10(iii), we get

COROLLARY 2.13. *If there is a set $\mathcal{A}$ of the form assumed in Proposition 2.5 such that $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is a connected partial linear space with constant line rank $\boldsymbol{\kappa}$, then $(\boldsymbol{\kappa} - 1) \mid p^m - 1$.*

We close this part with a result converse to Proposition 2.5.

PROPOSITION 2.14. *Assume that the set $\mathcal{A}$ has form (2.2), where $c_{l+1} = bp^m$. Moreover, assume that $\mathcal{A}$ satisfies (2.3), and (2.4) for suitable permutations α_i, as claimed in Proposition 2.5(i). Finally, assume the following*

(2.5)

$$p^\mu \mid (c_{i'}c_{i''} - c_{j'}c_{j''}) \text{ yields } i' = j',\ i'' = j'',\ \text{or } i' = j'',\ i'' = j',\ \text{or } \mu \leq m,$$

for all $0 \leq i', i'', j', j'' \leq l$. Then the structure $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is a partial linear space with line rank $\boldsymbol{\kappa} = l + 2$.

PROOF. It suffices to prove that, under the above assumptions, if $x_1, x_2 \in Z_{p^n}$, $x_1, x_2 \neq 0$, and $|F[x_1] \cap F[x_2]| \geq 2$, then $F[x_1] = F[x_2]$.

Note, first, that if $x \in \mathcal{Z}_{p^n}^{(i)}$ for some i, then $F[x] \cap \mathcal{Z}_{p^n}^{(j)} \neq \emptyset$ iff $j = i$ or $j = \min\{n, i + m\}$. In the first case $F|[x] \cap \mathcal{Z}_{p^n}^{(j)}| = l + 1$, in the second one $|F[x] \cap \mathcal{Z}_{p^n}^{(j)}| = 1$.

Assume that $|F[x_1] \cap F[x_2]| \geq 2$. In view of the above it suffices to consider two cases:

(a) $c_{i_1}x_1 = c_{i_2}x_2$ and $bp^m x_1 = bp^m x_2$ holds in $\mathbb{Z}_{p^n}$, or

(b) $c_{i_1}x_1 = c_{i_2}x_2$, $c_{j_1}x_1 = c_{j_2}x_2$, and $c_{i_1}x_1 \neq c_{j_1}x_1$ holds in $\mathbb{Z}_{p^n}$,

for some $i_1, i_2, j_1, j_2 \leq l$. Let us start with case (a). We get $p^{n-m} \mid (x_2 - x_1)$ so, $x_2 = x_1 + ep^{n-m}$ for some e. Substituting we obtain $p^{n-m} \mid x_1(c_{i_2} - c_{i_1})$. From (2.3) we conclude with: $c_{i_1} = c_{i_2}$ (which gives $x_1 = x_2$) or $p^{n-m} \mid x_1$. There is t such that $c_{i_1}c_t \equiv c_{i_2} \mod p^m$ and thus $c_{i_1}x_1 \equiv c_{i_2}x_2 \equiv c_{i_1}c_t x_2 \mod p^n$. This gives, finally, $x_1 \equiv c_t x_2 \mod p^n$. From the assumed Proposition 2.5(i) we directly compute now $F[x_1] = F[x_2]$.

Next, let (b) holds. We have $x_1 = c_{i_1}^{-1}c_{i_2}x_2$ so, $c_{j_1}c_{i_1}^{-1}c_{i_2}x_2 = c_{j_2}x_2$ holds in $\mathbb{Z}_{p^n}$ i.e. $p^n \mid (c_{j_1}c_{i_1}^{-1}c_{i_2} - c_{j_2})x_2$. Therefore we can write $p^{n-\mu} \mid x_2$ and $p^\mu \mid (c_{j_1}c_{i_1}^{-1}c_{i_2} - c_{j_2})$. Suppose that $\mu > m$; then $p^\mu \mid (c_{j_1}c_{i_2} - c_{i_1}c_{j_2})$ and from

condition (2.5) we infer that $c_{i_1} = c_{j_1}$ (which is impossible) or $c_{i_1} = c_{i_2}$, which gives $x_1 = x_2$. If $\mu \leq m$, then $p^{n-m} \mid x_2, x_1$. In particular, $bp^m x_1 = bp^m x_2$; from (a) we obtain $F[x_1] = F[x_2]$. □

It is worth to point out that condition (2.5) guarantees, in particular, that condition (2.1) holds and thus $\mathbf{D}(\mathbb{Z}^*_{p^n}, \mathcal{A}^*)$ is a partial linear space.

3. Structures of rank $\boldsymbol{\kappa} = 3$

We begin with structures $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ with blocks of rank 3 (some of these structures will turn out to be partial Steiner triple systems). To this aim we consider $\mathcal{A} = \{1, c, b'\}$ with $c \in Z^*_{p^n}$ and $b' \in Z_{p^n} \setminus (Z^*_{p^n} \cup \{0\})$ i.e.

$$\mathcal{A} = \{1, c, bp^m\}, \text{ where } \mathrm{GCD}(c, p) = 1 = \mathrm{GCD}(b, p) \text{ and } 1 \leq m < n, \tag{3.1}$$

and $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$.

We write $r_\nu = \min\{i \colon p^\nu \mid (c^i - 1)\}$ for the rank of the cyclic group $\langle c \rangle_\nu$ generated by c in the multiplicative group $\mathbb{Z}^*_{p^\nu}$, $\nu = 1, \ldots, n$.

Note that $\mathfrak{M}$ need not to be a partial linear space. A counterexample, with arbitrary $\mathcal{A}$ of the form (3.1), can be obtained by the following observation:

Fact 3.1. *Let* $\mathrm{GCD}(c - 1, p) = 1$ *so, in view of Lemma 2.1* $|F[a]| = 3$ *for every* $a \in Z_{p^n} \setminus \{0\}$. *Assume that* $n > 1$. *Then either* $p^m \mid c + 1$, *or* $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ *is not a partial linear space.*

Proof. Assume that $\mathbf{D}^*(\mathbb{Z}^*_{p^n}, \mathcal{A})$ is a partial linear space. From Proposition 2.5 we obtain that (cf. (2.4)) $p^m \mid c^2 - 1 = (c-1)(c+1)$. Since $p \not\mid (c-1)$, we get the claim. □

As an immediate consequence of Fact 3.1 and Proposition 2.5(ii) we obtain

Fact 3.2. *Let* $p \neq 2$ *and let* $c \equiv -1 \mod p^m$ *i.e. let* $c + 1 = d \cdot p^{m+k}$ *for some* $d \in Z^*_{p^n}$ *and some* $0 \leq k < n - m$. *If* $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ *is a partial linear space, then* $k = 0$.

Then, finally, we get that $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p, c\})$ is a partial linear space for some "sporadic" values of c. As an immediate consequence of Facts 3.1 and 3.2 we obtain the following characterization:

Theorem 3.3. *Let* $\mathcal{A} = \{1, c, bp^m\}$, p *be a prime number distinct from* 2, $\mathrm{GCD}(b, p) = 1$, *and* $n > m \geq 1$. *Then the following conditions are equivalent:*

(i) The structure $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ *is a partial linear space with constant line rank equal to* 3.

(ii) $c = d \cdot p^m - 1$ *for some* $d \in Z^*_{p^n}$.

Proof. In view of Facts 3.1 and 3.2, (i) immediately implies (ii).

Assume (ii). Since $p \mid c+1$, we cannot have $p \mid (c-1)$ and from Lemma 2.1 we get $|F[x]| = 3$ for every $x \in Z_{p^n} \setminus \{0\}$. The condition (2.5) reduces to the

following: *if* $p^\mu \mid (c^2-1)$, *then* $\mu \le m$, which is evidently valid. To close the proof it suffices to use Proposition 2.14. □

EXAMPLE 3.4. As a direct consequence of Theorem 3.3 we get that if $n \ge k > 1$, then the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^k-1, p\})$ is not a partial linear space, and the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p-1, p\})$ is a partial linear space. Though, in particular, $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^n-1, p\})$ with $n \ge 2$ is not a partial linear space, it has a quite regular, fractal-like structure. To give an idea how such a structure looks like we use several times the following construction. Let a be a point of $\mathfrak{M}$. Through the points $a, -a$, if $a \ne -a$, there pass two blocks: $F[a]$ and $F[-a]$. Their third points are ap and $-ap$, respectively, Through these two points we have next two blocks $F[ap]$ and $F[-ap]$ with $ap^2, -ap^2$ as corresponding third points. Continuing, we obtain a sequence of pairs of points $\{ap^i, -ap^i\} = \{u_i, v_i\}$ such that $\{u_{i-1}, v_{i-1}\} \subset A_i, B_i$, $u_i \in A_i$, $v_i \in B_i$, and $\{u_i, v_i\} \subset A_{i+1}, B_{i+1}$ for some blocks $A_i, A_{i+1}, B_i, B_{i+1}$. Assume that $\mathrm{GCD}(a, p) = 1$; then with $i = n-1$ our procedure closes: $F[ap^{n-1}] = F[-ap^{n-1}] \ni 0$. Examples of structures obtained in this way are presented in Figures 1 and 2.

