Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 176-180*

Parallelisms of $PG(3,5)$ with automorphisms of order 13 [1]

Svetlana Topalova svetlana@math.bas.bg
Stela Zhelezova stela@math.bas.bg
Institute of Mathematics and Informatics, BAS, Bulgaria

Dedicated to the memory of Professor Stefan Dodunekov

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. Some constructions of constant dimension codes that contain lifted MRD codes are based on parallelisms of projective spaces. We construct all (321) parallelisms in $PG(3,5)$ with automorphisms of order 13 and find the order of their full automorphism groups.

1 Introduction

The relation to translation planes [4] has been one of the main reasons for the consideration of t-spreads and t-parallelisms. There are applications of spreads and parallelisms in Coding Theory too. For instance, parallelisms are used in constructions of constant dimension error-correcting codes that contain lifted MRD codes [5]. The relation of parallelisms to resolutions of Steiner systems leads to a cryptographic usage for anonymous $(2, q+1)$-threshold schemes [13].

For the basic concepts and notations concerning spreads and parallelisms of projective spaces, refer, for instance, to [4], [7] or [15].

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). 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. A parallelism is called transitive if it has an automorphism group which is transitive on the spreads.

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

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 [15, 2.35-2.36]). There is a one-to-one correspondence between the parallelisms of $PG(3, 5)$ and the resolutions of the 2-(156,6,1) design of its points and lines.

A construction of parallelisms in $PG(n, 2)$ is presented by Zaicev, Zinoviev and Semakov [19] and independently by Baker [1], and in $PG(2^n - 1, q)$ by Beutelspacher [2]. Several constructions are known in $PG(3, q)$ due to Denniston [3], Johnson [7], Penttila and Williams [9].

Several computer aided classifications of t-parallelisms are available too. Prince classified parallelisms of $PG(3, 3)$ with automorphisms of order 5 [10], and parallelisms of $PG(3, 5)$ with automorphisms of order 31 [11]. Stinson and Vanstone classified parallelisms of $PG(5, 2)$ with a full automorphism group of order 155 [14], Sarmiento with a point-transitive cyclic group of order 63 [12], and Zhelezova with a cyclic group of order 31 [20]. Topalova and Zhelezova classified parallelisms of $PG(3, 4)$ with automorphisms of orders 7 [17] and 5 [18], and 2-parallelisms of $PG(5, 2)$ with automorphisms of order 31 [16].

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. Each regular parallelism of $PG(3, q)$ corresponds to a translation plane of order q^4 [8].

In 1998 Prince constructed all 45 transitive parallelisms of $PG(3, 5)$. They are cyclic and possess automorphisms of order 31. Among them there are two regular parallelisms. A little later in 1998 Penttila and Williams constructed two regular cyclic parallelisms of $PG(3, q)$ for any $q \equiv 2 \ (mod\ 3)$ [9]. All presently known examples of regular parallelisms are among them and the existence of other regular parallelisms is an open question.

We check all the constructed parallelisms for regularity. There are no regular ones among them.

Our C++ programmes performing the computer computations are based on the exhaustive backtrack search techniques. To filter away isomorphic parallelisms, we find the normalizer of the chosen subgroup of order 13 in the automorphism group of the projective space.

We use design approach to the problem. We actually make all the computations on the related to $PG(3, 5)$ designs, namely, we choose the 26 spread elements among the 806 blocks of the 2-$(156, 6, 1)$ point-line design, and construct the parallelisms as its resolutions. We find a generating set of the automorphism group of $PG(3, 5)$ as generating set of the automorphism group of the related 2-$(156, 31, 6)$ point-hyperplane design.

2 Construction of the parallelisms

There are 156 points and 806 lines in $PG(3,5)$. Denote by G the full automorphism group of $PG(3,5)$. It is of order $29016000000 = 2^9.3^2.5^6.13.31$. A spread has 26 lines which partition the point set and a parallelism has 31 spreads.

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 (v_1, v_2, v_3, v_4) over $GF(5)$ such that $v_i = 1$ if i is the maximum index for which $v_i \neq 0$. We sort these 156 vectors in ascending lexicographic order and then assign them numbers such that $(1,0,0,0)$ is number 1, and $(4,4,4,1)$ number 156. We then construct the related designs and find the generators of their full automorphism group G.

By Sylow's Theorems all subgroups of order 13 are conjugate, and we can choose an arbitrary one of them. We use GAP [6] to find a Sylow subgroup of order 13 and denote it G_{13}.

We sort the 806 lines (blocks of the 2-$(156, 6, 1)$ 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_{13} partitions the points in 12 orbits of length 13 and the lines in 62 orbits of length 13. We look for line orbits whose lines contain each point at most once. This holds for 26 line orbits, and therefore G_{13} cannot fix more than 13 spreads. It follows that parallelisms with an automorphism of order 13 have

- 5 fixed spreads made of 2 line orbits and
- 2 orbits of 13 spreads each.

We construct the spreads by backtrack search. The first element in each spread is a line, containing point 1. If there are already m elements in the spread, we choose the $m+1$-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. Any spread we construct is lexicographically greater than the ones constructed before it. Each spread determines all the other spreads of its orbit. We call the first spread *orbit leader*. To obtain a parallelism with G_{13} we need to construct only the seven orbit leaders.

