

ON THE PARAMETERS OF TWO-INTERSECTION SETS IN $PG(3, q)$ STEFANO INNAMORATI ^{a*} AND FULVIO ZUANNI ^a

ABSTRACT. In this paper we study the behaviour of the admissible parameters of a two-intersection set in the finite three-dimensional projective space of order $q = p^h$ a prime power. We show that all these parameters are congruent to the same integer modulo a power of p . Furthermore, when the difference of the intersection numbers is greater than the order of the underlying geometry, such integer is either 0 or 1 modulo a power of p . A useful connection between the intersection numbers of lines and planes is provided. We also improve some known bounds for the cardinality of the set. Finally, as a by-product, we prove two recent conjectures due to Durante, Napolitano and Olanda.

1. Introduction and motivation

Let us denote by $PG(3, q)$ the three-dimensional projective space over the finite field $GF(q)$ with $q = p^h$ a prime power. A k -set of $PG(3, q)$ is a set of k points of $PG(3, q)$. We say that K is a set of type $(m, n)_2$, with $m < n$, if each plane of $PG(3, q)$ meets K in exactly m or n points; the numbers m and n are the intersection number of K with respect to the planes of $PG(3, q)$. For further details on this topic see Thas (1973), Tallini Scafati (1976), Hirschfeld (1985), De Finis (1986), De Resmini (1987), Tallini (1987), and De Resmini (1988). Moreover, Blokhuis and Lavrauw (2000), Hamilton and Penttila (2001), Blokhuis and Lavrauw (2002), and Cossidente and Van Maldeghem (2007) gave some constructions of two-intersection sets in projective spaces. One of the fundamental aspects of finite geometry is understanding the behavior of the intersection numbers of a certain set with respect to subspaces of a r -dimensional projective space. This area of research uses the simplest ingredients of finite geometry, but paradoxically it is one of the most difficult areas to make progress in. Although ingredients are simple, it is quite difficult to do anything with them. Recently, on this topic, the authors showed how to recognize specific configurations only by intersection numbers (see Innamorati and Zuanni 2015, 2017). Moreover, Jungnickel (2011) reached a characterization of classical quasi-symmetric designs among all designs with the same parameters by adding an additional hypothesis concerning the intersection numbers of the designs.

The determination of the admissible parameters (m, n, k) of two-intersection sets in finite projective spaces is a fascinating problem which can be tackled by an interplay of number

theory and combinatorial techniques. Biliotti and Francot (1999) studied this problem in projective planes of prime power order. A basic equation due to Tallini Scafati shows that such parameters can be expressed by the coordinates of the points of a non-singular quadric. When the difference of the intersection numbers is the order of the underlying geometry, according to the terminology introduced by Penttila and Royle (1995), such parameters are called *standard* and they are easily determined. So we focus our attention mainly on the non-standard case, since it seems that not much is known about it. For the relationships between two-intersection sets, strongly regular graphs and two-weight codes the reader is referred to the article of Calderbank and Kantor (1986).

Finally, we summarize here the contents of the paper. In Section 2 we recall some well-known results due to Maria Tallini Scafati. In order to search for all the k -sets of type $(m, n)_2$ in $PG(3, q)$, in Section 3 we show how to narrow the search area and we prove that for any $q = p^h$ such that h is not a power of 2 there are at least four triples (m, n, k) of non-standard admissible parameters. In Section 4 we prove that there is a link between line intersection numbers and plane intersection numbers. In Section 5, by using Tallini-Scafati Hyperbole we provide new lower and upper bounds for the size of a two-intersection set. An integer, which is useful to study admissible parameters, is introduced in Section 6. In Section 7 we consider the case $n - m \leq q$ proving sufficient conditions for the non-existence of non-standard parameters and, as a by-product, in Section 8 we prove that two conjectures of Durante, Napolitano and Olanda are true. Finally, in Section 9 we deal the case $n - m > q = p^h$ proving that all the admissible parameters are congruent either zero or one modulo a suitable power of p .

2. A remarkable result by Tallini Scafati

The following result is due to Tallini Scafati (1976).

