A Combinatorial Proof of Wilson's Theorem

Amitabha Tripathi
Department of Mathematics, Indian Institute of Technology, Hauz Khas, New Delhi - 110016, India
e-mail: atripath@maths.iitd.ac.in

Abstract

We give a combinatorial proof of *Wilson's Theorem:* p divides $\{(p-1)!+1\}$ if p is *prime*.

2000 Mathematics Subject Classification: 05A05, 11A07, 11B75

Keywords: Linear chain, permutation

Wilson's Theorem is one of the basic results in congruence arithmetic. The English mathematician, Edward Waring (1741–1793) stated it as a new and interesting property of primes in his book *Meditationes Algebraicae* published in 1770. The result was reported to him by his student, John Wilson, who appears to have guessed the result on the basis of numerical evidence. Neither Waring nor Wilson had a proof; in fact, Waring added, "Theorems of this kind will be very hard to prove, because of the absence of a notation to express prime numbers." Lagrange gave the first formal proof in 1771 and also observed that its converse holds. However, there seems to be some evidence that Leibniz was aware of the result almost a century earlier although he published nothing on the subject.

Wilson's Theorem is usually proved by drawing upon basic properties of linear congruences or by factoring polynomials over $\mathbb{Z}_p$ or by using the result that p has a primitive root. The first two methods are commonly

found in textbooks, for instance [2], and the third often appears as an exercise. The purpose of this note is to give a proof of Wilson's Theorem using combinatorial methods.

Definition 1. *A linear chain $a_1a_2\dots a_n$ of n positive integers $a_1, a_2, \dots, a_n$ is called an* n-linear chain, *or an $\mathcal{L}(n)$ chain, if the following three conditions hold:*

(a) $1 \le a_i \le n-1$ *for* $1 \le i \le n$;
(b) $\sum_{i=j}^{k} a_i \not\equiv 0 \pmod{n}$ *for* $1 \le j < k \le n-1$;
(c) $\sum_{i=1}^{n} a_i \equiv 0 \pmod{n}$.

Lemma 1. *Let $a_1a_2\dots a_n$ be an $\mathcal{L}(n)$ chain. Then $a_i, a_i + a_{i+1}, \dots, a_i + a_{i+1} + \cdots + a_n + a_1 + a_2 + \cdots + a_{i-1}$ is a complete system of residues modulo n for each i, $1 \le i \le n$.*

Proof. If any two numbers in the n-set were congruent modulo n, condition (b) of the definition would be violated. Thus, no two members of the n element set are congruent modulo n, and so the set represents a complete system of residues modulo n. □

Lemma 2. *There are $(n-1)!\,\mathcal{L}(n)$ chains.*

Proof. Let $a_1a_2\dots a_n$ be an $\mathcal{L}(n)$ chain. There are $n-1$ choices for a_1 by condition (a), and then $n-2$ choices for a_2 by condition (b). Inductively, a_k can be chosen in $n-k$ ways given that $a_1, a_2, \dots, a_{k-1}$ have already been chosen. This gives a total of $(n-1)!$ ways of selecting the linear chain. □

To each permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, so that $\pi(i) = a_i$ for $1 \le i \le n$, we associate the chain

$$\mathcal{D}(\pi) = d_1d_2\dots d_n,$$

where

$$d_i = \begin{cases} a_{i+1} - a_i \pmod{n} & \text{if } 1 \le i \le n-1; \\ a_1 - a_n \pmod{n} & \text{if } i = n. \end{cases}$$

It is easy to verify that $\mathcal{D}(\pi)$ is indeed an $\mathcal{L}(n)$ chain.

