Contributions to Discrete Mathematics

Volume 15, Number 1, Pages 1–9
ISSN 1715-0868

AN ELEMENTARY, GEOMETRIC PROOF OF THE NONEXISTENCE OF A PROJECTIVE PLANE OF ORDER 6.

MARCIN DUMNICKI, JANUSZ GWOŹDZIEWICZ, AND JUSTYNA SZPOND

Abstract. We present a fairly elementary, self-contained proof of the nonexistence of a finite projective plane of order 6. Our approach is motivated by theory of binary codes but does not appeal to it directly.

1. Introduction

We begin with a definition of the protagonist of this note.

Definition 1.1 (Finite Projective Plane)**.** *A finite projective plane (FPP for short) is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ consisting of a finite set $\mathcal{P}$, whose elements are called points, a set $\mathcal{L} \subset 2^{\mathcal{P}}$ of subsets of $\mathcal{P}$, whose elements are called lines and a relation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$, called the incidence relation, subject to the following axioms:*

A1) *for a pair of distinct points $P, Q \in \mathcal{P}$ there is a unique line l such that $(P, l), (Q, l) \in \mathcal{I}$;*
A2) *for a pair of distinct lines $l, m \in \mathcal{L}$, there is a unique point P such that $(P, l), (P, m) \in \mathcal{I}$;*
A3) *there is a set of 4 points, no 3 of which are collinear.*

It is easy to check (see Lemma 2.1) that there exists a number s such that each line $l \in \mathcal{L}$ contains $s + 1$ points and there are $s + 1$ lines through every point $P \in \mathcal{P}$. This number s is called *the order of the FPP*.

The following question motivated considerable amount of research in combinatorics in recent decades.

Problem 1.2 (The Existence Problem)**.** *Determine all integers s such that there exists a FPP of order s.*

It is well-known that if $s = p^r$ is a power of a prime number p, then an FPP of order s exists. The standard construction of $\mathbb{P}^2(\mathbb{F})$, as a projectivization of the vector space $\mathbb{F}^3$, where $\mathbb{F}$ is a finite field, works in this case.

Received by the editors April 6, 2018, and in revised form November 19, 2018.
2000 *Mathematics Subject Classification.* MSC 05B25, MSC 51D20, and MSC 51E15.
Key words and phrases. finite projective plane, finite geometry, configurations of lines.
The research of the first and the last author was partially supported by National Science Centre, Poland, grant 2014/15/B/ST1/02197 and 2018/30/M/ST1/00148.

Remark. There are FPP's of order p^r, which are not constructed out of finite fields, see [5].

It is expected that there are no FPP's of order s different from a power of a prime. Important evidence towards this statement is provided by the following result due to Bruck and Ryser, see [2].

Theorem 1.3 (Bruck, Ryser [2])**.** *If $s \equiv 1$ or $2 \pmod 4$ and the square-free part of s contains at least one prime $p \equiv 3 \pmod 4$, then there does not exist a FPP of order s.*

Thus there are no FPPs of order

$$6, 14, 21, 22, 30, 33, 38, 42, 46, 54.$$

The first ten integers which are not powers of primes and are not covered by Theorem 1.3 are

$$10, 12, 15, 18, 20, 24, 26, 28, 34, 35.$$

The purpose of this note is to give a self-contained, relatively elementary proof of the following theorem.

Theorem 1.4. *There is no FPP of order* 6*.*

This result is not new. It has been anticipated by Euler in 1782 (see [4]). The first proof, using the concept of orthogonal latin squares, was given by Tarry in 1900 (see [7]). The result also follows from Theorem 1.3. In 1949 Bruck and Ryser proved the more general Theorem 1.4 using arithmetic properties of quadratic forms.. A graph-theoretic proof has been recently (2011) given by Burger, Kidd and van Vuuren [3]. Other proofs can be found in [1] and [6]. The reason for this note is to provide a streamlined proof, which starts from first principles and is self-contained.

2. Preliminaries

We begin by establishing the existence of an order of a finite projective plane.