We see that after identifying every pair of the form $(a, -a)$ we obtain a tree. Therefore, the automorphism group of the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p, -1\})$ can be presented as follows: Let f be an automorphism of $\mathfrak{M}$. If $0 \in L$ and $x, y \in L$ for some block L of $\mathfrak{M}$, then $f(0) \in f(L)$ and $f(x), f(y) \in f(L)$. When we remove the blocks which contain the point 0, we obtain $\frac{p-1}{2}$ isomorphic substructures.

Let $x \in \mathcal{Z}_{p^n}^{(n-1)}$ so, $x = ep^{n-1}$ with $e \in Z_p^*$ and thus $F[x]$ is (an arbitrary, in fact) block through 0. Set $\mathcal{F}_{n-1}[x] = \{x, -x\} = F[x] \setminus \{0\}$. Blocks, which cross $F[x]$, are exactly those, which pass through the points x and $-x$; they have form $F[y]$, where $py = x$ or $py = -x$. Let us represent a point y from Z_{p^n} in the form

$$y = y_{n-1}p^{n-1} + y_{n-2}p^{n-2} + \ldots + y_2p^2 + y_1p + y_0$$

(cf. (1.1)). Then $F[y]$ crosses $F[x]$ iff $y_{n-2} = e$ or $y_{n-2} = -e$ and $y_{n-3} = \ldots = y_0 = 0$. Note that the points on $F[y]$ not on $F[x]$ are y and $-y$; they are in $\mathcal{Z}_{p^n}^{(n-2)}$. Let us denote by $\mathcal{F}_{n-2}[x]$ the family of such points. Continuing, we consider other blocks that pass through these points, and new points on these blocks; let $\mathcal{F}_{n-3}[x]$ be the set of them. It is seen that the elements of $\mathcal{F}_{n-3}[x]$ can be characterized as those $y \in \mathcal{Z}_{p^n}^{(n-3)}$ which have representation $y = \sum_{i=0}^{n-1} y_i p^i$, where $y_{n-3} = e$ or $y_{n-3} = -e$ and $y_{n-4} = \ldots = y_0 = 0$. Inductively, we construct the family $\mathcal{F}[x] = \bigcup\{\mathcal{F}_i[x] \colon i = 0, \ldots, n-1\}$ of points, which form one "leaf" around $F[x]$. Elements y of $\mathcal{F}[x]$ are characterized by the condition: *if* $y \in \mathcal{Z}_{p^n}^{(i)}$, *then* $y_i = \pm e$ *in the representation given in (1.1).*

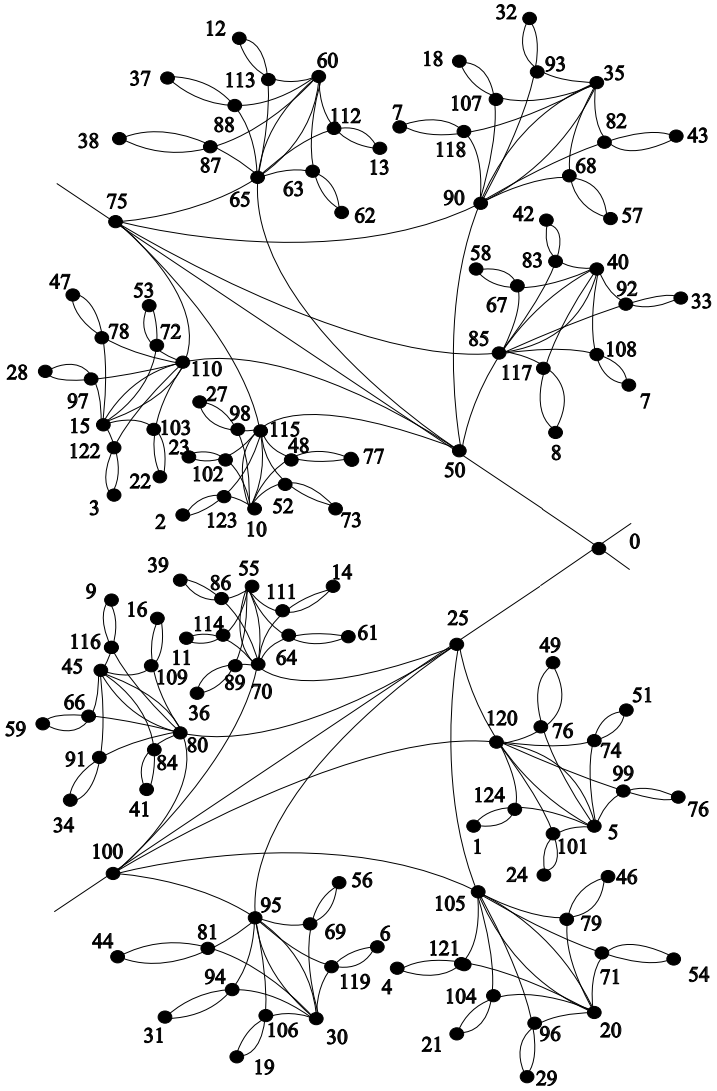

FIGURE 1. The structure $\mathbf{D}^*(\mathbb{Z}_{5^3}, \{1, 5, -1\})$.

Now, it is evident that for two $x' = p^{n-1}e', x'' = p^{n-1}e'' \in \mathcal{Z}_{p^n}^{(n-1)}$ the map

$$f\colon \sum_{j=n-1}^{n-i+1} y_j p^j + e' p^{n-i} \longmapsto \sum_{j=n-1}^{n-i+1} y_j p^j + e'' p^{n-i}$$

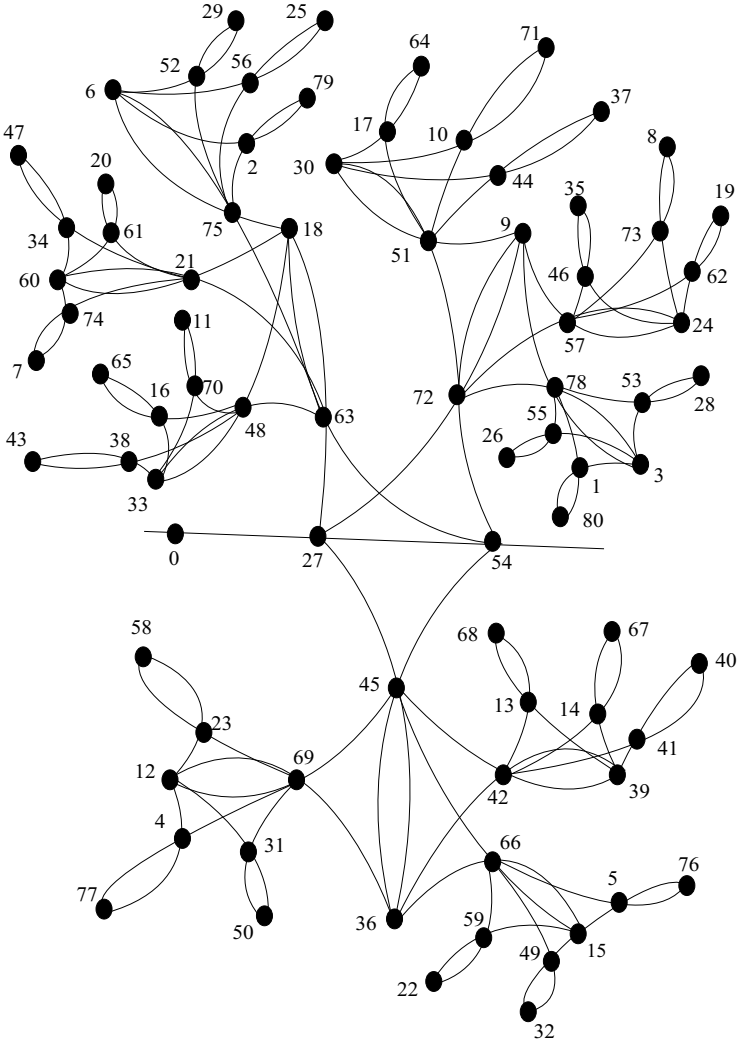

FIGURE 2. The structure $\mathbf{D}^*(\mathbb{Z}_{3^4}, \{1, 3, -1\})$.

is an isomorphism between the substructures $\mathcal{F}[x']$ and $\mathcal{F}[x'']$ of $\mathfrak{M}$.