Conversely, given an $\mathcal{L}(n)$ chain $a_1a_2\dots a_n$, the permutation

$$\pi_i = (i \quad i + a_1 \quad i + a_1 + a_2 \quad \dots \quad i + a_1 + a_2 + \cdots + a_{n-1}),$$

where each entry $i + a_1 + a_2 + \cdots + a_k$ is reduced modulo n for $1 \leq i, k \leq n$ is such that $\mathcal{D}(\pi_i) = a_1 a_2 \ldots a_n$. Here π_i maps each entry within brackets to the succeeding entry, the permutations $\pi_1, \pi_2, \ldots, \pi_n$ are distinct and there can be no other permutation corresponding to the given $\mathcal{L}(n)$ chain.

Thus, from a given permutation we can construct a *unique* $\mathcal{L}(n)$ chain while a given $\mathcal{L}(n)$ chain yields n distinct permutations corresponding to this chain. Since there are $n!$ permutations, we have $(n-1)!$ $\mathcal{L}(n)$ chains. Therefore, by Lemma 2, all the $\mathcal{L}(n)$ chains may be obtained in the above manner from the permutations.

Definition 2. *Two permutations* π_1, π_2 *of* $\{1, 2, \ldots, n\}$ *are* congruent *provided* $\mathcal{D}(\pi_1) = \mathcal{D}(\pi_2)$.

Theorem 1. (Wilson's Theorem)

If p *is a* prime, *then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. If we arrange the $\mathcal{L}(n)$ chain $a_1 a_2 \ldots a_n$ in a circle, the n linear sequences starting with a_i for $1 \leq i \leq n$ determine the same circular sequence. However, the n linear sequences corresponding to a circular sequence need not all be distinct. If, for $d|n$, the sequence $a_1 a_2 \ldots a_n$ consists of n/d repetitions of the block $a_1 a_2 \ldots a_d$, the linear sequences repeat after the first d. To each circular sequence of length n we may associate a *least* positive integer d such that the circular sequence consists of n/d repetitions of a sequence of length d. Moreover, each circular sequence of length d and period d may be repeated n/d times to give a circular sequence of length n and period d provided $d|n$.

If $\mathcal{N}(d)$ denotes the number of circular sequences of length and period d, then $d\mathcal{N}(d)$ is the number of linear sequences of length n corresponding to them. It follows that

$$\sum_{d|n} d\mathcal{N}(d) = (n-1)!.$$

Now, $\mathcal{N}(1)$ counts the number of circular sequences of length and period 1, and this equals $n-1$, one for each nonzero value. When $n = p$ is a *prime*, the displayed equation reduces to $(p-1)! \equiv \mathcal{N}(1) \equiv -1 \pmod{p}$, and that completes the proof. □

The converse of Wilson's Theorem is also true: If $(n-1)! \equiv -1 \pmod{n}$ for $n > 1$, then n must be prime. Indeed, if $n > 1$ is composite, n always

has two distinct positive factors a, b, each less than n. Thus $(n-1)! \equiv 0 \pmod{n}$ whenever n is composite. Together with Wilson's Theorem, it gives a primality test for $n > 1$, albeit a computationally infeasible one.

Acknowledgement. The author wishes to thank the referee for making several suggestions towards the improvement of this article.

References

[1] David M. Burton. *Elementary Number Theory.* Wm. C. Brown Publishers, Third edition, 1994.

[2] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, Fourth edition, 1959.

ON THE EMBEDDING OF COMPLEMENTS OF SOME HYPERBOLIC PLANES

İ. GÜNALTILI , P. ANAPA and S. OLGUN
Osmangazi University
Departmant of Mathematics
26480 Eskişehir-Türkiye
E-mail : igunalti@ogu.edu.tr, panapa@ogu.edu.tr

Abstract

In this paper, we studied that a linear space, which is the complement of a linear space having points are not on a trilateral or a quadrilateral in a projective subplane of order m, is embeddable in a unique way in a projective plane of order n. In addition, we showed that this linear space is the complement of certain regular hyperbolic plane in the sense of Graves [5] with respect to a finite projective plane.

AMS Subject Classification : 05B25 , 51E20 , 51A45.
Keywords : Linear spaces , projective planes, hyperbolic planes.