Lemma 2.1. *Let $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a finite projective plane. Then there is a number s such that each line contains exactly $(s+1)$ points.*

Proof. We begin by the observation that for a point P not contained in a line l, the number of lines passing through P is equal to the number of points on l. Indeed, it follows from A1) that the number of lines through P is at least the number of points on l, whereas the opposite inequality follows from A2).

Let P, Q, R, S be points satisfying A3). Then it follows from the above observation that the number of points on each line QR, QS, and RS is equal to the number of lines through P. Then this holds for an arbitrary point T since T is not contained in one of these lines. But then the same holds for any line as not all points are collinear. □

Now we proceed to a general construction on sets. Let X be an arbitrary set. For any subsets A, $B \subset X$ we define the symmetric difference $A \oplus B = (A \cup B) \setminus (B \cap A)$. This operation is associative and commutative. Moreover, if X is a finite set, then $|A \oplus B| = |A| + |B| - 2|A \cap B|$. This gives a congruence $|A \oplus B| \equiv |A| + |B| \pmod 2$ which easily generalizes to

$$|A_1 \oplus \cdots \oplus A_n| \equiv |A_1| + \cdots + |A_m| \pmod 2\,. \tag{2.1}$$

Note that for arbitrary subsets $A, B, C, D \subset X$ we have the implication

$$A = B \oplus C \Longrightarrow A \cap D = (B \cap D) \oplus (C \cap D). \tag{2.2}$$

3. Proof of Theorem 1.4

Our proof is strongly motivated by binary code theory but does not directly appeal to this concept. We assume to the contrary that there exists an FPP $\mathbb{P} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ of order 6. Let $\mathcal{C}$ be a family of subsets of $\mathcal{P}$ which are of the form

$$l_1 \oplus \cdots \oplus l_m,$$

where l_i are lines in $\mathbb{P}$. Every set of this family will be called *a configuration.* A point P belongs to $l_1 \oplus \cdots \oplus l_m$ if and only if P belongs to the odd number l_i's.

We have the following parity Lemma.

Lemma 3.1. *Let $A = l_1 \oplus \cdots \oplus l_m$ be a configuration and $l \in \mathcal{L}$ a line. Then*

$$|A \cap l| \equiv |A| \pmod 2\,. \tag{3.1}$$

Proof. By (2.2) we have

$$A \cap l = (l_1 \cap l) \oplus \ldots \oplus (l_m \cap l).$$

Since $|m \cap l| \equiv |m| \pmod 2$ for any $m, l \in \mathcal{L}$, then claim follows from (2.1) and (2.2). □

Let A be a configuration. If l is a line and $B = A \oplus l$ then $A = B \oplus l$. The sets $A \cap l$, $B \cap l$ form a partition of l and $A \setminus (A \cap l) = B \setminus (B \cap l)$. This gives the equalities

$$|A \cap l| + |B \cap l| = 7, \tag{3.2}$$

$$|A| - |A \cap l| = |B| - |B \cap l|. \tag{3.3}$$

Given a configuration A of n points, denote by b_i the number of lines that intersect A at exactly i points. Simple counting yields the following equalities:

$$\sum_{i=0}^{7} b_i = 43, \tag{3.4}$$

$$\sum_{i=2}^{7} \binom{i}{2} b_i = \binom{n}{2}, \tag{3.5}$$

$$\sum_{i=0}^{7}(7-i)b_i = 7(43-n). \tag{3.6}$$

In (3.4) we count the total number of lines. In (3.5) we count the number of pairs $(\{P,Q\},l)$, where l is a line and $P,Q \in l \cap A$, $P \neq Q$. In (3.6) we count the number of pairs (P,l), where l is a line and $P \in l \setminus A$.