Result 2.1. *If K is a k -set of type $(m, n)_2$ with $0 \leq m < n \leq q^2 + q + 1$ in $PG(3, q)$ where $q = p^h$ is a prime power, then*

- (1) $m = 0$ if and only if K is a point or the complementary-set of a plane; $n = q^2 + q + 1$ if and only if K is a plane or the complementary-set of a point; (we call them trivial two-intersection sets);
- (2) the triple (m, n, k) is a point of the following quadric

$$\theta_1 k^2 + \theta_3 mn - \theta_2 mk - \theta_2 nk + q^2 k = 0 \quad (1)$$

where $\theta_d := \sum_{i=0}^d q^i$ (we call it the Tallini Scafati's quadric and it is easy to see that it is a hyperbolic hyperboloid);

- (3) if $n - m = q$ then we obtain

$$[k - m(q + 1)][k(q + 1) - (m + q)(q^2 + 1)] = 0 \quad (2)$$

- (4) $mq + 1 \leq k \leq nq$; furthermore
 - if $n \leq q^2 + q$, then $mq + n/(q + 1) \leq k$;
 - if $1 \leq m \leq q^2 - 1$, then $k \leq nq - (q^2 - m)/(q + 1)$;
- (5) if we denote by u_n the number of n -planes passing through a point not in K (an external point), then we have $(n - m)u_n = k\theta_1 - m\theta_2$;

- (6) if we denote by v_n , the number of n -planes passing through a point of K (an inner point), then we have
 $(n - m)v_n = (n - m)u_n + q^2$
 so $n - m$ divides q^2 ;
- (7) if we denote by $PG(3, q)^*$ the dual space of $PG(3, q)$, then the set of the n -planes of K is in $PG(3, q)^*$ a k^* -set K^* of type $(m^*, n^*)_2$, where $n^* = v_n$ and $m^* = u_n$.

3. Where to look?

Definition 3.1. A triple of parameters (m, n, k) satisfying the Tallini Scafati's equation (1) is said an admissible triple.

Definition 3.2. According to the terminology introduced by Penttila and Royle (1995), when $n - m = q$, i.e. the difference of the intersection numbers is the order of the underlying geometry, then the parameters are said standard.

The standard admissible parameters are well determined as we can see in the following

Remark 3.3. By equation (2) it is immediate to see that

- for any m , the triple $(m, m + q, m(q + 1))$ is a standard admissible triple;
- if $q + 1$ divides $2(m - 1)$, then the triple $(m, m + q, \frac{(m+q)(q^2+1)}{q+1})$ is a standard admissible triple.

We recall that a *spread* in $PG(3, q)$ is a partition of the set of points into lines. A *partial m -spread* is a collection of m pairwise disjoint lines that is not a spread. A *maximal partial m -spread* is a partial m -spread such that no line is disjoint from its lines. It is immediate to see that a partial m -spread is a two-intersection set whose parameters are $(m, m + q, m(q + 1))$.

It is well-known that $PG(3, q)$ has a cyclic projectivity, the Singer cycle σ of length $(q^2 + 1)(q + 1)$, which is transitive both on points and on planes. Now we recall a construction given by De Finis (1986). Consider the subgroup of $\langle \sigma \rangle$ generated by σ^{q+1} whose order is $q^2 + 1$. The orbit under σ^{q+1} of a point P in $PG(3, q)$ has length $q^2 + 1$. This orbit is an ovoid. Thus $\langle \sigma^{q+1} \rangle$ partitions $PG(3, q)$ into $q + 1$ ovoids. Any plane is tangent to exactly one of the ovoids and meets the q remaining ones in an oval. For any integer $m \leq q^2$ such that $q + 1$ divides $m - 1$ put $\delta_m := 1 + (m - 1)/(q + 1) \leq q$. Taking the point-set of δ_m of those pairwise skew ovoids we obtain an example of two-intersection set whose parameters are $(m, m + q, \frac{(m+q)(q^2+1)}{q+1})$.

As a matter of fact, relatively little is known about non-standard admissible parameters.

Remark 3.4. By 6. and 7. of Result 2.1 we have that

$$(n - m)(n^* - m^*) = q^2 \tag{3}$$

So there is a set of type $(m, n)_2$ with $n - m \leq q$ if and only if there is a set of type $(m^*, n^*)_2$ with $n^* - m^* \geq q$.

