МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2022
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2022
Proceedings of the Fifty First Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, April 5–9, 2022

PARALLELISMS OF PG(n, q)

Svetlana Topalova, Stela Zhelezova

Let PG(n, q) be the n-dimensional projective space over the finite field $GF(q)$. A set of lines, such that each point is in exactly one of these lines, is called a *spread*. A *parallelism* is a partition of the lines of the projective space to spreads. The present paper considers the main properties of parallelisms of PG(n, q), the motivation for their study, the known results and some open problems in this research area.

1. Introduction – definitions and notations. A finite field $GF(q)$ (*Galois field*) is a set of q elements with the operations addition, subtraction, multiplication, and division defined on them. Finite fields $GF(q)$ exist for $q = p^n$, where p is a prime. If q is a prime, the residues modulo q make up $GF(q)$.

Example 1.1. $GF(2)$ has two elements 0 and 1, and the three elements of $GF(3)$ are $0, 1$ and 2. The addition and multiplication in these fields is presented below, while subtraction and division follow from them in the usual way.

in GF(2)

+	0	1
0	0	1
1	1	0

in GF(2)

*	0	1
0	0	0
1	0	1

in GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

in GF(3)

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Consider the vector space $V(d, q)$, whose elements are all the d-dimensional vectors $\nu = (v_d, v_{d-1}, \ldots, v_1)$ with coordinates v_i from $GF(q)$. We denote by $\mathbf{0}$ the vector $(0, 0, \ldots, 0)$. Addition (subtraction) of vectors of $V(d, q)$ is defined as addition (subtraction) of their corresponding coordinates in $GF(q)$. Let $a \in GF(q)$. Then $a\nu$ is the vector obtained by multiplication of the coordinates of ν by a.

Example 1.2. Consider $V(4, 2)$. Its elements are the sixteen vectors

$(0,0,0,0)$	$(0,1,0,0)$	$(1,0,0,0)$	$(1,1,0,0)$
$(0,0,0,1)$	$(0,1,0,1)$	$(1,0,0,1)$	$(1,1,0,1)$
$(0,0,1,0)$	$(0,1,1,0)$	$(1,0,1,0)$	$(1,1,1,0)$
$(0,0,1,1)$	$(0,1,1,1)$	$(1,0,1,1)$	$(1,1,1,1)$

2020 Mathematics Subject Classification: 05B25, 05B40, 05E20.
Key words: Projective space, parallelism, classification, automorphism.
The research is partially supported by the Bulgarian National Science Fund under Contract No KP-06-N32/2-2019.

Example 1.3. Consider $V(4,3)$. Its elements are the 81 vectors

$(0,0,0,0)$	$(0,1,0,0)$	$(0,2,0,0)$	$(1,0,0,0)$	$(1,1,0,0)$	$(1,2,0,0)$	$(2,0,0,0)$	$(2,1,0,0)$	$(2,2,0,0)$
$(0,0,0,1)$	$(0,1,0,1)$	$(0,2,0,1)$	$(1,0,0,1)$	$(1,1,0,1)$	$(1,2,0,1)$	$(2,0,0,1)$	$(2,1,0,1)$	$(2,2,0,1)$
$(0,0,0,2)$	$(0,1,0,2)$	$(0,2,0,2)$	$(1,0,0,2)$	$(1,1,0,2)$	$(1,2,0,2)$	$(2,0,0,2)$	$(2,1,0,2)$	$(2,2,0,2)$
$(0,0,1,0)$	$(0,1,1,0)$	$(0,2,1,0)$	$(1,0,1,0)$	$(1,1,1,0)$	$(1,2,1,0)$	$(2,0,1,0)$	$(2,1,1,0)$	$(2,2,1,0)$
$(0,0,1,1)$	$(0,1,1,1)$	$(0,2,1,1)$	$(1,0,1,1)$	$(1,1,1,1)$	$(1,2,1,1)$	$(2,0,1,1)$	$(2,1,1,1)$	$(2,2,1,1)$
$(0,0,1,2)$	$(0,1,1,2)$	$(0,2,1,2)$	$(1,0,1,2)$	$(1,1,1,2)$	$(1,2,1,2)$	$(2,0,1,2)$	$(2,1,1,2)$	$(2,2,1,2)$
$(0,0,2,0)$	$(0,1,2,0)$	$(0,2,2,0)$	$(1,0,2,0)$	$(1,1,2,0)$	$(1,2,2,0)$	$(2,0,2,0)$	$(2,1,2,0)$	$(2,2,2,0)$
$(0,0,2,1)$	$(0,1,2,1)$	$(0,2,2,1)$	$(1,0,2,1)$	$(1,1,2,1)$	$(1,2,2,1)$	$(2,0,2,1)$	$(2,1,2,1)$	$(2,2,2,1)$
$(0,0,2,2)$	$(0,1,2,2)$	$(0,2,2,2)$	$(1,0,2,2)$	$(1,1,2,2)$	$(1,2,2,2)$	$(2,0,2,2)$	$(2,1,2,2)$	$(2,2,2,2)$

Define an equivalence relation $\approx$, such that for $x, y \in V(d,q)$, $x \approx y$ if there is a nonzero element a of $GF(q)$ such that $x = ay$.