It follows from (3.1) that for any configuration A with n points: If n is even, then $b_1 = b_3 = b_5 = b_7 = 0$ and (3.4)–(3.6) becomes:

$$\begin{array}{ccccccccc} b_0 & + & b_2 & + & b_4 & + & b_6 & = & 43, \\ & & b_2 & + & 6b_4 & + & 15b_6 & = & \binom{n}{2}, \\ 7b_0 & + & 5b_2 & + & 3b_4 & + & b_6 & = & 7(43-n). \end{array} \tag{3.7}$$

If n is odd, then $b_0 = b_2 = b_4 = b_6 = 0$ and (3.4)–(3.6) becomes:

$$\begin{array}{ccccccccc} b_1 & + & b_3 & + & b_5 & + & b_7 & = & 43, \\ & & 3b_3 & + & 10b_5 & + & 21b_7 & = & \binom{n}{2}, \\ 6b_1 & + & 4b_3 & + & 2b_5 & & & = & 7(43-n). \end{array} \tag{3.8}$$

In the sequel we will work with configurations of n points for

$$n \in \{7, 8, 11, 12, 15, 20\}.$$

Then (3.7) resp. (3.8) have the following one parameter families of solutions:

$$(b_1, b_3, b_5, b_7) = (43-t, -3+3t, 3-3t, t) \quad \text{if} \quad n = 7, \tag{3.9}$$

$$(b_0, b_2, b_4, b_6) = (15-t, 28+3t, -3t, t) \quad \text{if} \quad n = 8, \tag{3.10}$$

$$(b_1, b_3, b_5, b_7) = (27-t, 15+3t, 1-3t, t) \quad \text{if} \quad n = 11, \tag{3.11}$$

$$(b_0, b_2, b_4, b_6) = (7-t, 30+3t, 6-3t, t) \quad \text{if} \quad n = 12, \tag{3.12}$$

$$(b_1, b_3, b_5, b_7) = (15-t, 25+3t, 3-3t, t) \quad \text{if} \quad n = 15, \tag{3.13}$$

$$(b_0, b_2, b_4, b_6) = (3-t, 10+3t, 30-3t, t) \quad \text{if} \quad n = 20. \tag{3.14}$$

3.1. **Properties of configurations in the plane of order 6.**

Property 3.2. *Every nonempty configuration has at least 7 points.*

Proof. Let A be a nonempty configuration. Assume first that $|A|$ is odd. If $A = \mathcal{P}$, then we are done, otherwise take any point P outside A and consider 7 lines passing through P. By (3.1) each of these lines intersects A. Hence $|A| \geq 7$. Now assume that $|A|$ is even. Take any point $P \in A$ and consider 7 lines passing through P. By (3.1) each of these lines passes through some point of A different from P. In this case $|A| \geq 8$. □

Property 3.3. *Every configuration with exactly 7 points is a line.*

Proof. Let A be a configuration such that $|A| = 7$. The only solution of (3.9) in the nonnegative integers is $(b_1, b_3, b_5, b_7) = (42, 0, 0, 1)$. In particular $b_7 = 1$, hence A contains some line l. It follows that $A = l$. □

Property 3.4. *There is no configuration with 8 points.*

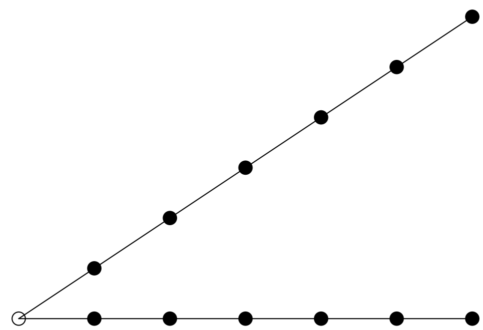

FIGURE 1. A configuration of 12 points

Proof. Assume that there exists a configuration A with 8 points. The only solution of (3.10) in the nonnegative integers is $(b_0, b_2, b_4, b_6) = (15, 28, 0, 0)$. Recall that $b_1 = b_3 = b_5 = b_7 = 0$. This means that every line that intersects A passes through exactly 2 points of A. In view of combinatorial Lemma 4.1 this is impossible. □

Property 3.5. *There is no configuration with* 11 *points.*

Proof. Assume that there exists a configuration A with 11 points. The only solution of (3.11) in the nonnegative integers is $(b_1, b_3, b_5, b_7) = (27, 15, 1, 0)$, hence there exists a line l such that $|A \cap l| = 5$. Then the configuration $A \oplus l$ has $11 - 5 + 2 = 8$ points which is impossible. □

