МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2015
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2015
Proceedings of the Forty Fourth Spring Conference
of the Union of Bulgarian Mathematicians
SOK "Kamchia", April 2–6, 2015

ON POINT-CYCLIC PARALLELISMS OF $PG(3,7)$*

Stela Zhelezova

A spread of lines 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 parallelism in $PG(n,q)$ is point-cyclic if it has an automorphism group which acts as a Singer automorphism. In $PG(3,7)$ no point-cyclic parallelisms have been known. We claim that such do not exist.

1. Introduction. Parallelisms of projective spaces can be used to construct difference sets in connection with code synchronization [17]. Also parallelisms are used in constructions of constant dimension error-correcting codes that contain lifted maximum rank distance codes [7]. The relation of parallelisms to resolutions of Steiner systems leads to a cryptographic usage for anonymous $(2, q+1)$-threshold schemes [15].

For the basic concepts and notations concerning spreads and parallelisms of projective spaces, refer, for instance, to [6], [10] or [16].

A *t-spread* in $PG(n,q)$ is a set of distinct t-dimensional subspaces which partition the point set. A *t-parallelism* is a partition of the set of t-dimensional subspaces by t-spreads. Usually 1-spreads (1-parallelisms) are called line spreads (line parallelisms) or just spreads (parallelisms). Line spreads and parallelisms could exist 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. A parallelism is *point-transitive* if it has an automorphism group which is transitive on the points. If a parallelism has an automorphism which acts as a cycle of length equals to the number of points then it is point-cyclic.

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a *2-design* with parameters 2-(v,k,λ) if any 2-subset of V is contained in exactly λ blocks of $\mathcal{B}$. A *parallel class* is a partition of the point set of the design by blocks. A *resolution* of the design is a partition of the collection of blocks by parallel classes.

The incidence of the points and t-dimensional subspaces of $PG(n,q)$ defines a 2-design (see for instance [16, 2.35-2.36]). There is a one-to-one correspondence between

*__2010 Mathematics Subject Classification:__ 05B25, 05B40, 05E20.

Key words: Projective space, parallelism, automorphism, combinatorial design.

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

the parallelisms of $PG(3,7)$ and the resolutions of the 2-$(400,8,1)$ design of its points and lines.

Beutelspacher [1] showed the existence of a parallelism in $PG(2^i-1,q)$ for all $i \geq 2$ and the case $i=2$ was proved independently by Denniston [4]. Several constructions of parallelisms are known in $PG(3,q)$ due to Denniston [5], Johnson [10], Prince [12], Penttila and Williams [11]. Several computer aided classifications of point-cyclic t-parallelisms are available too. Sarmiento classified 1 and 2-parallelisms of $PG(5,2)$ with a point-transitive cyclic group of order 63 [13], [14]. Hishida and Jimbo [9] showed that $PG(7,2)$ is point-cyclically resolvable and Braun gave a construction for $PG(9,2)$ [3]. Topalova and Zhelezova showed that the point-transitive parallelisms of $PG(3,4)$ do not exist[18].

A parallelism in $PG(3,7)$ exists by Beutelspacher's theorem [1] but there are no examples known.

We use design approach to the problem. We actually make all the computations on the related to $PG(3,7)$ designs. We choose the 50 spread elements among the 2850 blocks of the 2-$(400,8,1)$ point-line design, and construct the parallelisms as its resolutions. We find a generating set of the automorphism group of $PG(3,7)$ as generating set of the automorphism group of the related 2-$(400,57,8)$ point-hyperplane design. We choose the necessary subgroup of order 25 and compute its normalizer using GAP. Our C++ programmes performing the computer computations are based on the exhaustive backtrack search techniques.

2. Construction and result. There are 400 points and 2850 lines in $PG(3,7)$. Denote by G the full automorphism group of $PG(3,7)$. Hence $G \cong P\Gamma L(4,7)$, whose order is $2^{10}.3^4.5^2.19$. A spread has 50 lines which partition the point set and a parallelism has 57 spreads.

To construct $PG(3,7)$ we use the 4-dimensional vector space over $GF(7)$. The points of $PG(3,7)$ are then all 4-dimensional vectors (v_1,v_2,v_3,v_4) over $GF(7)$ such that $v_i=1$ if i is the maximum index for which $v_i \neq 0$. We sort these 400 vectors in ascending lexicographic order and then assign to each of them a number such that $(1,0,0,0)$ is number 1, and $(6,6,6,1)$ is number 400. We then construct the related designs. To find the generators of their full automorphism group G we use the "Isomorphism and automorphism group" module of Q-Extension program [2].