Remark 3.5. If we denote by K^c the complementary-set of K , then K^c is a k^c -set of type $(m^c, n^c)_2$ with $k^c = q^3 + q^2 + q + 1 - k$, $m^c = q^2 + q + 1 - n$ and $n^c = q^2 + q + 1 - m$. Let us explicitly note that $n^c - m^c = n - m$.

Lemma 3.6. *If $a := n - m \leq q$, then there is a k -set K of type $(m, n)_2$ with $m \leq (q^2 + q + 1 - a)/2$ if and only if there is a k^c -set K^c of type $(m^c, n^c)_2$ with $m^c \geq (q^2 + q + 1 - a)/2$.*

Proof. The following statements are equivalent

- $m \leq (q^2 + q + 1 - a)/2$
- $n = m + a \leq (q^2 + q + 1 + a)/2$
- $-(q^2 + q + 1 + a)/2 \leq -n$
- $(q^2 + q + 1 - a)/2 \leq q^2 + q + 1 - n = m^c$

□

By 6. of Result 2.1 there is an integer s with $0 \leq s \leq 2h$ such that $a = n - m = p^s$. Being $q = p^h$, we can partition all the possible cases in the following three areas

- (1) $s \leq h$ and $m \leq (q^2 + q + 1 - p^s)/2$;
- (2) $s \leq h$ and $m > (q^2 + q + 1 - p^s)/2$;
- (3) $h < s \leq 2h$.

If we search for all the k -sets of type $(m, n)_2$ in $PG(3, q)$, then it is sufficient to do an exhaustive search only in the first area. Indeed in such a way by Remark 3.4 and Lemma 3.6 we see all the k -sets of type $(m, n)_2$ lying in the other two areas.

Remark 3.7. *If there is a set K in the first area having $m < (q^2 + q + 1 - n + m)/2$, then there are also the set K^c in the second area and the sets K^* and $(K^*)^c$ in the third area.*

Example 3.8. *In $PG(3, 8)$, i.e. $q = 8$, there is a 39-set K of type $(3, 7)_2$, cf. Kiermaier (2013). We also have that*

- (1) K^c is a 546-set of type $(66, 70)_2$;
- (2) K^* is a 273-set of type $(33, 49)_2$;
- (3) $(K^*)^c$ is a 312-set of type $(24, 40)_2$.

Fixed p , h and s , we found (by computer) a number of non-standard admissible parameters lying in the first area. Then examining some of them having h different from a power of 2 and $s = h - 1$ we conjectured a function $m = m(p, h)$. Finally by equation (1) with $q = p^h$, $m = m(p, h)$ and $n = m + p^{h-1}$, we were able to find $k = k(p, h)$. Now we present this family.

Lemma 3.9. *For any integer x and for any odd integer $u \geq 3$, put*

- $q := x^u$;
- $m := (x^{u-1} - 1)(x^{u+1} - 1)/(x^3 + x^2 + x + 1)$;
- $n := m + x^{u-1}$; let us note that $n - m < q$;
- $k := (x^u + 1)(x^{2u} + 1)/(x^3 + x^2 + x + 1)$.

Then we have that both m and k are integers. Furthermore (q, m, n, k) is a solution of equation (1). Finally if $x \geq 2$, then we get $m < (q^2 + q + 1 - n + m)/2$.

Proof. If $u \equiv 1 \pmod{4}$, then $x^4 - 1$ divides $x^{u-1} - 1$. If $u \equiv 3 \pmod{4}$, then $x^4 - 1$ divides $x^{u+1} - 1$. Hence in any case $x^4 - 1$ divides $(x^{u-1} - 1)(x^{u+1} - 1)$. Now it is easy to see that $m = (x - 1)(x^{u-1} - 1)(x^{u+1} - 1)/(x^4 - 1)$. So m is an integer. Being u an odd integer, we have that $x + 1$ divides $x^u + 1$ and also that $x^2 + 1$ divides $(x^2)^u + 1$. Hence $x^3 + x^2 + x + 1 =$

$(x+1)(x^2+1)$ divides $(x^u+1)(x^{2u}+1)$. So k is an integer too. Furthermore if we substitute the quadruplet (q, m, n, k) in equation (1) we get an identity. Finally it is easy to see that if $x \geq 2$, then $m = (x^{2u} - x^{u-1} - x^{u+1} + 1)/(x^3 + x^2 + x + 1) < (x^{2u} + x^u + 1 - x^{u-1})/2 = (q^2 + q + 1 - n + m)/2$ \square

