ON REGULAR PARALLELISMS OF PG(3,5) WITH AUTOMORPHISMS OF ORDER 5

ОТНОСНО РЕГУЛЯРНИТЕ ПАРАЛЕЛИЗМИ НА PG(3,5) С АВТОМОРФИЗМИ ОТ РЕД 5

Dr. Zhelezova S.,
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria
e-mail: stela@math.bas.bg

Abstract: A spread is a set of lines of PG(n,q), which partition the point set. A parallelism is a partition of the set of lines by spreads. A regulus of PG(3,q) is a set R of q + 1 mutually skew lines such that any line intersecting three elements of R intersects all elements of R. A spread S of PG(3, q) is regular if for every three distinct elements of S, the unique regulus determined by them is a subset of S. A parallelism is regular if all its spreads are regular.

Regular parallelisms in PG(3,q) are known for any q ≡ 2 (mod 3) due to T. Penttila and B. Williams, 1998. In PG(3,5) these families of regular parallelisms are presented by two regular parallelisms with automorphisms of order 31 obtained early by A. Prince. Whether these are all regular parallelisms in PG(3,5) is an open question.

There are four relevant groups of order 5 and in the present paper it is established that the regular parallelisms of PG(3,5) cannot posses any automorphism of order 5.

Keywords: PARALLELISM, AUTOMORPHISM, REGULARITY, COMBINATORIAL DESIGN

1. Introduction

Parallelisms are used in constructions of constant dimension error-correcting codes that contain lifted maximum rank distance codes. They are closely related to resolutions of Steiner systems and therefore they can be used for cryptographic anonymous (2,q+1)-threshold schemes.

Regular parallelisms are connected to translation planes. Lunardon [9] and also Walker [17] established that every regular parallelism in PG(3,q) may be used to construct a spread in PG(7,q), and hence a translation plane of order q' with kernel GF(q) that admit SL(2,q) as a subgroup of their automorphism group.

For the basic concepts and notations concerning spreads and parallelisms of projective spaces, refer, for instance, to [6], [8] or [15].

A spread in PG(n,q) is a set of lines which partition the point set. A parallelism (line parallelisms) is a partition of the set of lines by spreads. There can be line spreads and parallelisms if n is odd.

Two parallelisms are isomorphic if there exists an automorphism of the projective space which maps each spread of the first parallelism to a spread of the second one.

A subgroup of the automorphism group of the projective space which maps each spread of the parallelism to a spread of the same parallelism is called automorphism group of the parallelism.

There are some general constructions of parallelisms: in PG(n,2) by Zaitev et al. [19] and independently by Baker [1], and in PG(2n−1, q) by Beutelspacher [3]. Several constructions are known in PG(3,q) due to Denniston [4], Johnson [8], Penttila and Williams [10].

Computer aided classifications of parallelisms are also available. Stinson and Vanstone classified parallelisms of PG(5,2) with a full automorphism group of order 155 [14] and Sarmiento with a point-transitive cyclic group of order 63 [13]. Topalova and Zhelezova classified parallelisms of PG(3,4) with automorphisms of order 5 [16]. Recently all parallelisms of PG(3,3) were classified by Betten [2].

A regulus of PG(3,q) is a set R of q + 1 mutually skew lines such that any line intersecting three elements of R intersects all elements of R.

A spread S of PG(3,q) is regular if for every three distinct elements of S, the unique regulus determined by them is a subset of S. A parallelism is regular if all its spreads are regular.

Parallelisms of PG(3,2) are regular. Denniston [5] showed two regular parallelisms in PG(3,8). Among the constructed by Prince [11] parallelisms of PG(3,5) with automorphisms of order 31 there are two regular ones. Next Penttila and Williams constructed two families of regular cyclic parallelisms of PG(3,q) for any q ≡ 2 (mod 3) [10]. All presently known examples of regular parallelisms are among them and the existence of other regular parallelisms is an open question.

2. Construction and results

To construct PG(3,5) we use the 4-dimensional vector space over GF(5). The points of PG(3,5) are then all 4-dimensional vectors (v1,v2,v3,v4) over GF(5) such that if v4 = 0 for all k > i then v k = 1. We sort these 156 vectors in ascending lexicographic order and then assign them numbers such that (1,0,0,0) is number 1, and (4,4,4,4) is number 156.

There are 806 lines in PG(3,5). We sort them in ascending lexicographic order defined on the numbers of the lines they contain and assign to each line a number according to this order. The first line contains points {1,2,3,4,5,6} and the last one (806) = \{31,56,75,94,113,132\}.

A spread has 26 lines which partition the point set and a parallelism has 31 spreads.