A point-cyclic parallelism in $PG(3,7)$ has 400 points, that is why the order of point-cyclic automorphism group must be divisible by 25. This is the reason we first try to construct parallelisms with automorphisms of order 25. By Sylow's Theorems all subgroups of order 25 are conjugate, and we can choose an arbitrary one of them. We use GAP [8] to find a Sylow subgroup of order 25 and denote it G_{25}.

We sort the 2850 lines (blocks of the 2-$(400,8,1)$ design) in lexicographic order defined on the numbers of the points they contain and assign to each line a number according to this order. G_{25} partitions the points in 16 orbits of length 25 and the lines in 114 orbits of length 25. We look for line orbits whose lines contain each point at most once. This holds for 50 line orbits, and therefore G_{25} cannot fix more than 25 spreads. There are 57 spreads in a parallelisms, so G_{25} can fix exactly 7 spreads. It follows that parallelisms with an automorphism of order 25 have:

- 7 fixed spreads made of 2 line orbits and
- 2 orbits of 25 spreads each.

Each spread determines all the other spreads through its orbit. We call the first spread *orbit leader*. The fixed spreads are also orbit leaders of orbit length one. To obtain a parallelism with G_{25} we need to construct nine orbit leaders.

At first we start with the fixed part of the parallelism. We use backtrack search on the 50 orbits with disjoint lines and get 49 fixed spreads each lexicographically ordered. Next we find all groups of 7 fixed spreads from the 49 ones. Any fixed part we construct is lexicographically greater than the ones constructed before it. There are many such fixed parts, so at this step we need rejection of isomorphic solutions.

We construct only parallelisms which are invariant under G_{25}. To establish isomorphism of two of the constructed fixed parts it is enough to consider only automorphisms from the normalizer of G_{25} in G – $N(G_{25})$ [18], which is defined as $N(G_{25}) = \{g \in G \mid gG_{25}g^{-1} = G_{25}\}$ and $|N(G_{25})| = 1600$. The normalizer group is transitive on the points. For each fixed part obtained, we check if an automorphism of $N(G_{25})$ maps it to a fixed part with a lexicographically smaller orbit leader sequence, and drop it if so. As a result we obtain 876372 fixed parts.

We next need to construct two orbit leaders from the remaining 100 orbits of length 25. We try two different approaches:

- backtrack search on orbits. The first element in each spread is a line, containing point 1. Then the orbits are shortened by the first spread line – all orbit lines incident with this first line are removed.
- backtrack search on lines not in the fixed part. The first element in each spread is a line, containing point 1. If there are already m elements in the spread, we choose the $m + 1^{-\mathrm{st}}$ one among the lines containing the first point which is in none of the m spread elements and we take in consideration the orbits of the spread lines.

It turns out that this is a very hard computational problem. So we decide to consider only point-cyclic parallelisms.

One of the generators of $N(G_{25})$ is the Singer Cycle. It generates a Singer cyclic group of $G \cong P\Gamma L(4, 7)$. Denote it G_S. We use G_S to construct point-cyclic parallelisms of $PG(3, 7)$. It partitions the lines in one orbit of length 50 and 7 orbits of length 400. Then a point-cyclic parallelism has:

- 1 fixed spread consisting of a line orbit of length 50 and
- 7 spread orbits of length 8 from each orbit of length 400.

We sort each orbit under G_S in lexicographic order defined on the line numbers. We are looking for invariance under G_S, so one spread from each orbit of length 400 is enough to determine the other 7 spreads from this orbit. The first line in each orbit contains point 1. Without loss of generality the spreads we construct from each orbit can contain the corresponding first line. There are no 50 disjoint lines from the line orbit of the line with points $\{1, 9, 10, 11, 12, 13, 14, 15\}$, so a spread cannot be constructed on this orbit.