Finally, note that every of the substructures $\mathcal{F}[x]$ is isomorphic with the structure $\mathbf{D}^*(\mathbb{Z}_{p^{n-1}}, \{1, p, -1\})$; to this aim it suffices to consider the map $\mathcal{F}[p^{n-1}e] \ni y \longmapsto py$ with $e = 1$. To establish the automorphism group of $\mathfrak{M}$ we note, first, that arbitrary element $f \in \mathrm{Aut}(\mathfrak{M})$ determines a permutation of the lines through 0 and thus it determines a permutation of the

substructures $\mathcal{F}[p^{n-1}e]$ with $e \in \mathbb{Z}_p^*$. Then, in every such a substructure the map which interchanges $p^{n-1}e$ and $-p^{n-1}e$ is its automorphism. Finally, we inductively reduce the problem, since $\mathrm{Aut}(\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p, -1\})) \cong S_{\frac{p-1}{2}} \ltimes \big(C_2 \oplus \mathrm{Aut}(\mathbf{D}^*(\mathbb{Z}_{p^{n-1}}, \{1, p, -1\}))\big)$.

4. Multiply wound polygons and their automorphisms

Here, we shall explain (in more geometrical terms) the nature of a partial linear space determined by $\mathcal{A}$ of the form (3.1). To make the picture more clear, let us begin with a more general construction. First, for an arbitrary k-gon $\mathcal{C}$ we label its points with symbols (i) and sides with symbols $[i]$ $(i \in C_k)$ in such a way that $[i]$ joins (i) and $(i+1)$. Thus, we identify $\mathcal{C}$ with the group C_k – more formally, with the cyclic configuration $\mathbf{D}(C_k, \{0, 1\})$ (consult [9] for details). For arbitrary $v \in C_k$ we consider the maps τ_v, σ_v defined by $\tau_v(i) = i + v$, $\sigma_v(i) = -i + v$. These maps form the dihedral group D_k, and yield all the automorphisms of $\mathcal{C}$ acting on its points and lines as follows:

$$\tau_v\colon (i) \longmapsto (\tau_v(i)), \qquad \tau_v\colon [i] \longmapsto [\tau_v(i)],$$
$$\sigma_v\colon (i) \longmapsto (\sigma_v(i)), \qquad \sigma_v\colon [i] \longmapsto [\sigma_{v-1}(i)].$$

Let $\mathcal{C}$ be an arbitrary k_1-gon (so identified with C_{k_1}), and let k_2 be an arbitrary positive integer. We spool on $\mathcal{C}$ a $(k_1 \cdot k_2)$-gon $\mathcal{C}'$ such that each vertex (i) of $\mathcal{C}$ $(i \in C_{k_1})$ is on k_2 sides of $\mathcal{C}'$ of the form $[i + jk_1]$ $(j \in C_{k_2})$. On the other hand this situation can be seen as a k-gon with $k = k_1 \cdot k_2$, represented as $\mathbf{D}(C_k, \{0, 1\})$, on whose sides new points were added in such a way that edges $[i]$ and $[i+jk_1]$ of $\mathcal{C}'$ are extended with a common point for $j = 0, 1, \ldots, k_2 - 1$. Then $\mathcal{C}$ results as a k_1-gon inscribed into $\mathcal{C}'$, joining the new points. After that, the procedure can be iterated, so as a $(k_3 k_2 k_1)$-gon $\mathcal{C}''$ is wound round $\mathcal{C}'$, and so on, for arbitrary sequence of positive integers $k_1, k_2, \ldots, k_m$. The resulting configuration $\mathcal{K}$ which is the union of the polygons $\mathcal{C}, \mathcal{C}', \ldots, \mathcal{C}^{m-1}$ will be written as $C_{k_1,k_2,\ldots,k_m}$ and will be called *a hank of polygons*. The polygon $\mathcal{C}^{m-1}$ will be referred to as *the border of* $\mathcal{K}$, and $\mathcal{C}$ is its *kernel*. Let us write down a simple observation

Fact 4.1. *Let $k = k_1 k_2 \ldots k_m$. We consider the series of configurations $\mathcal{K}_i = C_{k_1,\ldots,k_i}$. Let $\mathcal{C}^i$ $(= C_{k_1 \cdot \ldots \cdot k_i})$ be corresponding polygons, where $\mathcal{C}^{i+1}$ is k_{i+1}-times wound on $\mathcal{C}^i$, and $\mathcal{K}_i$ is the union of $\mathcal{C}^1, \ldots, \mathcal{C}^i$. For arbitrary $v \in C_k$ the maps τ_v and σ_v determine automorphisms of all the polygons $\mathcal{C}^i$ and thus they are automorphisms of $\mathcal{K}_i$ for $i = 1, \ldots, m$.*

Proof. Set $\mathcal{C} = \mathcal{C}^m$ and $\mathcal{C}' = \mathcal{C}^{m-1}$. Let $[i]$ and $[i + k_m]$ be two sides of $\mathcal{C}$, which have the same point of $\mathcal{C}'$. Then τ_v maps them onto sides $[i + v]$ and $[i + v + k_m]$ which, evidently, have a common point of $\mathcal{C}'$. The function σ_v maps the sides $[i]$ and $[i + k_m]$ onto the sides $[-i + v - 1]$ and $[-i + v - 1 + k_1 \ldots k_{m-1}(k_m - 1)]$ which have a common point of $\mathcal{C}'$ as well. Therefore,

both τ_v and σ_v determine permutations of the points of $\mathcal{C}'$. It is clear that neighbor sides of $\mathcal{C}$ are mapped onto neighbor sides. This, finally, proves that the maps τ_v and σ_v determine automorphisms of $\mathcal{C}'$. By induction, we get our claim. □

It is immediate from definition that (in notation of Fact 4.1) for $j < m$ the points of $\mathcal{C}^j$ have rank $2 + k_{j+1}$ in $\mathcal{K}^m$, and points of $\mathcal{C}^m$ have rank 2. From Fact 4.1 we thus obtain

FACT 4.2. $\mathrm{Aut}(C_{k_1,k_2,\ldots,k_m}) \cong D_{k_1 \cdot k_2 \cdot \ldots \cdot k_m}$.

Now, we are coming back to the incidence structure

$$\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, bp^m, dp^m - 1\})$$

with $b, d \in \mathbb{Z}_{p^n} = \mathcal{Z}_{p^n}^{(0)}$. Set, as usual, $c = dp^m - 1$.

Let δ, μ be integers such that

$$n - 1 = \delta m + \mu, \quad 0 \leq \mu < m, \quad \delta \geq 0. \tag{4.1}$$

This means that $\delta m \leq n - 1 < (\delta + 1)m$ i.e. $(\delta - 1)m < n - m \leq \delta m$. In view of Corollary 2.12 this yields that

FACT 4.3. $\mathrm{dist}(x, 0) = \delta + 1$ *for* $x \in \mathcal{Z}_{p^n}^{(0)}$.

Now, let $x = ep^i \in \mathcal{Z}_{p^n}^{(i)}$ be arbitrary. Then $F[x] = \{x, cx, bp^m x\}$ and, clearly, $cep^i = cx \in \mathcal{Z}_{p^n}^{(i)}$. It is seen that the points xc^j form a closed polygon contained in $\mathcal{Z}_{p^n}^{(i)}$. Its length ρ_i is determined as the minimum $\min\{j \colon p^n \mid (c^j ep^i - ep^i)\}$ so, $\rho_i = \min\{j \colon p^{n-i} \mid (c^j - 1)\}$ and thus this polygon has r_{n-i} points, which form the set $x \cdot \langle c \rangle_{n-i}$. For better readability we write

$$\rho_i = r_{n-i} = \text{ the lenght of } (ep^i, c^1 ep^i, c^2 ep^i, \ldots)$$

for $e \in \mathbb{Z}_{p^n}^*$.