1 Introduction

The complementation problem with respect to a projective plane is the following: Remove a certain configuration of points and lines from the plane, determine the parameters of the resulting space. Complementation problems have been considered by various authors ([1],[2],[3],[4],[11],[12],[13],[18]). In 1970, Dickey solved the problem for the case where the configuration removed was a unital [20] . (The one exceptional case here was completed by de Witte in 1977 [3]). Totten in 1976 considered the complement of two lines [2]. In 1987, L.M. Batten characterized linear spaces which are the complements of affine or projective subplanes of finite projective planes and showed that these spaces can be embeddable in a unique way in a projective plane of order n [4]. A generalization of Batten's Theorem [4] was given by Günaltılı and Olgun [13].

After then, the problem of embedding the " complements " of various configuration in projective planes has arised and this problem has been studied by various authors ([1],[2],[3],[4],[11],[12]).

In this paper, we showed that a linear space, which is the complement of a linear space having points are not on a trilateral or a quadrilateral in a projective subplane of order m, is embeddable in a unique way in a projective plane of order n. In addition, we determined that this linear space is the complement of certain regular hyperbolic plane in the sense of Graves [5] with respect to a finite projective plane.

Now, we give some definitions required.

Definition 1.1 : Let $\mathcal{P}$ be a set of points and $\mathcal{L}$ be a subset of the power set of $\mathcal{P}$. Then $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ is called a linear space if :

L1. Any two points belong to a unique line.

L2. Every line contains at least two points.

While in talking about finite linear spaces we shall use a rather easy-going terminology borrowed from classical geometry; for example, we shall use words such as "collinear," "concurrent," "meeting," "joining," and expressions such as " a line (passing) through a point" or "a point (lying) on a line".

If $v = |\mathcal{P}|$ and $b = |\mathcal{L}|$ are finite then $\mathcal{S}$ is called finite. The total number of lines through P is denoted by $b(P)$, and the total number of points on l is denoted by $v(l)$. Thus, if $b(P) = k$ and $v(l) = k$ then P is called a $k-$point and l is called a $k-$line. Furthermore, the total number of $k-$lines is denoted by b_k and the parameters k_m, k_M, r_m and r_M are defined as stated below:

$$k_m = \min \{v(l) \,|\, l \in \mathcal{L}\}$$
$$k_M = \max \{v(l) \,|\, l \in \mathcal{L}\}$$
$$r_m = \min \{b(P) \,|\, P \in \mathcal{P}\} \text{ and}$$
$$r_M = \max \{b(P) \,|\, P \in \mathcal{P}\}$$

If every point of $\mathcal{S}$ lies on exactly t lines of $\mathcal{S}$ then $\mathcal{S}$ is called $t-$regular. ($t \geq 1, t \in \mathbb{Z}$).

The order of a non-trivial finite linear space is defined as one less than the highest degree of both points and lines.

A finite projective plane of order $n \geq 2$ is a finite linear space with $n^2 + n + 1$ points in which $v(l) = b(P) = n + 1$ for every line l and every point P.

Definition 1.2 : A linear space $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ is said to be embeddable in a linear space $\mathcal{S}' = (\mathcal{P}', \mathcal{L}')$ if $\mathcal{S}'$ can be obtained from $\mathcal{S}$ by addition of some points called as ideal points and some lines called as ideal lines.

Definition 1.3 : A finite $(m+1)-$regular hyperbolic plane $(\mathcal{P}, \mathcal{L})$, in the sense of Graves, is a non-trivial $(m+1)-$regular linear space such that :

H1 : There are four points, no three of which are collinear.

H2 : If P is a point not on a line l, then there exist at least two lines , not meeting l and through P .

H3 : If a subset $\mathcal{P}'$ of the points of $\mathcal{P}$ contains three non-collinear points and contains all points on the lines through pairs of distinct points of P', then the subset P' contains all points of P.