Since software mistakes are always possible, we try to construct point-cyclic parallelisms of $PG(3, 7)$ in different manner. If some element of $N(G_{25})$ maps a parallelism to itself, it is its automorphism. So the same is for a fixed part. We obtain 621 fixed parts with automorphism of order 1600. Next we consider the line orbits under $N(G_{25})$. There is one orbit of length 50, one of length 400 and three orbits of length 800. To extend fixed parts and obtain point-cyclic parallelism we need to add two more orbit leaders. We construct them on each of non used line orbits under $N(G_{25})$. We perform backtrack search on lines in each sorted orbit as mentioned above (second approach in constructing orbit leaders under G_{25}). The result was the same – a spread cannot be constructed on line orbit of line with points $\{1, 9, 10, 11, 12, 13, 14, 15\}$. We can conclude that there are no point-cyclic parallelisms of $PG(3, 7)$.

REFERENCES

[1] A. Beutelspacher. On parallelisms in finite projective spaces, *Geometriae Dedicata*, **3**, No 1 (1974) 35–45.

[2] I. Bouyukliev. What is Q-extension? *Serdica Journal of Computing*, **1**, No 2 (2007) 115–130.

[3] M. Braun. Construction of a point-cyclic resolution in $PG(9, 2)$. *Innov. Incidence Geom.*, **3** (2006) 33–50.

[4] R. Denniston. Some packings of projective spaces. *Atti Accad. Naz. Lincei.*, **52** (1972) 36–40.

[5] R. Denniston. Packings of $PG(3, q)$. In: Finite Geometric Structures and Their Applications, Edizioni Cremonese, Rome, 1973, 193–199.

[6] J. Eisfeld, L. Storme. (Partial) t-spreads and minimal t-covers in finite projective spaces. Lecture notes from the Socrates Intensive Course on Finite Geometry and its Applications, Ghent, April 2000.

[7] T. Etzion, N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Trans. Inform. Theory* **59**, No 2 (2013) 1004–1017.

[8] GAP – Groups, Algorithms, Programming – a System for Computational Discrete Algebra, `http://www.gap-system.org/`.

[9] T. Hishida, M. Jimbo. Possible patterns of cyclic resolutions of the BIB design associated with $PG(7, 2)$. *Congr. Numer.* **131** (1998) 179–186.

[10] N. Johnson. Combinatorics of Spreads and Parallelisms. Iowa City, CRC Press, 2010.

[11] T. Penttila, B. Williams. Regular packings of $PG(3, q)$. *Eur. J. Combin.*, **19**, No 6 (1998) 713–720.

[12] A. Prince. Parallelisms of $PG(3, 3)$ invariant under a collineation of order 5. In: Mostly Finite Geometries (Norman L. Johnson, ed.), Iowa City, 1996, 383–390; *Lect. Notes Pure Appl. Math.* **190**, Marcel Dekker, New York, 1997.

[13] J. Sarmiento. Resolutions of $PG(5, 2)$ with point-cyclic automorphism group. *J. Comb. Des.*, **8**, No 1 (2000) 2–14.

[14] J. Sarmiento. On Point-Cyclic Resolutions of the 2-(63,7,15) Design Associated with $PG(5, 2)$. *Graph Combinator*, **18** (2002) 621–632.

[15] D. Stinson. Combinatorial Designs: Constructions and Analysis. New York, Springer-Verlag, 2004.

[16] L. Storme. Finite Geometry. In: The CRC Handbook of Combinatorial Designs, CRC Press, second edition, 2006, 702–729.

[17] V. Tonchev. Partitions of difference sets and code synchronization. *Finite Fields Appl.*, **11**, *3* (2005) 601–621.

[18] S. Topalova, S. Zhelezova. On point-transitive and transitive deficiency one parallelisms of $PG(3, 4)$. *Design Code Cryptogr.*, online first at DOI: 10.1007/s10623-013-9887-3.

Stela Zhelezova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.Box 323
5000 Veliko Tarnovo, Bulgaria
e-mail: stela@math.bas.bg

ЗА ЦИКЛИЧНИТЕ ВЪРХУ ТОЧКИТЕ ПАРАЛЕЛИЗМИ НА $PG(3, 7)$

Стела Димитрова Железова

Спредът е множество от прави на $PG(n, q)$, които разбиват множеството от точки. Паралелизмът е разбиване на множеството от прави на спредове. Един паралелизъм е цикличен върху точките, ако притежава група от автоморфизми, действаща като цикъл с дължина броя на точките. До сега циклични върху точките паралелизми на $PG(3, 7)$ не са известни. Ние твърдим, че такива не съществуват.