Property 3.6. *Every configuration with* 12 *points is a symmetric difference* $l_1 \oplus l_2$ *of two distinct lines.*

Proof. Assume that $|A| = 12$. If there exists a line l such that $|A \cap l| = 4$ then by (3.3) the configuration $A \oplus l$ has 11 points which is impossible. Hence $b_4 = 0$. By (3.12) one gets $b_6 = 2$. Let k be a line passing through 6 points of A and let $B = A \oplus k$. Then the configuration B has $12 - 6 + 1 = 7$ points and by Property 3.3 B is a line. Thus $A = B \oplus k$ is a symmetric difference of two lines. □

Figure 1 indicates a configuration of 12 points.

Property 3.7. *Every configuration with* 15 *points is a symmetric difference* $l_1 \oplus l_2 \oplus l_3$ *of three distinct lines sharing no common point.*

Proof. Assume that $|A| = 15$. If there exists a line l such that $|A \cap l| = 7$ then by (3.3) the configuration $A \oplus l$ has $15 - 7 = 8$ points which is impossible. Hence $b_7 = 0$. By (3.13) one gets $(b_1, b_3, b_5, b_7) = (15, 25, 3, 0)$. In particular $b_5 \neq 0$. Let k be a line passing through 5 points of A and let $B = A \oplus k$. By (3.3) the configuration B has 12 points and by (3.2) $|B \cap k| = 2$. Thus $A = B \oplus k$ is a symmetric difference of three lines that form a triangle. □

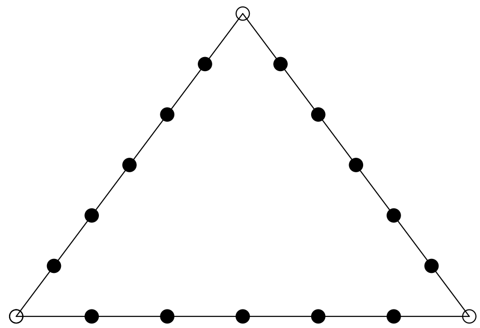

Figure 2. A configuration of 15 points

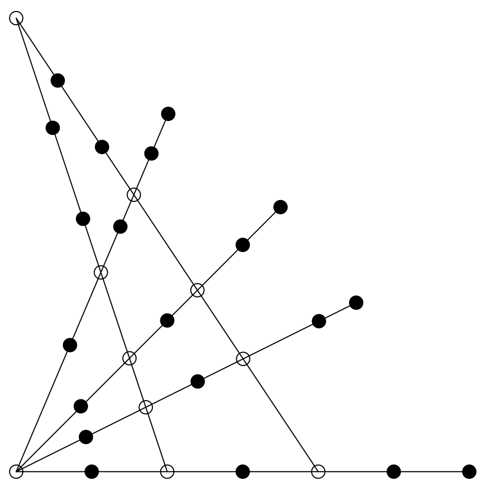

Figure 3. A configuration of 20 points

Figure 2 indicates a configuration of 15 points.

Now we turn our attention to configuration with 20 points. Such configurations exist, an example is indicated in Figure 3.

Property 3.8. *For every configuration of* 20 *points either* $b_0 = 0$ *or* $b_0 = 3$.

Proof. Assume that $|A| = 20$ and there exists a line l such that $|A \cap l| = 6$. Then $B = A \oplus l$ is a configuration of 15 points and $|B \cap l| = 1$. By Property 3.7, $B = l_1 \oplus l_2 \oplus l_3$, where l_1 l_2, l_3 form a triangle. Since $|B \cap l| = 1$, the line l passes through a vertex of this triangle. Without loss of generality we may assume that l passes through the intersection point of l_1 and l_2.

Then $|A \cap l| = |A \cap l_1| = |A \cap l_2| = 6$ which shows that $b_6 \geq 3$. On the other hand we get by (3.14) that $b_6 \leq 3$ this implies that for $|A| = 20$, either $b_6 = 0$ or $b_6 = 3$. By (3.14) $b_0 + b_6 = 3$, which completes the proof. □

Property 3.9. *There exists a configuration of* 20 *points with* $b_0 > 0$.