Examples of hyperbolic planes have been constructed by Graves [5], Sandler [6], Crowe [15],[16],[17] and Kaya-Olgun [8].

Proposition 1.1 : (Bumcrot, 10) Any finite linear space satisfying the following conditions:

1. $r_m \geq k_m + 2$
2. $k_m(k_m - 1) \geq r_M$

is a hyperbolic plane in the sense of Graves [5].

2 MAIN RESULTS

Proposition 2.1 : Any $(m+1)-$regular linear space satisfying the following conditions for every $k \in \{3,4\}$ is a hyperbolic plane in the sense of Graves [5] (this hyperbolic plane is called as a hyperbolic plane of $(k,m)-$type) :

(i) $b = m^2 + m + 1 - k$, $v = m^2 + 1 + \binom{k}{2} - k - (k-1)m$ and

(ii) $b_i \geq 1$, for every $i \in \{m-1, m-2, m+1-k\}$.

Proof : Let $\mathcal{S}$ be a linear space satisfying the conditions (i) and (ii). It is clear that $r_m \geq k_M + 2$ and $k_m(k_m - 1) = (m+1-k)(m-k) \geq m+1$, since $k \in \{3,4\}$, $k_m = m+1-k$, $k_M = m-1$ and $r_m = r_M = m+1$. By the Proposition 1.1 , $\mathcal{S}$ is a hyperbolic plane which is called $(k,m)-$type.

Examples of hyperbolic planes of $(k,m)-$type are obtained by removing all points of k lines such that any three of which are not concurrent for $k \in \{3,4\}$ from projective planes of order m. (See [6],[8],[9]).

Proposition 2.2 : Let $\mathcal{S}$ be hyperbolic plane of $(3,m)-$type. If $b_{m-1} = 3(m-1)$ and $m \geq 7$ then $\mathcal{S}$ is a real complement of a triangle in a projective plane of order m.

Proof : By the Proposition 2.1, $\mathcal{S}$ is $(m+1)-$regular linear space with $(m-1)^2$ points, $(m^2 + m - 2)$ lines and every line has degree $m-2$ or

$m-1$. Thus, $\mathcal{S}$ is a real complement of a triangle in a projective plane of order m, $m \geq 7$ in according to Raltson ([11]).

Proposition 2.3 : Let $\mathcal{S}$ be a hyperbolic plane of $(4,m)$−type. If $b_{m-1} \geq 3$ and $m > 23$ then $\mathcal{S}$ is a real complement of a quadrilateral in a projective plane of order m.

Proof : Due to the Proposition 2.1, $\mathcal{S}$ is $(m+1)$−regular linear space with (m^2-3m+3) points, (m^2+m-3) lines and every line has degree $m-1, m-2$ or $m-3$. Thus $\mathcal{S}$ is a real complement of a quadrilateral in projective plane of order m in according to Montakhab [12].

Theorem 2.1 : Let $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ be an $(n+1)$−regular linear space such that :

(i) $b = n^2+n+1$, $v = n^2+n-m^2+2m$, $2 \leq m < n$

(ii) $b_{n+2-m} = 3(m-1)$

(iii) every line has $n+1, n, n+2-m, n+3-m$ points.

If m lines of degree $n+2-m$ are not mutually parallel, then $\mathcal{S}$ is embeddable in a unique way in a projective plane of order n and it is the complement of a hyperbolic plane of $(3,m)$−type.

Proof :

Let P_{ij} be the set of points of $\mathcal{S}$ such that there are i lines of degree $n+2-m$, j lines of degree $n+3-m$, k lines of degree n and h lines of degree $n+1$ through every point of it. Then;

$$(n+1-m)i+(n+2-m)j+(n-1)k+nh = v-1$$
$$i+j+k+h = n+1$$
$$\sum_{i,j}|P_{ij}| = v, \qquad \sum_{t} b_t = b, \qquad t \in \{n+1, n, n+2-m, n+3-m\}$$