Next, let us observe the "third points" of $\mathfrak{M}$ on sides of a polygon $\mathcal{C} := x \cdot \langle c \rangle_{n-i}$. They have form $bp^m xc^j = bep^{m+i}c^j$ for $j = 1, 2, \ldots$. Two consecutive third points $bp^m xc^j$ and $bp^m xc^{j+1}$ are joined by the line $F[bp^m xc^j]$. Thus, in fact, these points form the polygon $\mathcal{C}' := bp^m x \cdot \langle c \rangle_{n-i-m}$ such that $\mathcal{C}$ is wound (p^m times, cf. Proposition 2.10 with $l = 1$) on $\mathcal{C}'$. The length of $\mathcal{C}'$ is r_{n-i-m} and $\mathcal{C}'$ is contained in $\mathcal{Z}_{p^n}^{(i+m)}$. This justifies the following recursive formula

$$\rho(i) = p^m \rho(i + m).$$

Continuing this procedure we obtain a series of polygons $\mathcal{C}^j = eb^j p^{i+jm} \cdot \langle c \rangle_{n-i-jm}$ such that $\mathcal{C}^j$ is contained in $\mathcal{Z}_{p^n}^{(i+jm)}$ and is wound on $\mathcal{C}^{j+1}$; the length of $\mathcal{C}^j$ is $\rho_{i+jm} = r_{n-i-jm}$. One can also say that the family of points thus constructed starting from a given $x \in \mathcal{Z}_{p^n}^{(i)}$ form a hank of polygons, whose kernel is a 2-gon, each next polygon being p^m-times wound on the

previous one, and whose border is $x\cdot\langle c\rangle_{n-i}$. It is seen that the above procedure of "inscribing" stops ($\mathcal{C}^j$ is a 2-gon), when $p^{n-m} \mid p^{i+jm}$ i.e. $n-m \le i+jm$. The minimal value of j with $n-m \le i+jm$ is $\beta_i - 1$, where $\beta_i = \mathrm{dist}(ep^i, 0)$ (with arbitrary $e \in \mathbb{Z}^*_{p^n}$).

Finally, the two sides of $\mathcal{C}^{\beta_i-1}$ are identified, and the point 0 of $\mathfrak{M}$ is placed on this side.

Let us consider a point $x = ep^i \in \mathcal{Z}^{(i)}_{p^n}$ of rank 2; from Proposition 2.10, $0 \le i < m$. Therefore, $n-m < n-i \le n$. We have

$$\mathrm{dist}(x,0) = \begin{cases} \delta+1 & \text{for } \delta m < n-i \le n \\ \delta & \text{for } n-m < n-i \le \delta m \end{cases},$$

and thus, from the above recursive formula we get

$$\rho_i = \begin{cases} 2p^{\delta m} & \text{if } \delta m < n-i \le n \\ 2p^{(\delta-1)m} & \text{if } n-m < n-i \le \delta m. \end{cases}$$

Therefore, $\mathfrak{M}$ has $(p-1)p^{n-i-1}/2p^{\delta m} = \frac{p-1}{2}p^{n-i-1-\delta m}$ polygons contained in $\mathcal{Z}^{(i)}_{p^n}$ with $\delta m < n-i \le n$, and $(p-1)p^{n-i-1}/2p^{(\delta-1)m} = \frac{p-1}{2}p^{n-i-1-(\delta-1)m}$ polygons contained in $\mathcal{Z}^{(i)}_{p^n}$ with $n-m < n-i \le \delta m$; consequently, these are numbers of hanks which have border polygons build from points of rank 2 of $\mathfrak{M}$ (on the other hand, their sum is the number of lines through 0). With a careful computation (use: $n-i = \delta m + \mu + 1 - i$) we obtain finally

FACT 4.4. *The structure $\mathfrak{M}$ contains $\frac{1}{2}(p^{\mu+1}-1)$ hanks with border points at distance $\delta+1$ from 0, and $\frac{p^{\mu+1}}{2}(p^{m-\mu-1}-1) = \frac{p^m-1}{2} - \frac{p^{\mu+1}-1}{2}$ hanks with border points at distance δ from 0.*

Now, assume that

$$\text{either} \quad m = 1, \quad \text{or} \quad 2m \le n$$

so, as a consequence of Fact 2.11 with $l = 1$, no point $x \neq 0$ of $\mathfrak{M}$ has rank 1. Then $\mathfrak{M}$ can be seen as a union of the hanks given in Fact 4.4. The case, when $\mathfrak{M}$ has points of rank 1 needs only small modification of the reasoning below.

Note, first, that the representation of $\mathfrak{M}$ defined in Fact 4.4 depends entirely on the parameters p, n, and m. Slightly informally we can say that $\mathfrak{M}$ consists of $\gamma_1 := \frac{p^{\mu+1}-1}{2}$ copies of the hank $C_{2,\underbrace{p^m,\ldots,p^m}_{\delta \text{ times}}}$, and $\gamma_2 := \frac{p^m-1}{2} - \frac{p^{\mu+1}-1}{2}$ copies of the hank $C_{2,\underbrace{p^m,\ldots,p^m}_{(\delta-1) \text{ times}}}$, if $\gamma_2 > 0$, i.e. if $2 < m+1 < n$ (cf. Fact 2.11). These copies are linked with 0 by lines passing through kernels of the hanks. On the other hand, this gives also that $\mathfrak{M}$ uniquely determines the values of the parameters μ and δ. This yields, as an immediate consequence

COROLLARY 4.5. *Let $b, d \in \mathbb{Z}_{p^n}^*$. The structures $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^m, p^m - 1\})$ and $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, bp^m, dp^m - 1\})$ are isomorphic. If $1 \leq m_1, m_2 < n$ and $m_1 \neq m_2$ then $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^{m_1}, p^{m_1} - 1\})$ and $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^{m_2}, p^{m_2} - 1\})$ are not isomorphic.*

Another important consequence is

THEOREM 4.6. *Let $\mathfrak{G}$ be the automorphism group $\mathfrak{G} = \mathrm{Aut}(\mathfrak{M})$. Then*

$$\mathfrak{G} \cong \begin{cases} S_{\gamma_1} \ltimes \left(D_{2p^{\delta m}}\right)^{\gamma_1} & \text{if } \gamma_2 \leq 0 \\ S_{\gamma_1} \ltimes \left(D_{2p^{\delta m}}\right)^{\gamma_1} \oplus S_{\gamma_2} \ltimes \left(D_{2p^{(\delta-1)m}}\right)^{\gamma_2} & \text{if } \gamma_2 > 0. \end{cases}$$

PROOF. Clearly, every automorphism of $\mathfrak{M}$ must leave the set of points of rank 2 invariant. One can note that the point 0, even if it has rank 2, cannot be interchanged with other points of rank 2 (which, as it follows from the above considerations, are the border points of hanks defined in Fact 4.4).

Let $f \in \mathfrak{G}$. Particularly, from the above, f fixes 0. Suppose that f preserves one of the hanks $\mathcal{K}$ whose border is a polygon $\mathcal{C}$ lying at distance $\delta+1$ from 0. Then $\mathcal{C} \cong C_{2p^{\delta m}}$ and $g = f \restriction \mathcal{C}$ must be an element of the dihedral group $D_{2p^{\delta m}}$. From Fact 4.2, g determines uniquely an automorphism of the hank $\mathcal{K}$. Moreover, g may be an arbitrary element of $D_{2p^{\delta m}}$. Analogous reasoning applies to a hank $\mathcal{K}$ with border at distance δ from 0, and then for f preserving $\mathcal{K}$, $f \restriction \mathcal{K}$ can be considered as an element of $D_{2p^{(\delta-1)m}}$. Since arbitrary $f \in \mathrm{Aut}(\mathfrak{M})$ determines, first, a permutation of the hanks with borders at the same distance from 0, and then it constitutes isomorphisms between corresponding hanks, we conclude with the desired formula. □

A representation involving series of wound polygons and families of hanks can be given generally, for arbitrary incidence structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$, where $\mathcal{A}$ has form (3.1). Note that for some values of the parameter c we can obtain structures, which look like "mixtures" of the fractal-like structures of the form $\mathbf{D}^*(\mathbb{Z}_{p^{n'}}, \{1, -1, p\})$, and the partial linear spaces of the form $\mathbf{D}^*(\mathbb{Z}_{p^{n''}}, \{1, p, pd - 1\})$. This happens, when on some level the polygon $\mathcal{C}^j$ degenerates to a 2-gon, but this one does not yield a line through 0. As an example, we can quote the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \{1, p^k - 1, p\})$ for $1 < k < n$. On Figure 3 we give the schema of the structure of this type for $p = 3$, $n = 3$, and $k = 2$.