Example 1.4. Consider $V(4,3)$. Since $(2,1,2,0) = 2(1,2,1,0)$, the vectors $(2,1,2,0)$ and $(1,2,1,0)$ are in one and the same $\approx$-equivalence class, namely $(2,1,2,0) \approx (1,2,1,0)$.

Given the vector space $V(n+1,q)$, the set of $\approx$-equivalence classes of $V(n+1,q) \setminus \{\mathbf{0}\}$ is the *n-dimensional projective space over* $GF(q)$. It is denoted by $\mathrm{PG}(n,q)$. Without loss of generality we can assume that its elements (called *points*) are the vectors $\nu = (v_{n+1}, v_n \ldots, v_1)$ of $V(n+1,q)$ for which $v_i = 1$ if $v_k = 0$ for each $k > i$. The projective space $\mathrm{PG}(n,q)$ has projective subspaces of dimension t for $0 \leq t < n$, where the subspaces of dimension 0 are the points, the subspaces of dimension 1 are called *lines*, of dimension 2 – *planes*, and of dimension $n-1$ – *hyperplanes*. The relations between the subspaces define geometric properties, namely: any two points are together in a unique line, a line has $q+1$ points, two lines can intersect in at most one point, two intersecting lines define a plane, etc.

Let $X = \{x_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of X, called *blocks*. $D = (X, \mathcal{B})$ is a *2-design* with parameters 2-(v,k,λ) if any 2-subset of X is contained in exactly λ blocks of $\mathcal{B}$.

We assign numbers to the points and lines of $\mathrm{PG}(n,q)$ in a convenient way (usually in a defined on them lexicographic order). This way the projective space can be presented by the point-line incidence matrix. Denote by v the number of the points, and by b the number of the lines of $\mathrm{PG}(n,q)$. The point-line incidence matrix is a $\{0,1\}$ matrix with v rows and b columns, such that the element in the i-th row and j-th column is equal to 1 if line j contains point i and equal to 0 if it does not. Because of the above-mentioned geometric properties of $PG(n,q)$, the point-line incidence defines a 2-design and the point-line incidence matrix is the incidence matrix of a 2-design.

Example 1.5. Consider $\mathrm{PG}(3,2)$. Its elements are all the fifteen nonzero vectors of $V(4,2)$:

	4) $(0,1,0,0)$	8) $(1,0,0,0)$	12) $(1,1,0,0)$
1) $(0,0,0,1)$	5) $(0,1,0,1)$	9) $(1,0,0,1)$	13) $(1,1,0,1)$
2) $(0,0,1,0)$	6) $(0,1,1,0)$	10) $(1,0,1,0)$	14) $(1,1,1,0)$
3) $(0,0,1,1)$	7) $(0,1,1,1)$	11) $(1,0,1,1)$	15) $(1,1,1,1)$

There are 15 points, 35 lines and 15 hyperplanes. For example points 1, 2 and 3 are the points of one line, because $(0,0,0,1) + (0,0,1,0) = (0,0,1,1)$, $(0,0,0,1) + (0,0,1,1) = (0,0,1,0)$ and $(0,0,1,0) + (0,0,1,1) = (0,0,0,1)$. It is easy to check that points $1, 2, \ldots, 7$ are the points of one hyperplane because addition of any two of the vectors of the corresponding set of 7 vectors gives a vector from this set. The point-line incidence defines a 2-$(15, 3, 1)$ design. Its incidence matrix is presented in Figure 1, where dots stand in place of zeros.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
1	1	1	1	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
2	1	.	.	.	.	.	.	1	1	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
3	1	.	.	.	.	.	.	.	.	.	.	.	.	1	1	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
4	.	1	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	.	.	1	1	1	1	.	.	.	.	.	.	.	.	.	.	.	.
5	.	1	.	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	.	.	.	.	.	1	1	1	1	.	.	.	.	.	.	.	.
6	.	.	1	.	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	.	1	1	1	1	.	.	.	.
7	.	.	1	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1	1	1	1
8	.	.	.	1	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.
9	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1	.	.
10	.	.	.	.	1	.	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1	.
11	.	.	.	.	1	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	1
12	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	.	.	1	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1
13	.	.	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	1	.	1	.	.	1	.	.	.	.	.	.	1	.	.	1	.
14	.	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	.	.	1	.	.	1	.	.	.	.	1	1	.	.	.	.	1	.	.
15	.	.	.	.	.	.	1	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	1	.	.	1	.	.	1	.	.	.