Also, by simple counting methods,

$$k = (m-1)^2 - i(m-1) + j(m-2),$$
$$h = n+1-(m-1)^2 + i(m-2) + j(m-3),$$
$$\sum_{i,j}|P_{ij}|\, i = 3(n+2-m)(m-1),$$
$$\sum_{i,j}|P_{ij}|\, j = (n+3-m)b_{n+3-m}$$
$$\sum_{i,j}|P_{ij}|\, k = nb_n \text{ and}$$
$$\sum_{i,j}|P_{ij}|\, h = (n+1)b_{n+1}.$$

Thus,

$$b_n = (m-1)^2(n-m)$$
$$b_{n+1} = n^2 - n(m^2-2m) + (m^2-5m-1)$$
$$b_{n+3-m} = (m-1)^2 \text{ and}$$
$$b_{n+2-m} = 3(m-1).$$

It is easily shown that there is an n–line misses a given line of degree $n+2-m$ by using all of the assumptions of theorem.

Let l be an n–line . The number of lines not meeting l is n, since S is $(n+1)$ regular linear space with n^2+n+1 lines. Therefore, every n–line induces a parallel class of $n+1$ lines none of which is an $(n+1)$–line.

Let c and d be the numbers of $(n+2-m)$–line and $(n+3-m)$–line in a fixed class, respectively. Then

$$c(n+2-m) + d.(n+3-m) + (n+1-c-d)n = n^2+n-m^2+2m$$

implies that $d = m+1-c+\dfrac{c-3}{m-3}$.

Since $c < m$, by hypothesis $c = 3$, $d = m-2$. Thus, the number of n–lines in a parallel class is $n-m$. And the number of different parallel classes is $(m-1)^2$, since $b_n = (m-1)^2(n-m)$.

Consider the structure $\mathcal{S}^* = (\mathcal{P}^*, \mathcal{L}^*)$ where $\mathcal{P}^*$ is $\mathcal{P}$ along with the parallel classes and $\mathcal{L}^*$ consisting of the lines of $\mathcal{L}$ extended by those parallel classes to which they belong. We shall prove that $\mathcal{S}^*$ is a linear space. It is clear that two old points (points of $\mathcal{P}$) or an old and a new point are on a unique line of $\mathcal{L}^*$, since $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ is a linear space.

Let X and Y be two new different points. We must show that they determine a unique line of $\mathcal{L}^*$.Let l_X and l_Y be n-lines which determine the parallel classes corresponding to X and Y , respectively . If l_X and l_Y do not meet, then $X = Y$ which is a contradiction. So l_X and l_Y meet. Each point of l_Y is on a unique line of the parallel class determined by l_X. Thus, l_Y does not meet precisely one line of the parallel class determined by l_X. This leaves precisely one line parallel to both l_X and l_Y. Thus $\mathcal{S}^*$ is a linear space with n^2+n+1 points and n^2+n+1 lines. $\mathcal{S}^*$ is a projective plane of order n, by [18].

Consider the complement of $\mathcal{S}$ in $\mathcal{S}^*$. The lines of $\mathcal{S}^* \setminus \mathcal{S}$ are sets of $(m-1)$ or $(m-2)$ points, the extensions of the $(n+2-m)$–lines or $(n+3-m)$–lines of $\mathcal{S}$, respectively. It is clear that $\mathcal{S}^* \setminus \mathcal{S}$ is a linear space and there is at least one point not on a given line in $\mathcal{S}^* \setminus \mathcal{S}$. It is known that there are exactly three lines of degree $m-1$ and $(m-2)$ lines of degree

$m-2$ through any new point added to $\mathcal{S}$ (any point of $\mathcal{S}^* \setminus \mathcal{S}$). Thus $\mathcal{S}^* \setminus \mathcal{S}$ is a $(m+1)$−regular linear space with $(m-1)^2$ points and m^2+m-2 lines such that every line has degree $m-2$ or $m-1$. Therefore; $\mathcal{S}^* \setminus \mathcal{S}$ is a $(m+1)$−regular hyperbolic plane of $(3,m)$−type, by the Proposition 2.1.