5. STRUCTURES OF RANK $\boldsymbol{\kappa} = 4$

Now, let us pay attention to structures $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$, where $|\mathcal{A}| = 4$. In accordance with our general stipulation we have

(5.1) $\mathcal{A} = \{1, b', c_1, c_2\}$ for some $c_1, c_2 \in Z_{p^n}^*$ and $b' \in Z_{p^n} \setminus (Z_{p^n}^* \cup \{0\})$.

Consequently, $b' = bp^m$ for some $b \in \mathbb{Z}_{p^n}^*$ and $1 \leq m < n$.

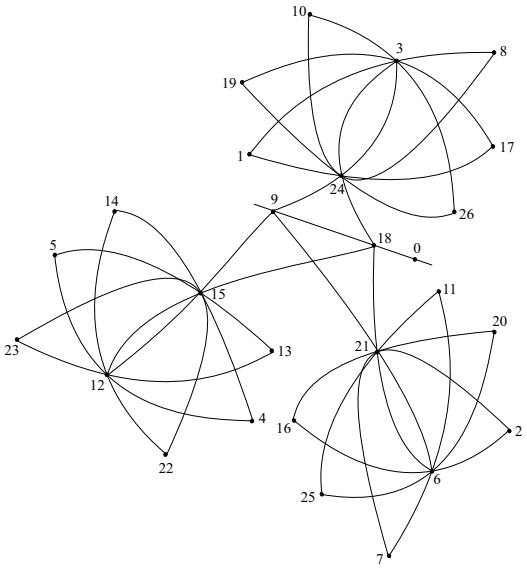

FIGURE 3. The structure $\mathbf{D}^*(\mathbb{Z}_{3^3}, \{1, 3, 8\})$.

Note, first, that the requirement similar to the one given in Theorem 3.3 is defective: if $c_i = p^{m_i} d_i - 1$ for some $d_1, d_2 \in Z^*_{p^n}$ and $m_i \geq 1$, then $p \mid (c_1 - c_2)$, which contradicts global assumptions (2.3).

Now, let us state some conditions necessary to get a partial linear space with $\mathcal{A}$ of the form (5.1).

LEMMA 5.1. *Let $\mathbf{D}^*(\mathbb{Z}^*_{p^n}, \mathcal{A})$ be a partial linear space with rank 4 lines, where $\mathcal{A} = \{1, bp^m, c_1, c_2\}$ for some $b, c_1, c_2 \in Z^*_{p^n}$. Then the following conditions hold.*

(i) $p^m \mid c_1 c_2 - 1$;
(ii) $p^m \mid c_1^2 - c_2$ *and* $p^m \mid c_2^2 - c_1$;
(iii) $p^m \mid c_1 + c_2 + 1$;
(iv) $c_1^2 - c_2 = p^m g$ *and* $c_2^2 - c_1 = p^m f$ *for some* $g, f \in Z^*_{p^n}$;
(v) $c_1 c_2 - 1 = p^m h$ *for some* $h \in Z^*_{p^n}$.

The condition (iii) is a consequence of (ii); clearly, (i) follows from (v), and (ii) follows from (iv).

PROOF. In view of Proposition 2.5 it suffices to determine the corresponding permutations α. It is seen, that the only possible are two:

(a) $p^m \mid (c_1^2 - 1)$ and $p^m \mid (c_2 - c_1 c_2)$, or
(b) $p^m \mid (1 - c_1 c_2)$ and $p^m \mid (c_2 - c_1^2)$.

In the case (a) we have $p^m \mid c_2(c_1-1)$, which is impossible. Therefore, (b) holds, which immediately implies (i) and (ii).

Now, assume (ii). Then $p^m \mid ((c_1^2-c_2)-c_2^2-c_1) = (c_1-c_2)(c_1+c_2+1)$, which, since $p^m \nmid (c_1-c_2)$ gives (iii).

Finally, (iv) and (v), in view of (i) and (ii) follow directly from Proposition 2.5(iii). □

LEMMA 5.2. *Let c_1, c_2 satisfy conditions (i) and (iii) of Lemma 5.1. Let $r = [c_1]_{p^m}$ and $s = [c_2]_{p^m}$. Then r and s are solutions of the equation*

$$\lambda^2 + \lambda + 1 = 0 \tag{5.2}$$

in the ring $\mathbb{Z}_{p^m}$.

PROOF. Let us write $c_1 = tp^m + r$, where $r \in \{0, 1, \ldots, p^m - 1\}$. Since $p^m | (c_2 + c_1 + 1)$ we can write $c_2 = dp^{m+k} - c_1 - 1 = dp^{m+k} - tp^m - r - 1$ for some $k \geq 1$ and $d \in Z_{p^n}^* \setminus \{0\}$. Then $p^m \mid (c_1c_2 - 1) = (tp^m + r)(dp^{m+k} - tp^m - r - 1) - 1 = tdp^{2m+k} + t^2p^{2m} + tp^m r - tp^m + dp^{m+k}r - rtp^m - r^2 - r - 1$ yields $p^m \mid (r^2 + r + 1)$, as required. For s the reasoning runs analogously. □

Then, some other necessary conditions appear. Let us state them here.

LEMMA 5.3. *Let $\mathcal{A} = \{1, bp^m, c_1, c_2\}$, where $b, c_1, c_2 \in Z_{p^n}^*$, $c_1 \neq c_2$.*

(i) Let $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ be a partial linear space with all lines of rank 4. Then $p > 3$.

(ii) Let $p > 3$ and let c_1, c_2 satisfy the conditions (iv) and (v) of Lemma 5.1. Then $p \nmid (c_1 - c_2), (c_1 - 1), (c_2 - 1)$.

PROOF. To prove (i) assume that equation (5.2) has a solution in $\mathbb{Z}_{p^m}$. Then (5.2) has a solution also in $\mathbb{Z}_p$. Suppose that $p = 3$. Since 1 is the only solution of equation (5.2) in $\mathbb{Z}_3$, we can write $r = 3u + 1$ for some $u \in N$. Then $r^2 + r + 1 = (3u+1)^2 + (3u+1) + 1 = 9u^2 + 6u + 3u + 1 + 1 + 1 = 9u^2 + 9u + 3 = 3(3u^2 + 3u + 1) \equiv 0 \mod 3^m$ i.e. $3u^2 + 3u + 1 \equiv 0 \mod 3^{m-1}$. Consider two cases. If $m > 1$, then $3|1$, which is inconsistent. If $m = 1$, then $3 \mid (c_1 - c_2)$, which contradicts (2.3).

Next, to prove (ii) suppose that $p \mid (c_1 - 1)$, which gives $[c_1]_p = 1$. From Lemma 5.1 we get that the conditions (i) and (iii) of Lemma 5.1 are also valid. In view of Lemma 5.2, $1^2 + 1 + 1 = 0$ holds in $\mathbb{Z}_{p^m}$, so $p = 3$. Next, suppose that $p \mid (c_1 - c_2)$; we get $c_2 = c_1 + pd$ for some d. Then $c_2^2 = p^2d^2 + 2pdc_1 + c_1^2$. From $p \mid (c_2^2 - c_1)$ we obtain $p \mid (c_1^2 - c_1) = c_1(c_1 - 1)$, which is impossible. □

Finally, we note that the conditions established in the above lemmas turn out to be sufficient to obtain a partial linear space.

THEOREM 5.4. *Let $\mathcal{A} = \{1, bp^m, c_1, c_2\}$, where $1 \leq m < n$, $b, c_1, c_2 \in Z_{p^n}^*$ with $p > 3$, and c_1, c_2 satisfy conditions (iv) and (v) of Lemma 5.1, Then the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is a partial linear space with lines of rank 4.*

PROOF. At the beginning, from Lemma 5.3(ii) and Lemma 2.1 we get that lines of $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ have rank 4.

Now, assume that p^μ divides one of the following.

$c_1c_2 - 1$, $c_1^2 - c_2$, $c_2^2 - c_1$: from Lemma 5.1 we infer that $\mu \leq m$.

$c_1^2 - 1$, $c_2^2 - 1$: since $p \not| (c_1 - 1)$, we obtain $p^\mu \mid c_1 + 1$. Suppose that $\mu > 0$; from Lemma 5.1(iii) we have $p \mid c_2$, which is impossible.

$c_1^2 - c_2^2$: since $p \not| (c_1 - c_2)$, we get $p^\mu \mid (c_1 + c_2)$. Suppose that $\mu > 0$; from Lemma 5.1(iii) we obtain, inconsistently, $p \mid 1$.