The main steps of the used method for constructing regular parallelisms with the chosen automorphism group are:

- construction of all regular spreads;
- test the regular spreads if they are invariant under the chosen automorphism group or all its lines are from different orbits under the chosen automorphism group;
- combine the obtained orbit leaders to form a parallelism.

We are interested in regular parallelisms so we begin with the construction of regular spreads. We use backtrack search on the lines [20]. A regular spread of PG(3,5) contains:

\[
\left(\frac{q^2 + 1}{3}\right)\left(\frac{q + 1}{3}\right) = 130 \text{ reguli.}
\]

For each of the 31 lines containing the first point 5000 regular spreads are obtained. This number can be verified by:
Denote by $G$ the full automorphism group of $PG(3,5)$. $G \cong PHL(4,5)$ and it is of order $2^93^25^513.31$. The Sylow 5-subgroups of $G$ have order $5^3$. We use GAP [7] to find an arbitrary Sylow 5-subgroup $G_{5^3}$. It has 6 subgroups of order 5 which are in four conjugacy classes. Any subgroup of $G$ of order 5 is in one of these four conjugacy classes.

With respect to the group action a spread can be of two types:

- fixed – contains the whole orbit of any of its lines;
- not fixed – its lines are from different orbits of one and the same length.

To form a fixed spread some fixed lines are needed together with some of the orbits consisting of skew lines. If a spread is not fixed, we choose for it lines with orbits of one and the same length. Therefore, we already know the other spreads of its orbit. We call the first one orbit leader (a fixed spread is also an orbit leader). To obtain a parallelism we need to obtain only the orbit leaders.

We take an arbitrary subgroup of order 5 from each conjugacy class, namely we consider the following four subgroups:

- subgroup $G_{5^1}$ which fixes 31 points and 56 lines and partitions the lines in 150 orbits;
- subgroup $G_{5^2}$ which fixes 6 points and 31 lines and partitions the lines in 155 orbits;
- subgroup $G_{5^3}$ which fixes 6 points and 6 lines and partitions the lines in 160 orbits;
- subgroup $G_{5^4}$ which fixes a point and a line and partitions the lines in 161 orbits.

Each of these subgroups has at least one fixed line, therefore a resolution has to contain some fixed spreads and the remaining spreads have to be in orbits of length 5.

There aren’t orbits consisting of skew lines under the action of subgroup $G_{5^3}$, so a fixed spread cannot be formed. Therefore a resolution with $G_{5^3}$ doesn’t exist.

The subgroup $G_{5^2}$ fixes 31 lines and 30 of the line orbits are with skew lines. The parallelisms invariant under $G_{5^2}$ have:

- one fixed spread containing a fixed line and 5 orbits with skew lines;
- five fixed spreads containing six fixed lines and 4 orbits with skew lines;
- five orbits of five spreads each.

There are 250 regular spreads with a fixed line but noone with six fixed lines, hence a regular resolution with $G_{5^2}$ doesn’t exist.

The subgroup $G_{5^1}$ fixes the first 6 lines in our lexicographic order, which cover the first 31 points. They share a point (point 1) so each of them has to be in different spread. The smallest point which is in a orbit with skew lines is point 12. Each line in $PG(3,5)$ is incident with six points, so to cover all points until point 12 at least two fixed lines are needed. That is why a resolution with $G_{5^1}$ doesn’t exist.

The subgroup $G_{5^4}$ fixes a line and 100 of the line orbits are with skew lines. The parallelisms invariant under $G_{5^4}$ have:

- one fixed spread containing a fixed line and 5 orbits with skew lines;
- six orbits of five spreads each.

There are 33441 regular spreads with orbit of length 5 but noone with a fixed line, hence a regular resolution with $G_{5^4}$ doesn’t exist.

### 3. Conclusion

We compute the necessary groups and its conjugacy classes using GAP. Our C++ programmes performing the computer computations are based on the exhaustive backtrack search techniques.

Since software mistakes are always possible, we obtain the same number of regular spreads in $PG(3,4)$ as in [12]. To test our software we construct two regular parallelisms of $PG(3,2)$.

As a result of our investigation we can conclude that two of the subgroups of order 5 ($G_{5^1}$ and $G_{5^2}$) cannot produce any parallelism in $PG(3,5)$ while the other two - $G_{5^2}$ and $G_{5^4}$ can be used to construct parallelisms in general but they cannot be regular. So regular parallelisms with automorphisms of order 5 in $PG(3,5)$ do not exist.

### 4. References

[1] Baker, R., Partitioning the planes of $AG_{2m}(2)$ into 2-designs, Discrete Math 15, 1976, 205 – 211.


1 This research is partially supported by the Bulgarian National Science Fund under Contract No I01/0003