Theorem 2.2 : Let $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ be an $(n+1)$−regular linear space, with satisfying the following conditions :

(i) $b = n^2+n+1$, $v = n^2+n-m^2+3m-2$, $\quad 2 \leq m < n$,

(ii) $b_{n+2-m} = 3$ and $b_{n+3-m} = 6(m-2)$

(iii) every line has $n+1, n, n+2-m, n+3-m, n+4-m$ points.

If m lines of degree $(n+3-m)$ are not mutually parallel, $\mathcal{S}$ is embeddable in a unique way in a projective plane of order n and is complement of a hyperbolic plane of $(4,m)$−type.

Proof :

Let P_{ijk} be the set of points such that there are exactly i lines of degree $n+2-m$, j lines of degree $n+3-m$, k lines of degreen $+4-m$, h lines of degree n and w lines of degree $n+1$ through every point P of it. Then;

$$(n+1-m)i+(n+2-m)j+(n+3-m)k+(n-1)h+nw = v-1,$$
$$i+j+k+h+w = n+1,$$
$$\sum_{i,j,k} |P_{ijk}| = v, \quad \sum_t b_t = b, \quad t \in \{n+1, n, n+2-m, n+3-m, n+4-m\}.$$

Also, by simple counting methods,

$$h = (m^2-3m+3) - i(m-1) - j(m-2) - k(m-3),$$
$$w = n+1-(m^2-3m+3) + i(m-1) + j(m-2) + k(m-3),$$
$$\sum_{i,j,k} |P_{ijk}|\, i = 3(n+2-m),$$
$$\sum_{i,j,k} |P_{ijk}|\, j = 6(m-2)(n+3-m),$$
$$\sum_{i,j,k} |P_{ijk}|\, k = (n+4-m)b_{n+4-m},$$
$$\sum_{i,j,k} |P_{ijk}|\, h = nb_n \text{ and}$$
$$\sum_{i,j,k} |P_{ijk}|\, w = (n+1)b_{n+1}.$$

and the following results are obtained.

$$b_n = (m^2 - 3m + 3)(n - m),$$
$$b_{n+1} = n^2 - (m-2)(m-1)n + m(m^2 - 4m + 2) + 4,$$
$$b_{n+2-m} = 3,$$
$$b_{n+3-m} = 6(m-2),$$
$$b_{n+4-m} = (m-3)(m-2).$$

It is easily shown that there is an $n-$line misses a given line of degree $n+2-m$ by using all of the assumptions of theorem.

Let l be an $n-$line and $\pi(l)$ be a parallel class corresponding to l. $\pi(l)$ contains at most three $(n+2-m)-$lines, since the total number of $(n+2-m)-$lines of S is exactly three. Thus, there are four cases which are needed to examine for $\pi(l)$.

Case 1: $\pi(l)$ contains none of $(n+2-m)-$lines. Let c and d be the number of $(n+3-m)-$lines and $(n+4-m)-$lines, respectively, in $\pi(l)$.

$$c(n+3-m) + d(n+4-m) + (n+1-c-d)n = n^2 + n - m^2 + 3m - 2$$

implies that $d = m + 1 - c - \dfrac{c-6}{m-4}$.

Since $c < m$, by hypothesis, $c = 6$ and $d = m - 5$. Thus, the number of $n-$lines, in $\pi(l)$, is $n - m$.

Case 2: $\pi(l)$ contains exactly one $(n+2-m)-$line. Let c and d be the number of $(n+3-m)-$lines and $(n+4-m)-$lines, respectively, in $\pi(l)$.

$$(n+2-m)+c(n+3-m)+d(n+4-m)+(n-c-d)n = n^2+n-m^2+3m-2$$

implies that $d = m - c - \dfrac{c-4}{m-4}$.