Fig. 1. The point-line incidence of PG$(3, 2)$ defines a 2-(15,3,1) design

Example 1.6. Consider PG$(3, 3)$. Its elements are the following 40 vectors of $V(4, 3)$:

1) $(0,0,0,1)$	5) $(0,1,0,0)$	14) $(1,0,0,0)$	23) $(1,1,0,0)$	32) $(1,2,0,0)$
2) $(0,0,1,0)$	6) $(0,1,0,1)$	15) $(1,0,0,1)$	24) $(1,1,0,1)$	33) $(1,2,0,1)$
3) $(0,0,1,1)$	7) $(0,1,0,2)$	16) $(1,0,0,2)$	25) $(1,1,0,2)$	34) $(1,2,0,2)$
4) $(0,0,1,2)$	8) $(0,1,1,0)$	17) $(1,0,1,0)$	26) $(1,1,1,0)$	35) $(1,2,1,0)$
	9) $(0,1,1,1)$	18) $(1,0,1,1)$	27) $(1,1,1,1)$	36) $(1,2,1,1)$
	10) $(0,1,1,2)$	19) $(1,0,1,2)$	28) $(1,1,1,2)$	37) $(1,2,1,2)$
	11) $(0,1,2,0)$	20) $(1,0,2,0)$	29) $(1,1,2,0)$	38) $(1,2,2,0)$
	12) $(0,1,2,1)$	21) $(1,0,2,1)$	30) $(1,1,2,1)$	39) $(1,2,2,1)$
	13) $(0,1,2,2)$	22) $(1,0,2,2)$	31) $(1,1,2,2)$	40) $(1,2,2,2)$

There are 40 points, 130 lines and 40 hyperplanes. For example, points 1, 2, 3 and 4 are the points of one line, and points $1, 2, \ldots, 13$ - of one hyperplane. The point-line incidence defines a 2-$(40, 4, 1)$ design. Its incidence matrix has 40 rows and 130 columns.

A *spread* in PG(n, q) is a set of disjoint lines, such that each point is in exactly one line. A *parallelism* of PG(n, q) is a partition of the line set to spreads. A necessary condition for the existence of spreads and parallelisms is n to be odd. A *parallel class* of a 2-(v, k, λ) design is a set of blocks, such that each point is in exactly one block. A *resolution* of a 2-(v, k, λ) design is a partition of its collection of blocks to parallel classes. There is a one-to-one correspondence between the parallelisms of PG(n, q) and the resolutions of its point-line design.

Example 1.7. A spread of PG$(3, 2)$ has 5 lines, and a parallelism contains 7 spreads. An example of a parallelism is presented in Figure 2, where there are vertical lines between the spreads.

An *automorphism* of PG(n, q) is a permutation of the points which maps each line to another line of PG(n, q). All the automorphisms make up a group which is called the *full automorphism group*. PG(n, q) has a lot of symmetry. Therefore its full automorphism

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
1	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.
2	1	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.
3	1	.	.	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.	.	.	1	.	.
4	.	1	.	.	.	1	.	.	.	.	.	.	.	1	.	.	.	.	1	.	.	.	1	.	.	.	1	.	.	.	.	.	.	1	.
5	.	.	1	.	.	1	.	.	.	.	.	.	.	.	1	.	.	1	.	.	.	.	.	1	.	.	.	.	1	.	.	1	.	.	.
6	.	.	.	1	.	.	.	.	1	.	1	.	.	.	.	.	.	1	.	.	.	.	.	.	1	.	1	.	.	.	.	.	.	.	1
7	.	.	.	.	1	.	.	.	.	1	1	.	.	.	.	.	.	.	.	1	.	.	1	.	.	.	.	.	.	1	.	1	.	.	.
8	.	1	.	.	.	.	1	.	.	.	.	.	.	.	1	1	.	.	.	.	.	.	.	.	1	.	.	.	.	1	.	.	1	.	.
9	.	.	.	.	1	.	.	.	1	.	.	1	.	.	.	1	.	.	.	.	.	.	.	1	.	.	.	1	.	.	.	.	.	1	.
10	.	.	1	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	1	1	.	.	.	.	.	.	1	.	.	.	.	.	.	1
11	.	.	.	1	.	.	.	.	.	1	.	1	.	.	.	.	.	.	1	.	1	.	.	.	.	.	.	.	1	.	.	.	1	.	.
12	.	1	.	.	.	.	.	.	.	1	.	.	1	.	.	.	1	.	.	.	.	.	.	1	.	1	.	.	.	.	.	.	.	.	1
13	.	.	.	1	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	1	.	1	.	.	.	1	.	.	.	.	.	.	.	1	.
14	.	.	.	.	1	.	.	1	.	.	.	.	.	1	.	.	1	.	.	.	.	.	.	.	1	.	.	.	1	.	1	.	.	.	.
15	.	.	1	.	.	.	.	.	1	.	.	.	1	.	.	.	.	.	1	.	.	1	.	.	.	.	.	.	.	1	1	.	.	.	.

Fig. 2. A parallelism of PG(3, 2) corresponds to a resolution of the point-line 2-(15,3,1) design

group is very rich. It is isomorphic to the group $P\Gamma L(n+1, q)$ a description of which can be found, for instance, in [3].