Proof. Take 4 lines l_1, l_2, l_3, l_4 that pass through a given point P and 2 lines l_5, l_6 that pass through a point $Q \notin (l_1 \cup l_2 \cup l_3 \cup l_4)$ and do not pass through P. Let $A = l_1 \oplus \cdots \oplus l_6$. Every intersection point of the lines l_1, $\ldots$, l_6 belongs to even number of these lines. Hence the intersection points do not belong to A. Let Z be the set of all intersection points $l_i \cap l_j$ for $1 \leq i < j \leq 6$. Every line l_i for $1 \leq i \leq 4$ has 3 points in Z and 4 remaining points and every line l_i for $5 \leq i \leq 6$ has 5 points in Z and 2 remaining points. Thus A has 20 points. It is clear that the line PQ does not intersect A, hence $b_0 > 0$. □

Theorem 3.10. *The projective plane of rank* 6 *does not exist.*

Proof. Suppose that the projective plane $\mathbb{P}$ of rank 6 exists. Let A be a configuration of 20 points with $b_0 > 0$ (by Property 3.9 such an A exists). By Property 3.8 there are 3 lines which do not intersect A. Denote these lines by k_1, k_2, k_3 and let $B = k_1 \oplus k_2 \oplus k_3$. If the lines k_1, k_2, k_3 form a triangle then $|B| = 15$, otherwise $|B| = 19$. Hence the configuration $C = A \oplus B$ has 35 or 39 points. The complementary configuration $C' = C \oplus \mathbb{P}$ has 8 or 4 points. This contradicts Properties 3.2 and 3.4 and completes the proof. □

4. A combinatorial result

Lemma 4.1. *A subset A of* 8 *points of the projective plane of rank* 6 *with the following property "Every line that has a nonempty intersection with A intersects A at exactly 2 points" does not exist.*

Proof. Suppose that $A = \{P_1, \ldots, P_8\}$ has this property. Take any point Q from the complement of A and consider the set of lines that pass through Q and have nonempty intersection with A. Since every such a line intersects A at 2 points this set consists of 4 lines. These lines induce a partition $W_Q = \{\{P_{n_1}, P_{n_2}\}, \{P_{n_3}, P_{n_4}\}, \{P_{n_5}, P_{n_6}\}, \{P_{n_7}, P_{n_8}\}\}$ of A. Now, let Q_1, Q_2 be two distinct points in the complement of A. Then $|W_{Q_1} \cap W_{Q_2}| \leq 1$ because two distinct lines intersect at exactly one point. Thus we obtain a family $\mathcal{W}$ of partitions of A into two-element sets W_Q satisfying the following property:

For every pairwise different elements n_1, n_2, n_3, n_4 of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ *there exists exactly one $W \in \mathcal{W}$ such that* $\{\{n_1, n_2\}, \{n_3, n_4\}\} \subset W$.

Note that in order to alleviate notation, we write i instead of P_i for $i = 1, \ldots, 8$. Without the loss of generality we may assume that

$$W_1 = \{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}\}$$

is a partition in $\mathcal{W}$. Let W_2 be the partition containing $\{\{1,2\},\{3,5\}\}$. Then $W_2 = \{\{1,2\},\{3,5\},\{4,6\}, \{7,8\}\}$, $W_2 = \{\{1,2\},\{3,5\},\{4,7\},\{6,8\}\}$, or $W_2 = \{\{1,2\},\{3,5\},\{4,8\},\{6,7\}\}$. The first possibility is excluded because in this case W_1 and W_2 have two pairs in common. Without loss of generality we may assume, switching the places of 7 and 8 if necessary, that

$$W_2 = \{\{1,2\},\{3,5\},\{4,7\},\{6,8\}\}.$$

Take the partition W_3 such that $\{\{1,2\},\{3,6\}\} \subset W_3$. Then $W_3 = \{\{1,2\}, \{3,6\},\{4,5\},\{7,8\}\}$, $W_3 = \{\{1,2\},\{3,6\},\{4,7\},\{5,8\}\}$, or $W_3 = \{\{1,2\}, \{3,6\},\{4,8\},\{5,7\}\}$.