Since $c < m$, by hypothesis $c = 4$ and $d = m - 4$. Thus, the number of $n-$lines in $\pi(l)$ is $n - m$.

Case 3: $\pi(l)$ contains exactly two $(n+2-m)-$lines. Let c and d be the number of $(n+3-m)-$line and $(n+4-m)-$line, respectively, in π.

$$2(n+2-m)+c(n+3-m)+d(n+4-m)+(n+1-c-d)n = n^2+n-m^2+3m-2$$

implies that $d = m - 1 - c - \dfrac{c-2}{m-4}$.

Since $c < m$, by hypothesis $c = 2$ and $d = m - 3$. Thus, the number of $n-$lines in $\pi(l)$ is $n - m$.

Case 4: $\pi(l)$ contains exactly three $(n+2-m)-$lines. Let c and d be the number of $(n+3-m)-$line and $(n+4-m)-$line, respectively, in $\pi(l)$.

$3(n+2-m)+c(n+3-m)+d(n+4-m)+(n-2-c-d)n = n^2+n-m^2+3m-2$

implies that $d = m-2-\dfrac{c(m-3)}{(m-4)}$. $d, m, c \in \mathbb{Z}^+$ require both $(m-3, m-4) = 1$ and $(m-4) \mid c$. Thus, there is $t \geq 0$, $t \in \mathbb{Z}$ such that $c = t(m-4)$. In this case

$$0 \leq d = (m-2) - t(m-3) \qquad ((1))$$

From (1), $t = 0$ or $t = 1$.

If $t = 1$, then it is easily calculated that the number of $(n+3-m)$–lines and $(n+4-m)$–lines in $\pi(l)$ are 1 and $m-4$, respectively. Thus the total number of n–lines in $\pi(l)$ is $n+1-m$.

Since the total number of $(n+2-m)$–lines of S is exactly three, parallel classes of S which are different from $\pi(l)$ don't contain $(n+2-m)$–lines. Let a be the total number of parallel classes of S. By the case 1, it is clear that S contains exactly one parallel class which has $n+1-m$ (n)–lines and $a-1$ parallel classes which have $n-m$ (n)–lines. Thus, the following equality is valid.

$$(n+1-m)+(a-1)(n-m) = b_n = (m^2-3m+3)(n-m) \qquad ((2))$$

From (2),

$$a = (m^2-3m+3) - \frac{1}{n-m}.$$

Since $n > m$, $a \notin \mathbb{Z}$. This contradicts $a \in \mathbb{Z}$. Thus, $t = 0$ and it is easily shown that $\pi(l)$ contains exactly $n-m$ (n)–lines.

Consequently, the number of n–lines in any parallel class is $(n-m)$. Therefore; the number of different parallel classes of S is m^2-3m+3, since $b_n = (m^2-3m+3)(n-m)$.

Consider the structure $\mathcal{S}^* = (\mathcal{P}^*, \mathcal{L}^*)$ defined above. It is easily shown that $\mathcal{S}^*$ is a projective plane of order n, by the similar technique in the proof of Theorem 2.1.. Consider the complement of S in $\mathcal{S}^*$. The lines of $\mathcal{S}^* \setminus \mathcal{S}$ are sets of $\{m-1\}, \{m-2\}$ or $\{m-3\}$ points, which are extensions of the $(n+2-m)$–lines, $(n+3-m)$–lines and $(n+4-m)$–lines of $\mathcal{S}$, respectively. It is clear that $\mathcal{S}^* \setminus \mathcal{S}$ is a linear space and there is at least one point not on a given line in $\mathcal{S}^* \setminus \mathcal{S}$. It is known that there are at most two $(m-1)$–lines on any new point (any point of $\mathcal{S}^* \setminus \mathcal{S}$). If there are two $(m-1)$–lines on any new point, this point of $\mathcal{S}^* \setminus \mathcal{S}$ is exactly on