Example 1.8. We present here the number of automorphisms of the projective spaces $\mathrm{PG}(n, q)$ with the smallest parameters $n > 2$ and $q \geq 2$.

projective space	automorphisms
$\mathrm{PG}(3, 2)$	$20160 = 2^6.3^2.5.7$
$\mathrm{PG}(3, 3)$	$12130560 = 2^8.3^6.5.13$
$\mathrm{PG}(3, 4)$	$1974067200 = 2^{13}.3^4.5^2.7.17$
$\mathrm{PG}(3, 5)$	$29016000000 = 2^9.3^2.5^6.13.31$
$\mathrm{PG}(5, 2)$	$20158709760 = 2^{15}.3^4.5.7^2.31$

Two spreads are *isomorphic* if there is an automorphism of the projective space which maps one to the other. Two parallelisms are *isomorphic* if there is an automorphism of $\mathrm{PG}(n, q)$ which maps the spreads of one parallelism to spreads of the other. An *automorphism* of a parallelism is an automorphism of $\mathrm{PG}(n, q)$ which maps each of its spreads to a spread of the same parallelism. A parallelism is called *cyclic* if it has an automorphism which maps its spreads to one another in one cycle.

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. Such a line is called *transversal*. All the transversals of a regulus form its *opposite regulus*. 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 spread which contains no reguli is *aregular*. A spread is called *Hall spread* if it can be obtained from a regular spread by a replacement of one regulus by its opposite.

2. Motivation. Research on t-spreads and t-parallelisms is motivated by their various relations and applications. Since parallelisms are resolutions of the point-line design, they can be successfully used in many known applications of resolutions, such as statistical experiment [9], cryptographic usage (anonymous $(2, q+1)$-threshold schemes [37], wireless key pre-distribution schemes [34], authentication codes [27]) and resolution-based constructions of error-correcting codes (optimal constant composition codes [13], equidistant q-ary codes [36], regular low density parity-check (LDPC) codes [21], fractional repetition codes with flexible repair [29]).

Example 2.1. The resolution of the point-line 2-(15,3,1) design from Figure 2 gives one possible answer to the famous *fifteen school girls arrangement problem* which was first considered by Kirkman [25], namely the fifteen girls of a class go for a walk three by three and we want that each day of the week each girl walks in a row with different other two girls. The seven parallel classes of the resolution present the arrangements for the seven days, where the girls are given numbers from 1 to 15. For instance, on the second day the five rows of girls are 1-4-5, 2-8-10, 3-13-14, 6-9-15 and 7-11-12. Suppose that you are interested in the behavior of some of the students during the walks. On a weekly basis your observations are not likely to depend on the arrangement. That is why design resolutions have applications in statistical experiments.

Example 2.2. Cryptographic applications of resolutions are often based on the fact that each parallel class is uniquely defined by any of its lines, and each line itself is uniquely defined by any two of its points. A perfect anonymous (t, k)-threshold scheme, for instance, is a method of sharing a secret value w among k participants in such a way that any t participants can compute the value of w but no group of $t-1$ (or fewer) participants can compute any information about the value of w from the information they hold collectively. The resolution from Fig. 2 can be successfully used to define a perfect anonymous $(2, 3)$-threshold scheme. The secret w is the number of a spread. Let $w = 4$. A line from this spread is chosen at random. Suppose this is $l_{13} \in S_4$. Next the $k = 3$ points of $l_{13} = \{3, 12, 15\}$ are distributed among the $k = 3$ participants. Since two points determine a unique line, the points of two participants are enough to determine the chosen line l_{13} and thus the secret value $w = 4$.

Parallelisms, however, have also relations and applications which do not exist for resolutions in general. One of the best known relations is to translation planes [8, 20], and the recently most investigated relation is that to subspace codes [15] because of their application in random network coding [26]. Examples of applications of parallelisms in this area can be found in [14], [17], and a recent survey in [15].

3. State-of-the-art and open problems. There has been a considerable interest in the construction of parallelisms in the last several decades. Some of the obtained results are purely theoretical, and some are computer-aided. There are several general constructions of infinite families of parallelisms. They are based on properties of the subspaces of $\mathrm{PG}(n, q)$. A construction of parallelisms in $\mathrm{PG}(n, 2)$ is presented by Zaicev, Zinoviev and Semakov [45] and independently by Baker [1], and in $PG(2^m - 1, q)$ by Beutelspacher [6]. Constructions in $PG(3, q)$ are known due to Denniston [10] and Johnson [19]. Note that for $q > 2$ there are many values of n for which no parallelisms of $\mathrm{PG}(n, q)$ are known. Presently there is only one example of parallelisms in a projective space with $q > 2$ and $n \neq 2^m - 1$, namely in $\mathrm{PG}(5, 3)$ [16].

Open problem 3.1. *Construct new infinite families of parallelisms of* $\mathrm{PG}(n, q)$.

Open problem 3.2. *Find more examples of parallelisms of* $\mathrm{PG}(n, q)$ *for* $q > 2$ *and* $n \neq 2^m - 1$.