In the first case $|W_3 \cap W_1| = 2$ and in the second case $|W_3 \cap W_2| = 2$. Hence

$$W_3 = \{\{1,2\},\{3,6\},\{4,8\},\{5,7\}\}.$$

Proceeding in this way and assuming $\{\{1,2\},\{3,7\}\} \subset W_4$, $\{\{1,2\},\{3,8\}\} \subset W_5$ we get

$$W_4 = \{\{1,2\},\{3,7\},\{4,6\},\{5,8\}\},$$
$$W_5 = \{\{1,2\},\{3,8\},\{4,5\},\{6,7\}\}.$$

Now, assume that $\{\{1,3\},\{2,4\}\} \subset W_6$. Then $W_6 = \{\{1,3\},\{2,4\},\{5,6\}, \{7,8\}\}$, $W_6 = \{1,3\},\{2,4\},\{5,7\},\{6,8\}\}$, or $W_6 = \{\{1,3\},\{2,4\},\{5,8\}, \{6,7\}\}$. The first case is impossible since W_6 and W_1 would have two common pairs. Assume that we are in the second case, i.e.,

$$W_6 = \{\{1,3\},\{2,4\},\{5,7\},\{6,8\}\}.$$

Then assuming that $\{\{1,3\},\{2,5\}\} \subset W_7$ and $\{\{1,3\},\{2,6\}\} \subset W_8$ we get

$$W_7 = \{\{1,3\},\{2,5\},\{4,6\},\{7,8\}\},$$
$$W_8 = \{\{1,3\},\{2,6\},\{4,7\},\{5,8\}\}.$$

Finally, take the partition W_9 such that $\{\{1,3\},\{2,8\}\} \subset W_9$. Then $W_9 = \{\{1,3\},\{2,8\},\{4,5\},\{6,7\}\}$, $W_9 = \{\{1,3\},\{2,8\},\{4,6\},\{5,7\}\}$, or $W_9 = \{\{1,3\},\{2,8\},\{4,7\},\{5,6\}\}$.

In the first case $|W_9 \cap W_5| = 2$, in the second case $|W_9 \cap W_7| = 2$, and in the third case $|W_9 \cap W_8| = 2$ hence we arrive at contradiction in each case.

The case $W_6 = \{\{1,3\},\{2,4\},\{5,8\},\{6,7\}\}$ is analogous and is left to the reader. □

References

1. A. Bichara, *An elementary proof of the nonexistence of a projective plane of order six*, Mitt. Math. Sem. Giessen (1989), no. 192, 89–93. MR 1010204
2. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian J. Math. **1** (1949), 88–93. MR 0027520
3. A. P. Burger, M. P. Kidd, and J. H. van Vuuren, *A graph-theoretic proof of the non-existence of self-orthogonal Latin squares of order 6*, Discrete Math. **311** (2011), no. 13, 1223–1228. MR 2793236
4. L. Euler, *Recherches sur une nouvelle espece de quarres magiques*, Verh. Zeeuwsch. Genootsch. Wetensch Vlissengen **9** (1782), 85–239.

5. F. W. Levi, *Finite Geometrical Systems*, University of Calcutta, Calcutta, 1942. MR 0006834
6. D. R. Stinson, *A short proof of the nonexistence of a pair of orthogonal Latin squares of order six*, J. Combin. Theory Ser. A **36** (1984), no. 3, 373–376. MR 744085
7. G. Tarry, *Le probléme des* 36 *officiers*, C.R. Assoc. Fr. Av. Sci. **1** (1900), 122–123, **2** (1901), 170–203.

Jagiellonian University, Institute of Mathematics, Łojasiewicza 6, PL-30-348 Kraków, Poland
E-mail address: Marcin.Dumnicki@im.uj.edu.pl

Department of Mathematics, Pedagogical University of Cracow, Podchorążych 2, PL-30-084 Kraków, Poland
E-mail address: gwozd63@gmail.com

Department of Mathematics, Pedagogical University of Cracow, Podchorążych 2, PL-30-084 Kraków, Poland
E-mail address: szpond@gmail.com