It is clear that the other conditions of the form $p^\mu \mid (c'c'' - c'''c'''')$ with $\mu > 0$, $c', c'', c''', c'''' \in \{1, c_1, c_2\}$, and $c' \neq c''', c''''$ cannot hold. In view of Proposition 2.14, the above proves that $\mathfrak{M}$ is a partial linear space. □

It is worth to note here (cf. Corollary 2.6) the following, evident

PROPOSITION 5.5. *Under assumptions of Theorem 5.4, the set $\mathcal{A}^*$ yields a subgroup of $\mathbb{Z}_{p^n}^*$ isomorphic to C_3.*

Clearly, in view of Lemmas 5.1 and 5.2, to construct a partial linear space of the form $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ with $\mathcal{A} = \{1, bp^m, c_1, c_2\}$, equation (5.2) must be solvable in $\mathbb{Z}_{p^m}$, so in $\mathbb{Z}_p$ as well. To this aim, there must exist a square root of -3 in $\mathbb{Z}_p$, which eliminates some values of p. In particular, $p \neq 5$ and the least possible value is $p = 7$. One can check that, indeed, the structure $\mathbf{D}^*(\mathbb{Z}_{7^2}, \{1, 7, 2, 11\})$ is a partial linear space.

To make our investigations more complete we formulate explicitly a strengthening of Corollary 2.13.

PROPOSITION 5.6. *Assume that there is a set $\mathcal{A} \subset Z_{p^n}$ such that $1, p^m \in \mathcal{A}$ and $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is a partial linear space with rank 4 lines. Then $\left(\frac{-3}{p}\right) = 1$ and, consequently, $p = 3k + 1$ for some natural k.*

PROOF. Clearly, the solvability of equation (5.2) in $\mathbb{Z}_p$ implies $\left(\frac{-3}{p}\right) = 1$. Since $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{[p]_3}{3}\right)$, $\left(\frac{1}{3}\right) = 1$, and $\left(\frac{2}{3}\right) = -1$, we get $[p]_3 = 1$, as required. □

6. STRUCTURES OF RANK $\boldsymbol{\kappa} = 5$

Finally, let us pay attention to structures $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$, where $|\mathcal{A}| = 5$. Consider the general case

$$\mathcal{A} = \{1, b', c_1, c_2, c_3\} \quad \text{for some } c_1, c_2, c_3 \in Z_{p^n}^* \text{ and } b' \in Z_{p^n} \setminus (Z_{p^n}^* \cup \{0\}). \tag{6.1}$$

THEOREM 6.1. *Let $\mathcal{A} = \{1, bp^m, c_1, c_2, c_3\}$, where $b, c_1, c_2, c_3 \in Z_{p^n}^*$, m is a positive integer $< n$, and p a prime number. If the structure $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$*

is a partial linear space with lines of rank 5*, then the following congruences must be satisfied*

$$c_{\alpha(1)} \equiv -1 \mod p^m \tag{6.2}$$

$$c_{\alpha(2)} \equiv -c_{\alpha(3)} \mod p^m \tag{6.3}$$

$$c_{\alpha(2)} \cdot c_{\alpha(3)} \equiv 1 \mod p^m \tag{6.4}$$

for some permutation α *of* $\{1,2,3\}$.

Then also the following holds: $1 \equiv c_{\alpha(1)}^2 \mod p^m$ *and* $c_{\alpha(2)}^2, c_{\alpha(3)}^2 \equiv -1 \mod p^m$.

In particular (cf. Corollary 2.6), the set $\mathcal{A}^*$ *yields a* C_4*-subgroup of* $\mathbb{Z}_{p^m}^*$.

Proof. Suppose that $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ is a partial linear space and consider the lines

$$\begin{aligned}
L_0 = F[p^{n-m}] &= \{\ p^{n-m},\ 0,\ c_1p^{n-m},\ c_2p^{n-m},\ c_3p^{n-m}\ \},\\
L_1 = F[c_1p^{n-m}] &= \{\ c_1p^{n-m},\ 0,\ c_1^2p^{n-m},\ c_1c_2p^{n-m},\ c_1c_3p^{n-m}\ \},\\
L_2 = F[c_2p^{n-m}] &= \{\ c_2p^{n-m},\ 0,\ c_1c_2p^{n-m},\ c_2^2p^{n-m},\ c_2c_3p^{n-m}\ \},\\
L_3 = F[c_3p^{n-m}] &= \{\ c_3p^{n-m},\ 0,\ c_1c_3p^{n-m},\ c_2c_3p^{n-m},\ c_3^2p^{n-m}\ \}.
\end{aligned}$$

It is seen that $0, c_ip^{n-m} \in L_0, L_i$ so, all the L_i must coincide; in particular, $L_0 = L_1$, and therefore one of the following must be true.

(a) $p^{n-m} = c_1^2p^{n-m}$, $c_2p^{n-m} = c_1c_2p^{n-m}$, and $c_3p^{n-m} = c_1c_3p^{n-m}$,
(b) $p^{n-m} = c_1^2p^{n-m}$, $c_2p^{n-m} = c_1c_3p^{n-m}$, and $c_3p^{n-m} = c_1c_2p^{n-m}$,
(c) $p^{n-m} = c_1c_2p^{n-m}$, $c_2p^{n-m} = c_1^2p^{n-m}$, and $c_3p^{n-m} = c_1c_3p^{n-m}$,
(d) $p^{n-m} = c_1c_2p^{n-m}$, $c_2p^{n-m} = c_1c_3p^{n-m}$, and $c_3p^{n-m} = c_1^2p^{n-m}$,
(e) $p^{n-m} = c_1c_3p^{n-m}$, $c_2p^{n-m} = c_1^2p^{n-m}$, and $c_3p^{n-m} = c_1c_2p^{n-m}$,
(f) $p^{n-m} = c_1c_3p^{n-m}$, $c_2p^{n-m} = c_1c_2p^{n-m}$, and $c_3p^{n-m} = c_1^2p^{n-m}$.

In the cases (a) and (f) we get $p^m \mid c_2(c_1 - 1)$, which is impossible. Similarly, in the case (c) we obtain $p^m \mid c_3(c_1 - 1)$, which is impossible, as well.

Now, let us consider case (b). We obtain $p^m \mid (c_1c_3 - c_2)$ and $p^m \mid (c_1c_2 - c_3)$. Therefore $p^m \mid (c_1c_3 - c_2 + (c_1c_2 - c_3)) = c_1(c_3 + c_2) - 1(c_3 + c_2) = (c_1 - 1)(c_3 + c_2)$, which gives $c_3 \equiv -c_2 \mod p^m$. Similarly, $p^m \mid (c_1^2 - 1)$, and thus $c_1 \equiv -1 \mod p^m$.

Then, comparing L_0 and L_2 we get two possibilities: either $c_2^2p^{n-m} = p^{n-m}$, which yields, inconsistently, $c_2 \equiv -1 \equiv c_1 \mod p$, or $c_2c_3p^{n-m} = p^{n-m}$ and $c_2^2p^{n-m} = c_1p^{n-m}$. Finally, comparing L_0 and L_3 we obtain $c_3^2p^{n-m} = c_1p^{n-m}$. It is seen that $c_2^2 \equiv c_1$, $c_2^3 \equiv c_3$, and $c_2^4 \equiv 1 \mod p^m$. This proves our claim with $\alpha = \mathrm{id}$.

In cases (d) and (e) we get our claim with different α's only. □

The conditions found in Theorem 6.1, which are, in fact, suitable specializations of Proposition 2.5(i), are not sufficient for $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ with $\mathcal{A}$ of the form (6.1) to be a partial linear space. In particular, in $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{5^2}, \{1,5,4,3,2\})$ the lines L_i defined above coincide, though $\mathfrak{M}$ *is not*

a partial linear space. However, in this case assumptions (2.1) are not valid! Note that from Theorem 6.1 we obtain another necessary condition (cf. Corollary 2.13).

FACT 6.2. *If* $\mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ *with* $\mathcal{A}$ *of the form (6.1) is a partial linear space, then* $p \equiv 1 \mod 4$.