Outside the known infinite families, however, there are plenty of explicitly constructed (usually by computer-aided methods) parallelisms in $\mathrm{PG}(n, q)$ with relatively small parameters n and q. Most of these parallelisms are available online and this makes them easy to use in applications and further investigations. All parallelisms of $\mathrm{PG}(3, 2)$ [20] and

PG(3, 3) [4] are known. For projective spaces with slightly bigger parameters the classification problem is open, but there are computer-aided classifications of parallelisms with certain assumed automorphism groups due to Stinson and Vanstone [38], Prince [31, 33], Sarmiento [35], Betten, Topalova and Zhelezova [5], Topalova and Zhelezova[40, 41, 42]. Computer-aided classifications are based on backtrack search with rejection of equivalent partial solutions [43]. Assuming an automorphism group makes the problem much easier. Parallelisms without the assumed automorphisms are not constructed, but the results contribute significantly to the study of the properties and the possible applications of parallelisms. Table 1 shows the number *num* of known parallelisms of PG(3, 4), PG(3, 5) and PG(5, 2) which possess *aut* nontrivial automorphisms.

Table 1. Known parallelisms with nontrivial automorphisms in PG(3, 4), PG(3, 5) and PG(5, 2)

PG(3,4)

aut	num
2	$\geq$ 303603
3	8 115 559
4	716 870
5	31 830
6	4 488
7	482
8	4480
10	76
12	52
15	40
16	206

PG(3,4)

aut	num
17	0
20	52
24	14
30	38
32	14
48	12
60	8
64	4
96	2
960	4

PG(3,5)

aut	num
3	$\geq$ 6
8	$\geq$ 8143
13	321
16	$\geq$952
24	$\geq$ 610
25	4146
32	$\geq$ 56
48	$\geq$ 90
50	120

PG(3,5)

aut	num
93	45
96	$\geq$ 6
100	80
200	82
400	17
600	4
1200	6
2400	2
other	$\geq$ 0

PG(5,2)

aut	num
21	$\geq$ 2134
31	1090208
63	14
155	286
other	$\geq$ 0

In PG(3, 4) only parallelisms with a full automorphism group of order 2 have remained not classified. In projective spaces with bigger parameters, however, it is supposed that there exist a lot of parallelisms with full automorphism groups for which no explicit examples are known yet.

Open problem 3.3. *For relatively small parameters n and q construct new parallelisms with certain properties or automorphism groups.*

The study of the properties of a parallelism (possible types of spreads, possible automorphism groups, etc.) and their dependence on the parameter set or other properties, has attained a lot of attention. The main theoretical results can be found in Johnson's book [20].

The construction of parallelisms with spreads of a particular type is of interest because of their relations to other combinatorial structures. Regular parallelisms in $PG(2r-1, q)$, for instance, are of major importance because of their relation to translation planes of order q^{2r} [18, 28, 46]. Regular parallelisms contain only regular spreads. Only one infinite family of regular parallelisms is known by now. It is provided by Pentilla and Williams who succeeded to generalize the computer results from [33] and constructed two regular cyclic parallelisms of $PG(3, q)$ for any $q \equiv 2 \pmod 3$ [30]. Computer-aided constructions show that there exist regular parallelisms of $PG(3, 5)$ which are not cyclic and do not belong to this infinite family [41]. Maybe this computer result can lead to a generalization too ...

Open problem 3.4. *Find new infinite families or/and new examples of regular parallelisms.*

Up to isomorphism there is only one regular spread. That is why the spreads of a regular parallelism are isomorphic to each other. Parallelisms with spreads which are isomorphic to each other, are called *uniform*. Cyclic parallelisms are obviously uniform. The known uniform parallelisms of small projective spaces are presented in Table 2, where *aut* is the order of their full automorphism group, and *spr* is the type of their spreads. Up to isomorphism there is one spread in $\mathrm{PG}(3,2)$ (the regular one) and all (two) parallelisms are regular (Table 2, a.). There are two spreads in $\mathrm{PG}(3,3)$ (regular and subregular), but all uniform parallelisms are subregular [4, 32] (Table 2, b.). There are no regular parallelisms in $\mathrm{PG}(3,4)$ either [2], where the nonisomorphic spreads are three - regular, subregular (Hall) and aregular (Table 2, c.). The nonisomorphic spreads of $\mathrm{PG}(3,5)$ are 21 and presently 51 uniform parallelisms are known with 45 cyclic [33] and 8 regular ones [41] among them. There are 1904640 spreads in $\mathrm{PG}(5,2)$ and 1090494 uniform cyclic parallelisms.

Table 2. Uniform parallelisms in $\mathrm{PG}(3,2)$, $\mathrm{PG}(3,3)$ and $\mathrm{PG}(3,4)$

a) PG(3,2)

spr\aut	168	all
regular	2	2

b) PG(3,3)

spr\aut	1	2	4	8	16	32	all
regular	–	–	–	–	–	–	0
subregular	2358	372	103	19	4	4	2860

c) PG(3,4)

spr\aut	1	2	4	5	7	10	20	all
regular	–	–	–	–	–	–	–	0
subregular	≥ 0	7999	244	346	24	2	8	≥ 8623
aregular	≥ 0	≥ 22144	4816	–	178	–	–	≥ 27138

A *deficiency one parallelism* is a partial parallelism with one spread less than the parallelism. Each deficiency one parallelism can be uniquely extended to a parallelism. Table 3 presents the types of the spreads of the known uniform deficiency one parallelisms of $\mathrm{PG}(3,4)$ and $\mathrm{PG}(3,5)$. Except for one spread (the deficiency spread), all the other spreads of such a parallelism (twenty for $\mathrm{PG}(3,4)$ and thirty for $\mathrm{PG}(3,5)$) are isomorphic to each other.