The rejection of isomorphic solutions is an important part of the computation. We construct only parallelisms which are invariant under G_{13}. Therefore we have to check if there is some permutation $\varphi \in G$ such that it maps a parallelism with G_{13} to another parallelism with G_{13}.

Let $\mathcal{P}$ and $\mathcal{P}'$ be two of the constructed parallelisms such that $\mathcal{P}' = \varphi\mathcal{P}$. Let $\alpha \in G_{13}$. Then $\varphi\mathcal{P} = \alpha\varphi\mathcal{P}$ and thus $\mathcal{P} = \varphi^{-1}\alpha\varphi\mathcal{P}$, namely $\varphi^{-1}\alpha\varphi$ is also an automorphism of $\mathcal{P}$. That is why $\mathcal{P}$ is invariant both under G_{13} and under $\varphi^{-1}G_{13}\varphi$. If $\varphi^{-1}G_{13}\varphi = G_{13}$, then φ is in the normalizer $N(G_{13})$ of G_{13} in G, which is defined as $N(G_{13}) = \{g \in G \mid gG_{13}g^{-1} = G_{13}\}$. If φ is not in the normalizer, then $\varphi^{-1}G_{13}\varphi$ is a conjugate subgroup and since φ is not an automorphism of $\mathcal{P}$, there must exist an automorphism ψ of $\mathcal{P}$ such that $\varphi^{-1}G_{13}\varphi = \psi G_{13}\psi^{-1}$. Then $G_{13} = \varphi\psi G_{13}\psi^{-1}\varphi^{-1}$ and therefore $\varphi\psi \in N(G_{13})$. Since $\varphi\psi\mathcal{P} = \varphi\mathcal{P}$, to establish isomorphism of two of the constructed parallelisms it is enough to consider only automorphisms from $N(G_{13})$.

For each parallelism $\mathcal{P}$ we obtain, we check if an automorphism of $N(G_{13})$ maps it to a parallelism with a lexicographically smaller orbit leader sequence, and drop it if so.

If some element of $N(G_{13})$ maps $\mathcal{P}$ to itself, it is its automorphism. So by the isomorphism test we also obtain some of the automorphisms of this parallelism. If $\mathcal{P}$ has an automorphism $\psi \notin N(G_{13})$, then it is invariant under $\psi G_{13}\psi^{-1}$. That is why we check if $\mathcal{P}$ is invariant under some conjugate subgroup of G_{13}. In fact we establish that none of the constructed parallelisms are invariant under conjugate subgroups.

3 Classification results

We obtain 321 non-isomorphic parallelisms. All of them have automorphisms of order 13 only. We find out that there are no regular ones among them.

Since software mistakes are always possible, we obtained the number of non-isomorphic parallelisms by two different C++ programmes (written by the two authors).

References

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

[2] A. Beutelspacher, On parallelisms in finite projective spaces, *Geometriae Dedicata* 3 (1), 1974, 35-45.

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

[4] 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.

[5] T. Etzion, N. Silberstein, Codes and designs related to lifted MRD codes, *IEEE Trans. Inform. Theory* 59 (2), 2013, 1004-1017.

[6] *GAP - Groups, Algorithms, Programming* - a System for Computational Discrete Algebra (http://www.gap-system.org/).

[7] N. Johnson, *Combinatorics of Spreads and Parallelisms*, CRC Press, 2010.

[8] G. Lunardon, On regular parallelisms in $PG(3,q)$, *Discrete Math.* 51, 1984, 229-335.

[9] T. Penttila, B. Williams, Regular packings of $PG(3,q)$, *Europ. J. Combin.* 19 (6), 1998, 713-720.

[10] A. Prince, Parallelisms of PG(3,3) invariant under a collineation of order 5, In *Mostly Finite Geometries* (Iowa City, 1996), 383-390 (Norman L. Johnson, ed.), *Lect Notes Pure Appl Math* 190, Marcel Dekker, New York (l997).

[11] A. Prince, The cyclic parallelisms of PG(3,5), *Europ. J. Combin.* 19 (5), 1998, 613-616.

[12] J. Sarmiento, Resolutions of PG(5,2) with point-cyclic automorphism group, *J. Combin. Des.* 8 (1), 200, 2-14.

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

[14] D. Stinson, S. Vanstone, Orthogonal packings in PG(5,2), *Aequationes Mathematicae* 31 (1), 1986, 159-168.

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

[16] S. Topalova, S. Zhelezova, 2-spreads and transitive and orthogonal 2-parallelisms of PG(5,2), *Graph. Combin.* 26 (5), 2010, 727-735.

[17] S. Topalova, S. Zhelezova, On transitive parallelisms of PG(3,4), *Appl. Algebr. Eng. Comm.*, online first at DOI: 10.1007/s00200-013-0194-z, 2013.

[18] S. Topalova, S. Zhelezova, On point-transitive and transitive deficiency one parallelisms of PG(3,4), *Design Codes Crypt.*, revision submitted.

[19] G. Zaicev, V. Zinoviev, N. Semakov, Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error--correcting codes, *Proc. of Second Intern. Symp. on Information Theory*, (Armenia, USSR, 1971), Budapest, Academiai Kiado, 1973, 257-263.

[20] S. Zhelezova, Cyclic parallelisms of PG(5,2), *Math Balkanica* 24 (1-2), 2010, 141-146.