PROOF. From (6.3) and (6.4) we get that there exists c with $c^2 \equiv -1 \mod p^m$. Consequently, $c^2 \equiv -1 \mod p$ and thus $(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right) = 1$, which proves the statement. □

A couple of examples of partial linear spaces with rank 5 lines can be obtained as follows. Let $p \equiv 1 \mod 4$; consider $c \in Z_p$ with $c^2 \equiv -1 \mod p$ (cf. Fact 6.2). Clearly, $(p-1) \equiv -1 \mod p$ and $c + (p-c) \equiv 0 \mod p$. The following *are* partial linear spaces:

1. $\mathbf{D}^*(\mathbb{Z}_{5^2}, \{1, 5, 5-1, c+5\cdot(5-c), (5-c)+5\cdot c\})$: $c = 3$ ($c_1 = 4$, $c_2 = 13$, $c_3 = 17$);
2. $\mathbf{D}^*(\mathbb{Z}_{5^3}, \{1, 5, 5-1, c+5\cdot(5-c), (5-c)+5\cdot c\})$: $c = 3$ ($c_1 = 4$, $c_2 = 13$, $c_3 = 17$);
3. $\mathbf{D}^*(\mathbb{Z}_{13^2}, \{1, 13, 13-1, c, (13-c)\})$: $c = 5$ ($c_1 = 12$, $c_2 = 5$, $c_3 = 8$);
4. $\mathbf{D}^*(\mathbb{Z}_{17^2}, \{1, 17, 17-1, c+17\cdot(17-c), (17-c)+17\cdot c\})$: $c = 4$ ($c_1 = 16$, $c_2 = 225$, $c_3 = 81$);
5. $\mathbf{D}^*(\mathbb{Z}_{29^2}, \{1, 29, 29-1, c, (29-c)\})$: $c = 12$ ($c_1 = 28$, $c_2 = 12$, $c_3 = 17$);
6. $\mathbf{D}^*(\mathbb{Z}_{37^2}, \{1, 37, 37-1, c+37\cdot(37-c), (37-c)+37\cdot c\})$: $c = 6$ ($c_1 = 36$, $c_2 = 1153$, $c_3 = 253$).

The following *are not* partial linear spaces:

$$\mathbf{D}^*(\mathbb{Z}_{5^2}, \{1, 5, 4, 3, 2\}), \mathbf{D}^*(\mathbb{Z}_{5^3}, \{1, 5, 4, 3, 2\}), \mathbf{D}^*(\mathbb{Z}_{13^2}, \{1, 13, 12, 109, 73\}),$$

$$\mathbf{D}^*(\mathbb{Z}_{17^2}, \{1, 17, 16, 4, 13\}), \mathbf{D}^*(\mathbb{Z}_{37^2}, \{1, 37, 36, 6, 31\}).$$

An example, a schema of the structure $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{5^2}, \mathcal{A})$ with $\mathcal{A} = \{1, 5, 4, 13, 17\}$ is presented in Figure 4. Solid lines on Figure 4 represent the structure $\mathbf{D}(\mathbb{Z}_{25}, \{1, 4\})$ (corresponding polygons). Solid lines extended with thick dashed lines represent the structure $\mathbf{D}^*(\mathbb{Z}_{25}, \{1, 5, 4\})$ – in this case it is a partial linear space as well, cf. Theorem 3.3. Finally, solid lines extended with thick and thin dashed lines represent $\mathfrak{M}$. It is worth to note that solid lines extended with thick dashed lines represent the structure $\mathfrak{M}^* = \mathbf{D}(\mathbb{Z}_{25}^*, \{1, 4, 13, 17\}) \cong \mathbf{D}(C_{20}, \{0, 1, 7, 17\})$, which can be seen as a 20-gon (inscribed into itself). A schema of $\mathfrak{M}^*$ is given in Figure 5.

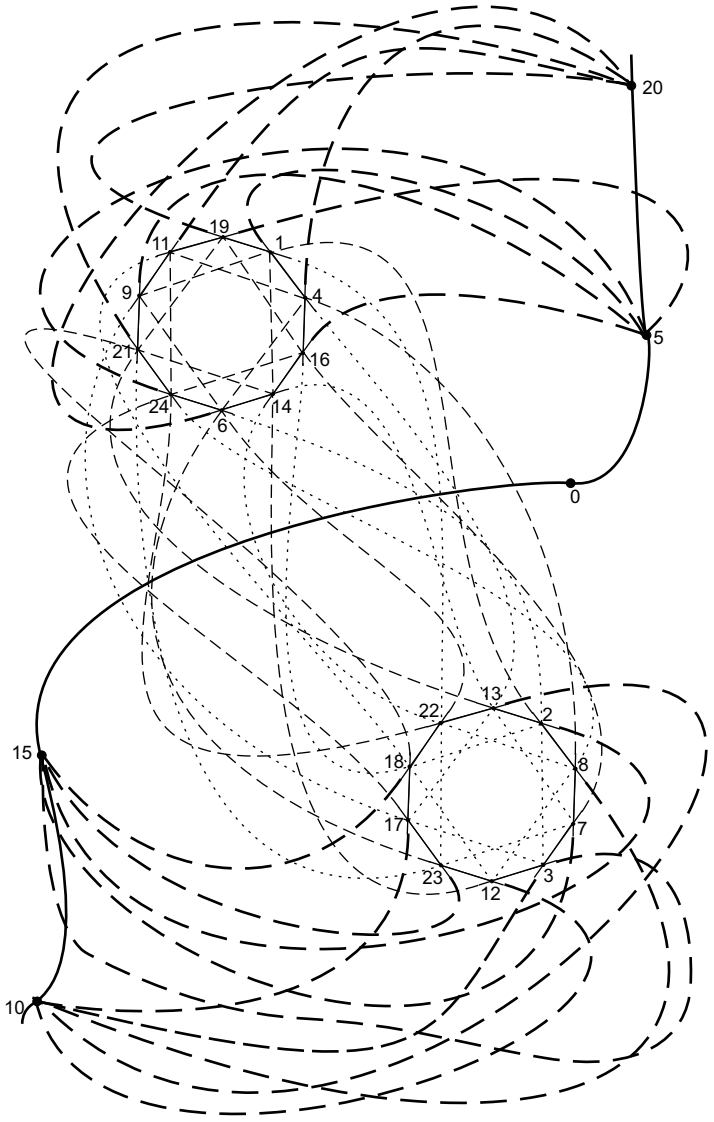

FIGURE 4. The structure $\mathbf{D}^*(\mathbb{Z}_{25}, \{1, 5, 4, 13, 17\})$.

7. Remarks on geometrical representation of partial linear spaces of the form $\mathbf{D}^*(\mathbb{Z}^*_{p^n}, \mathcal{A})$

Let $\mathfrak{M} = \mathbf{D}^*(\mathbb{Z}_{p^n}, \mathcal{A})$ be a partial linear space, where $\mathcal{A}$ has form (2.2). We take $c_{l+1} = bp^m$, where $b \in Z^*_{p^n}$ and then $\mathcal{A}^* = \{1, c_1, \ldots, c_l\}$.

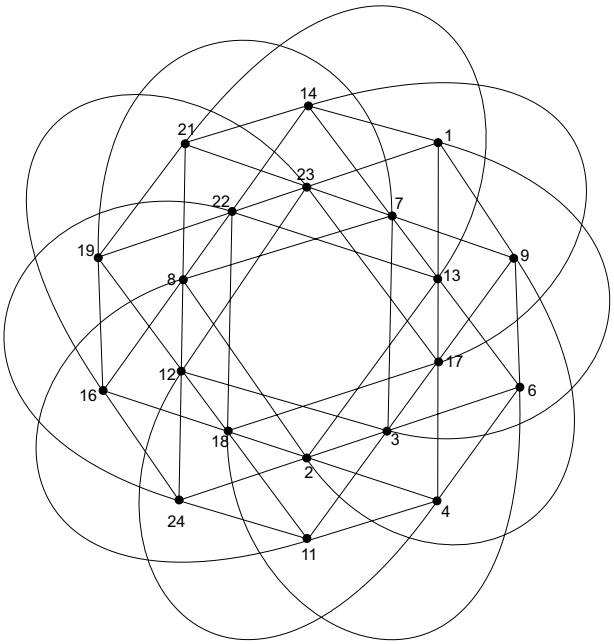

FIGURE 5. The structure $\mathbf{D}(\mathbb{Z}^*_{25}, \{1, 4, 13, 17\})$.