Open problem 3.5. *Find new uniform parallelisms and new uniform deficiency one parallelisms.*

Open problem 3.6. *Establish which spreads of* $\mathrm{PG}(n,q)$ *can take part in uniform parallelisms and which – in uniform deficiency one parallelisms.*

The possible automorphism groups of parallelisms have been intensively studied too [23], and in particular, investigations have been done on the existence of automorphism groups that are transitive on the spreads or on the points of a parallelism. A parallelism is *transitive* if it has an automorphism group which is transitive on its spreads. A parallelism is point-transitive if it has an automorphism group which is transitive on the points.

Table 3. Uniform deficiency one parallelisms in PG(3, 4) and PG(3, 5)

a) PG(3, 4)

spr\aut	≤2	3	4	5	6	8	10	12	15	16	20	24	30	32	48	60	64	96	960	all
1R, 20H	≥0		3291	142	124	970	2	52	4	118	8	6	4	6	12	8	4	2	4	≥4757
1R, 20A	≥0	259661	2018	1410		56	4		16				12							≥263177
1H, 20A	≥0			4250			6													≥4256
1A, 20H	≥0		1711																	≥1711

b) PG(3, 5)

spr\aut	8	16	24	25	32	48	50	96	100	200	400	600	1200	2400	other	all
1R, 30H	≥16	≥28	≥8	4124	≥8	≥16	120	≥6	80	82	17	4	6	2	≥ 0	≥4517
1R, 30N			≥6												≥ 0	≥6
1N, 30H	≥4		≥6												≥ 0	≥10
1N, 30N	≥8	≥40	≥10			≥8									≥ 0	≥66

spreads: R – regular, A – aregular, H – Hall, N – not isomorphic to R, A or H

Examples of transitive parallelisms of PG$(3, q)$ are presented in [10], [11], [30] and [33], and of $PG(5, 2)$ in [38] and [48]. Transitivity and double transitivity is considered by Johnson [20] and by Johnson and Montinaro [22, 23], who show that only two doubly-transitive parallelisms exist, and these are all the parallelisms in $PG(3, 2)$.

Most of the known transitive parallelisms are cyclic. Nonexistence of cyclic parallelisms in PG$(2n - 1, q)$ with $gcd(2n - 1, q - 1) > 1$ and in $PG(3, q)$ with $q \equiv 0$ $(mod\ 3)$ was shown by White [47]. Two cyclic parallelisms in PG$(3, q)$ exist for $q \equiv 2$ $(mod\ 3)$ by the infinite class constructed by Pentilla and Williams. They are also regular and dual to each other. Computer-aided constructions of cyclic parallelisms are known in PG$(3, 5)$ (45 parallelisms) [33] and PG$(5, 2)$ (1090494 parallelisms) [38, 48].

A parallelism is *point-cyclic* if it has an automorphism moving its points in one cycle. There are no point-cyclic parallelisms in PG$(3, q)$, $q \leq 5$. Point-cyclic parallelisms in PG$(n, 2)$, $5 \leq n \leq 9$ are classified.

Open problem 3.7. *Find the reason for the nonexistence of point-cyclic parallelisms in* PG$(3, q)$*,* $q \leq 5$.

A deficiency one parallelism is called *transitive* if it has an automorphism group, which is transitive on the spreads and fixes the deficiency spread. An infinite class of transitive deficiency one parallelisms of PG$(3, q)$ is provided by Johnson [19] for $q = p^r$ if p is odd, and further a group-theoretic characterization of the constructed parallelisms is presented by Johnson and Pomareda [24]. Properties of the automorphism groups and the spreads of transitive deficiency one parallelisms of PG$(3, q)$ are derived by Biliotti, Jha, and Johnson [7], and Diaz, Johnson, and Montinaro [12], who show that the deficiency spread must be regular, and the automorphism group should contain a normal subgroup of order q^2 (see also [20, chapter 38]). There are computer-aided constructions in PG$(3, 5)$ [44] which have these theoretically derived properties, but also show that there exist transitive deficiency one parallelisms which have the same spread structure as those of Johnson's infinite family [19], but do not belong to it.

Open problem 3.8. *Construct new infinite families of transitive deficiency one parallelisms of* PG$(3, q)$.

A t-spread in $\mathrm{PG}(n,q)$ is a set of disjoint t-dimensional subspaces, such that each point is in exactly one line. A t-parallelism of $\mathrm{PG}(n,q)$ is a partition of the set of t-dimensional subspaces to t-spreads. The only known examples of transitive t-parallelisms for $t > 1$ are 2-parallelisms in $PG(5,2)$ [39]. Johnson and Montinaro determine the structure of the automorphism group of a transitive t-parallelism of $PG(n,q)$ [23] and point out that transitive t-parallelisms in $PG(n,q)$ can only exist for $t = 1$, or for $t = 2$ and $(n,q) = (5,2)$ or $(n,q) = (5,3)$.

Open problem 3.9. *Establish if there exist or not transitive* 2*-parallelisms of* $\mathrm{PG}(5,3)$.