two lines of degree $m-2$ and $m-3$ lines of degree $(m-3)$. If there is one $(m-1)$–line on any new point; this point of $\mathcal{S}^* \setminus \mathcal{S}$ is exactly on four lines of degree $m-2$ and $m-4$ lines of degree $(m-3)$. If there is not any $(m-1)$–lines on a new point, this point of $\mathcal{S}^* \setminus \mathcal{S}$ is exactly on six lines of size $m-2$ and $m-5$ lines of size $(m-3)$. Thus $\mathcal{S}^* \setminus \mathcal{S}$ is a $(m+1)$–regular linear space with m^2-3m+3 points and m^2+m-3 lines in which a line is degree of $m-1, m-2$ or $m-3$. Therefore, $\mathcal{S}^* \setminus \mathcal{S}$ is a hyperbolic plane of $(4,m)$-type , by the Proposition 2.1.

References

[1] Bose R. C and Shrikhande S. S .; Embedding the complement of an oval in a projective plane of even order, Discrete Math. 6. (1973), 305-312

[2] Totten J.; Embedding the complement of two lines in a finite projective plane, J. Austral. Math. Soc. (A) 22 (1976), 27-34

[3] Witte P.; The exceptional case in a theorem of Bose and Shrikhande, J. Austral. Math. Soc. (A) 24 (1977), 64-78

[4] Batten L. M.; Embedding pseudo-complements in finite projective planes, Ars Combinatoria 24 (1987), pp. 129-132

[5] Graves, L.M.; A finite Bolyai-Lobachevsky plane, Amer.Math.Monthly 69 (1962), 130-132

[6] Sandler, R.; Finite homogeneous Bolyai-Lobachevsky planes, Amer. Math. Monthly 70 (1963),853-854

[7] Batten, L.M and Beutelspacher A.;The theory of finite linear space, Cambridge University Press, New-York-Melbourne, (1993)

[8] Kaya,R. and Olgun, Ş.;Construction of some hyperbolic planes using Baer subplanes, Combinatorics'88. Verlang: Mediterranean Press, 105-112

[9] Kaya, R. and Özcan, E.; On the construction of Bolyai-Lobachevsky planes from projective planes, Rendiconti del Seminario Matematica di Brescia 7 (1984), 427-434.

[10] Bumcrot, R.J.; Finite hyperbolic spaces, Atti Convegno Geom. Comb e sue Appl. Perugia, 113-130, (1971).

[11] Ralston, T.;On the embeddability of the complement of a complete triangle in a finite projective plane. Ars Combinatoria 11(1981) 271-274

[12] Montakhab, M.S., Embedding of finite pseudo-complement of quadrilaterals, Journal of Statistical Planning on Inference 13 (1986) 103-110

[13] Günaltılı I and Olgun Ş.; On the embedding of some linear spaces in finite projective planes, J.geom. 68(2000) 96-99

[14] Özcan E, Olgun Ş, Kaya R.; On the line classes in some finite hyperbolic planes, Commun.Fac.Sci.Univ.Ank.Series A,V38, pp 7-13 (1989)

[15] Crowe D.W.;The trigonometry of GF(2^{2n}), and finite hyperbolic planes, Mathematika 11, 83-88, 1964

[16] Crowe D.W.; The construction of finite regular hyperbolic planes from inversive planes of even order, Colloq.Math.13, 247-250, (1965)

[17] Crowe D.W.; Projective and inversive models for finite hyperbolic planes, Mich.Math.J.13, 251-255, (1966)

[18] De Bruijn, N.G. and Erdos P.; On a combinatorial problem, Nederl. Akad. Wetensch. proc. Sect. Sci. 51 (1948), 1277-1279, and Indag. Math. 10(1948), 421-423

[19] Demwoski, H.P. ; Finite geometries, Springer-Verlag, (1968).

[20] Dickey, L. J. : Embedding the complement of a unital in a projective plane, Atti del convegno di Geometria Combinatoria e sue Applicazioni, Perugia, 1971, p. 199-203.