To visualize the schema of $\mathfrak{M}$ let us recall (cf. (2.1)) that the structure $\mathfrak{M}^* = \mathbf{D}(\mathbb{Z}^*_{p^n}, \mathcal{A}^*)$ is a partial linear space, thus given by a quasi difference set $\mathcal{A}^*$ (cf. [9]). Therefore, constructing $\mathfrak{M}$ we can begin with drawing this structure. Note that the conditions given in Proposition 2.5 do not assure that the set $\mathcal{A}^*$ generates $\mathbb{Z}^*_{p^n}$ and thus $\mathfrak{M}^*$ may be not connected. We write, for short, $[\![x]\!]$ for the line $x \cdot \mathcal{A}^* = \{x, c_1 x, \ldots, c_l x\}$ of $\mathfrak{M}^*$.

Then on every line $[\![x]\!]$ of $\mathfrak{M}^*$ the point bxp^m is added. Since $bp^m x' \equiv bp^m x'' \mod p^n$ gives $1 \equiv {x'}^{-1} x'' \mod p^{n-m}$ which, for given x' has distinct solutions $x'' = x' + tp^{n-m}$ with arbitrary $t \leq p^m$, some distinct lines of $\mathfrak{M}^*$ are extended with a common point. This procedure can be considered as a kind of "introducing a parallelism" into the $\mathfrak{M}^*$. Formally, we can define this parallelism by the formula

$$[\![x]\!] \parallel [\![y]\!] \quad \text{iff} \quad p^{n-m} \mid (x - y). \tag{7.1}$$

It is seen that the directions of lines of $\mathfrak{M}^*$ with respect to the parallelism defined by (7.1) correspond uniquely to "added points" of $\mathfrak{M}$ and thus they correspond to the elements of $\mathcal{Z}^{(m)}_{p^n}$. On the other hand, they can be identified with elements of $\mathbb{Z}^*_{p^{n-m}}$ under the map $Z^*_{p^{n-m}} \ni y \longmapsto yp^m$. Note that the

lines of $\mathfrak{M}$, which link directions of $\mathfrak{M}^*$ have form

$$\{xbp^m, c_1xbp^m, \ldots, c_lxbp^m, xbp^{2m}\} = p^m \cdot [\![xb]\!]' \cup \{xbp^{2m}\},$$

where $[\![xb]\!]'$ is a line of $\mathbf{D}(\mathbb{Z}^*_{p^{n-m}}, \mathcal{A}^*)$. This justifies the following observation

FACT 7.1. *The horizon of $\mathbf{D}(\mathbb{Z}^*_{p^n}, \mathcal{A}^*)$ (i.e. the set of directions of lines of $\mathfrak{M}^*$ together with lines of $\mathfrak{M}$ which join these points) is isomorphic to $\mathbf{D}(\mathbb{Z}^*_{p^{n-m}}, \mathcal{A}^*)$. Shortly, $\mathfrak{M}^{*\infty} \cong \mathbf{D}(\mathbb{Z}^*_{p^{n-m}}, \mathcal{A}^*)$.*

This means, in particular, that $\mathcal{A}^*$ yields a quasi difference set in $\mathbb{Z}^*_{p^{n-m}}$ so, (2.1) must hold in it.

After that, the procedure is iterated, some new lines are added on the horizon of $\mathfrak{M}^{*\infty}$, which link its directions, and again new horizon is defined. The construction stops, when 0 appears as an element of the defined new lines. In view of Corollary 2.6 and Lemma 2.7 this means that the horizon reduces to a parallel pencil, in the next step closed with a single point 0.

The construction sketched above does not exhaust all the points of $\mathfrak{M}$, though. Similarly as in the case investigated in Section 4 one sees that the points of $\mathfrak{M}$ which are obtained as elements of the above series of "horizons" form the set $\bigcup\{\mathcal{Z}^{(jm)}_{p^n} : j = 0, 1, \beta - 1\}$, where $\beta = \mathrm{dist}(b, 0)$. However, we can repeat a portion of the investigations of Section 4 and note that for every i with $0 \le i < n - m$ a line K of $\mathfrak{M}$ which crosses $\mathcal{Z}^{(i)}_{p^n}$ in at least two points can be written in the form $K = p^i \cdot [\![x]\!] \cup \{bp^{m+i}x\} =: [\![x]\!]'$ for some $x \in Z^*_{p^n}$. As above, we note that K can be associated (uniquely) with $x' \in Z^*_{p^{n-i}}$ (such that $x \equiv x' \mod p^{n-i}$) and thus we conclude with the following

FACT 7.2. *The substructure of $\mathfrak{M}$ obtained as the restriction of $\mathfrak{M}$ to the set $\mathcal{Z}^{(i)}_{p^n}$ is isomorphic under the map $Z^*_{p^{n-i}} \ni x \longmapsto xp^i$ to the structure $\mathbf{D}(\mathbb{Z}^*_{p^{n-i}}, \mathcal{A}^*)$.*

Its horizon with respect to the parallelism defined by the condition:

$$[\![x]\!]' \parallel [\![y]\!]' \quad \textit{iff} \quad p^{n-i-m} \mid (x - y) \tag{7.2}$$

is isomorphic to $\mathbf{D}(\mathbb{Z}^*_{p^{n-i-m}}, \mathcal{A}^*)$.

This enables us to cover $\mathfrak{M}$ with a family of series of structures of the form $\mathfrak{M}^j_i$, where $\mathfrak{M}^j_i \cong \mathbf{D}(\mathbb{Z}_{p^{n-i-jm}}, \mathcal{A}^*)$ is the restriction of $\mathfrak{M}$ to $\mathcal{Z}^{(i+jm)}_{p^n}$, $0 \le i < m$. Moreover, $\mathfrak{M}^{j+1}_i$ is the horizon of $\mathfrak{M}^j_i$; we can write $\mathfrak{M}^{j+1}_i = \mathfrak{M}^{j\infty}_i$.

One can note now that the problem to determine the automorphism group of $\mathfrak{M}$ reduces to the problem of determining the groups G_{n-i} of those automorphisms of the structures $\mathbf{D}(\mathbb{Z}^*_{p^{n-i}}, \mathcal{A}^*)$ with $0 \le i < m$, which preserve the parallelism (7.2). Let τ_d be a translation over the group $\mathbb{Z}^*_{p^{n-i}}$; thus τ_d is defined by the formula $\tau_d(x) = dx$ for $x, d \in Z^*_{p^{n-i}}$. In accordance with the general theory, $\tau_d \in \mathrm{Aut}(\mathbf{D}(\mathbb{Z}^*_{p^{n-i}}, \mathcal{A}^*))$. It is seen that τ_d maps a line $[\![x]\!]$ onto the line $[\![dx]\!]$, from which we deduce that $\tau_d \in G_{n-i}$. As we learn from

the results of Section 4, G_{n-i} may contain some other maps as well. The solution of the problem to determine the whole group G_{n-i} depends, finally, on the set $\mathcal{A}^*$ and the geometry of the structure $\mathbf{D}(\mathbb{Z}^*_{p^{n-i}}, \mathcal{A}^*)$.

References

[1] J. André, *On non-commutative geometry*, Ann. Univ. Sarav. Ser. Math. **4** (1993), 93-129.

[2] W. Benz, Vorlesungen über Geometrie der Algebren, Springer Verlag, Berlin Heidelberg New York, 1973.

[3] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, Vol.I, Encyclopedia of Mathematics and its applications **69**, University Press, Cambridge, 1999.

[4] A. Herzer, *Chain Geometries*, Handbook of Incidence Geometries, North-Holland, Amsterdam, 1995, 781-842.

[5] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer Verlag, New York, 1990.

[6] W. Lipski, W. Marek, Analiza kombinatoryczna (in Polish), PWN, Warszawa, 1986.

[7] C. Luksch, *Die Automorphismengruppe der Polynomgeometrie vom Grad n*, Mitt. Math. Sem. Giessen **181** (1987), 1-56.

[8] A. Matraś, A. Mierzejewska, K. Prażmowski *Some chain geometries determined by transformation groups*, Result. Math. **46** (2004), 251-270.

[9] K. Petelczyc, *Series of inscribed n-gons and rank 3 configurations*, Beiträge Algebra Geom. **46** (2005), 283-300.

[10] H. Wefelscheid, *Über die Automorphismengruppen von Hyperbelstrukturen*, Beiträge zur geometrischen Algebra (Proc. Sympos., Duisburg, 1976), Birkhäuser, Basel, 1977, 337-343.

A. Kozłowski
Institute of Mathematics
University of Białystok
15 267 Białystok
Poland
E-mail: andrzej.k80@wp.pl

K. Prażmowski
Institute of Mathematics
University of Białystok
15 267 Białystok
Poland
E-mail: krzypraz@math.uwb.edu.pl

Received: 15.4.2005.
Revised: 9.11.2005.