4. Final remarks. The study of parallelisms of $\mathrm{PG}(n,q)$ is well motivated by their relations to various mathematical problems in different areas. There are many interesting open problems concerning parallelisms. Both theoretical and computer-aided methods can be applied to solve them. The topic is an interesting challenge for young scientists who might decide to start work in it.

REFERENCES

[1] R. D. Baker. Partitioning the planes of $\mathrm{AG}_{2m}(2)$ into 2-designs. *Discrete Math.* **15**, no. 3 (1976), 205–211.

[2] J. Bamberg. There are no regular packings of $\mathrm{PG}(3,3)$ or $\mathrm{PG}(3,4)$. `https://symomega.wordpress.com/2012/12/01/`. Last accessed 24 Jan 2019

[3] Th. Beth, D. Jungnickel, H. Lenz. Design Theory. Cambridge, Cambridge University Press, 1993.

[4] A. Betten. The packings of $\mathrm{PG}(3,3)$. *Des. Codes Cryptogr.* **79**, no. 3 (2016), 583–595.

[5] A. Betten, S. Topalova, S. Zhelezova. Parallelisms of $\mathrm{PG}(3,4)$ invariant under cyclic groups of order 4. In: 8-th International Conference, CAI 2019 (Eds M. Ciric, M. Droste, Jean-Eric Pin), 88–99. Lecture Notes in Comput. Sci., vol. **11545**, Springer, Heidelberg, 2019.

[6] A. Beutelspacher. On parallelisms in finite projective spaces. *Geom. Dedicata* **3**, no. 1 (1974), 35–40.

[7] M.Biliotti, V. Jha, N. Johnson. Classification of transitive deficiency one partial parallelisms. *Bull. Belg. Math. Soc.* **12** (2005), 371–391.

[8] R. H. Bruck, R. C. Bose. The construction of translation planes from projective spaces. *Journal of Algebra*, **1** (1), (1964), 85–102.

[9] T. Caliński, S. Kageyama. On the analysis of experiments in affine resolvable designs. *J. Statist. Plann. Inference* **138**, no. 11, (2008), 3350–3356.

[10] R. H. F. Denniston. Some packings of projective spaces. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)* **52**, (1972), 36–40.

[11] R. H. F. Denniston. Cyclic packings of the projective space of order 8. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)* **54** (1973), 373–377.

[12] E. Diaz, N. Johnson, A. Montinaro. Transitive deficiency one partial parallelisms. *Adv. Appl. Discrete Math.* **1**, no. 1 (2008), 1–34.

[13] C. Ding, J. Yin. A construction of optimal constant composition codes. *Des. Codes Cryptogr.* **40**, no. 2 (2006), 157–165.

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

[15] T. Etzion, L. Storme. Galois geometries and Coding Theory. *Des. Codes Cryptogr.* **78**, no. 1 (2016), 311–350.

[16] T. Etzion, A. Vardy. Automorphisms of codes in the Grassmann scheme. arXiv:1210.5724 [math.CO] (October 2012).
[17] D. Heinlein, Th. Honold, M. Kiermaier, S. Kurz. Generalized vector space partitions. *Australas. J. Combin.* **73** (2019), 162–178.
[18] V. Jha, N. L. Johnson. Regular parallelisms from translation planes. *Discrete Math.* **59**, no. 1–2 (1986), 91–97.
[19] N. L. Johnson. Some new classes of finite parallelisms. *Note Mat.* **20**, no. 22 (2000/01), 77–88.
[20] N. L. Johnson. Combinatorics of spreads and parallelisms. Pure and Applied Mathematics (Boca Raton), vol. **295**. Boca Raton, FL, CRC Press, 2010.
[21] S. L. Johnson, S. R. Weller. Resolvable 2-designs for regular low density parity-check codes. *IEEE Trans. Comm.* **51**, no. 9 (2003), 1413–1419.
[22] N. L. Johnson, A. Montinaro. The doubly transitive t-parallelisms. *Results Math.* **52**, no. 1–2 (2008) 75–89.
[23] N. L. Johnson, A. Montinaro. The transitive t-parallelisms of a finite projective space. *Adv. Geom.* **12**, no. 3 (2012), 401–429.
[24] N. L. Johnson, R. Pomareda. Transitive partial parallelisms of deficiency one. *European J. Combin.* **23**, no. 8 (2002), 969–986.
[25] T. P. Kirkman. Query VI. *Lady's and Gentlemen's Diary* (1850), 48.
[26] R. Kötter, F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory* **54**, no. 8 (2008), 3579–3591.
[27] K. Kurosawa, S. Kageyama. New bound for affine resolvable designs and its application to authentication codes. In: Computing and Combinatorics (Xi'an, 1995) (Eds Du DZ., Li M), 292–302. Lecture Notes in Comput. Sci., vol. **959**. Berlin, Springer, 1995.
[28] G. Lunardon. On regular parallelisms in $\mathrm{PG}(3,q)$. *Discrete Math.* **51**, no. 3 (1984), 229–335.
[29] O. Olmez, A. Ramamoorthy. Fractional repetition codes with flexible repair from combinatorial designs. *IEEE Trans. Inform. Theory* **62**, no. 4 (2016), 1565–1591.
[30] T. Penttila, B. Williams. Regular packings of $\mathrm{PG}(3,q)$. *European J. Combin.* **19**, no. 6 (1998), 713–720.
[31] A. R. Prince. Parallelisms of $\mathrm{PG}(3,3)$ invariant under a collineation of order 5. In: Mostly finite geometries (Iowa City, IA, 1996) (Ed. Johnson N. L.), 383–390. Lecture Notes in Pure and Appl. Math., vol. **190**, New York, Marcel Dekker, 1997.
[32] A. R. Prince. Uniform parallelisms of $\mathrm{PG}(3,3)$. In: Geometry, combinatorial designs and related structures (Spetses, 1996) (Eds Hirschfeld J., Magliveras S., Resmini M.), 193–200. London Math. Soc. Lecture Note Ser., vol. **245**. Cambridge, Cambridge Univ. Press, 1997.
[33] A. R. Prince. The cyclic parallelisms of $\mathrm{PG}(3,5)$. *European J. Combin.* **19**, no. 5 (1998), 613–616.
[34] S. Ruj, J. Seberry, B. Roy. Key predistribution schemes using block designs in wireless sensor networks. 12-th IEEE International Conference on Computational Science and Engineering, 2009, 873–878, doi: 10.1109/CSE.2009.35.
[35] J. Sarmiento. Resolutions of $\mathrm{PG}(5,2)$ with point-cyclic automorphism group. *J. Combin. Des.* **8**, no. 1 (2000), 2–14.
[36] N. V. Semakov, V. A. Zinov'ev. Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs. *Probl. Peredachi Inform.* **4**, no. 2 (1968), 3–10 (in Russian); English translation in: *Problems Inform. Transmission* **4**, no. 2 (1968), 1–7 (1971).
[37] *D. R. Stinson.* Combinatorial Designs: Constructions and Analysis. New York, Springer-Verlag, 2004.
[38] D. R. Stinson, S. A. Vanstone. Orthogonal packings in $\mathrm{PG}(5,2)$,*Aequationes Math.* **31**, no. 2–3 (1986), 159–168.

[39] S. Topalova, S. Zhelezova. 2-spreads and transitive and orthogonal 2-parallelisms of PG(5, 2). *Graph. Combin.* **26**, no. 5 (2010), 727–735.
[40] S. Topalova, S. Zhelezova. On point-transitive and transitive deficiency one parallelisms of PG(3, 4). *Des. Codes Cryptogr.* **75**, no. 1 (2015), 9–19.
[41] S. Topalova, S. Zhelezova. New regular parallelisms of PG(3, 5). *J. Combin. Des.* **24**, no. 10 (2016), 473–482.
[42] S. Topalova, S. Zhelezova. Types of spreads and duality of the parallelisms of PG(3, 5) with automorphisms of order 13. *Des. Codes Cryptogr.* **87**, no. 2–3 (2019),495–507.
[43] S. Topalova, S. Zhelezova. Backtrack search for parallelisms of projective spaces. In: Combinatorial algorithms (Eds Flocchini P., Moura L.) 544–557. Lecture Notes in Comput. Sci., vol. **12757**. Cham, Springer, 2021.
[44] S. Topalova, S. Zhelezova. Parallelisms of PG(3, 5) with an automorphism group of order 25. In: Extended Abstracts EuroComb 2021 (Eds Nešetřil J., Perarnau G., Rué J., Serra O.), 668–674. Trends in Mathematics, vol. **14**. Cham, Springer, 2021.
[45] G. Zaicev, V. Zinoviev, N. Semakov. Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes. In: Proc. Sec. Intern. Symp. on Information Theory, (Armenia, USSR, 1971), Budapest, Academiai Kiado, (1973), 257–263.
[46] M. Walker. Spreads covered by derivable partial spreads. *J. Combin. Theory Ser. A* **38**, no. 2 (1985), 113–130.
[47] C. T. White. Two cyclic arrangement problems in finite projective geometry: Parallelisms and two-intersection set, Ph.D. Thesis, California Institute of Technology, 2002.
[48] S. Zhelezova. Cyclic parallelisms of PG(5, 2). *Mathematica Balkanica (N.S.)* **24**, no. 1–2, (2010), 141–146.

Svetlana Topalova
e-mail: svetlana@math.bas.bg
Stela Zhelezova
e-mail: stela@math.bas.bg
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 8
1113 Sofia, Bulgaria

ПАРАЛЕЛИЗМИ НА PG(n, q)

Светлана Топалова, Стела Железова

Нека PG(n, q) е n-мерното проективно пространство над крайното поле $GF(q)$. Множество от прави на PG(n, q) такива, че всяка точка се съдържа точно в една от тях, се нарича *спред*. *Паралелизъм* наричаме множество от спредове, за което е в сила, че всяка права на PG(n, q) се съдържа в точно един негов спред. Настоящата статия се спира на свойствата на паралелизмите на PG(n, q), на причините за интереса към тях, на резултатите, получени в тази област, и на някои отворени въпроси.