Theorem 3.10. *For each $q = p^h$ such that h is not a power of 2 there is at least one triple (m, n, k) of non-standard admissible parameters with $n - m < q$ and $m < (q^2 + q + 1 - n + m)/2$.*

Proof. There is an odd integer $u \geq 3$ such that $h = u\theta$, since h is not a power of 2. So $q = p^{u\theta} = (p^\theta)^u$. By Lemma 3.9 with $x = p^\theta \geq 2$ we have that

- $m = (p^{(u-1)\theta} - 1)(p^{(u+1)\theta} - 1)/(p^{3\theta} + p^{2\theta} + p^\theta + 1)$
- $n = m + p^{(u-1)\theta}$
- $k = (p^{u\theta} + 1)(p^{2u\theta} + 1)/(p^{3\theta} + p^{2\theta} + p^\theta + 1)$

and also that (m, n, k) is a triple of non-standard admissible parameters with $m < (q^2 + q + 1 - n + m)/2$. \square

By Remark 3.7 and Theorem 3.10 we immediately get the following

Corollary 3.11. *For each $q = p^h$ such that h is not a power of 2 there are at least four triples (m, n, k) of non-standard admissible parameters.*

Remark 3.12. *Let us note that the parameters of the 39-set K of type $(3, 7)_2$ in $PG(3, 8)$ as in Example 3.8 belong to the family seen in Theorem 3.10 with $p = 2$ and $h = 3$.*

Again by examining a number of non-standard admissible triples we got another family of parameters as we can see in the following

Example 3.13. *If $p \equiv 3 \pmod{4}$, $h \equiv 1 \pmod{2}$, $q = p^{3h}$, $m = (p^{3h} - p^{2h} - p^h + 2)(p^h + 1)/4$ and $n = m + p^{2h}$, then by equation (1) we get $k = (p^{2h} - p^h + 2)(p^{4h} - p^{2h} + 1)(p^h + 1)/4$.*

4. How line intersection numbers and plane intersection numbers are linked?

If we do not consider the trivial two-intersection sets as in 1. of Result 2.1, then $n - m \geq p > 1$ as we can see in the following

Remark 4.1. *If $1 \leq m < n \leq q^2 + q$, then $n - m \geq p > 1$.*

Proof. By 6. of Result 2.1 there is an integer s with $0 \leq s \leq 2h$ such that $n - m = p^s$. If $s = 0$, i.e. $n = m + 1$, then the discriminant of (2.1.2) is $\Delta = (q+1)^2 - 4mq^2(q^2 + q - m)$. Being $m(q^2 + q - m) \geq 1$ we have $\Delta \leq (q+1)^2 - 4q^2 = -(3q-1)(q-1) < 0$, a contradiction. Hence $s \geq 1$ and $n - m = p^s \geq p > 1$. \square

From now on we will not consider the trivial two-intersection sets. So the set K will ever be a k -set of type $(m, n)_2$ in $PG(3, q)$ with $1 \leq m < n \leq q^2 + q$ and hence $n - m = p^s$ with $s \geq 1$.

If a line r meets K in j points we say that r is a j -line. If $j = 0$, respectively $j = 1$, we say that r is an external line, respectively a tangent line. Finally if $j = q + 1$, we say that r is a contained line. We start with the following

Lemma 4.2. *If there are j -lines, then the number of n -planes through a j -line does not depend on the chosen j -line. If we denote by $w_n(j) \geq 0$ such a number, then*

$$(n-m)w_n(j) = k - m(q+1) + jq \quad (4)$$

Proof. Let r be a j -line and let x be the number of n -planes passing through r . Counting the number of points of $K \setminus r$ by the planes through r we have $(m-j)[q+1-x] + (n-j)x = k-j$ from which we get $(n-m)x = k - m(q+1) + jq$. So x does not depend from the j -line r and $x = w_n(j)$. \square

If there is an external line, then the lower bound ($k \geq mq+1$) seen in 4. of Result **2.1** can be improved with the following

Corollary 4.3. *If there is an external line, then $m \leq q^2$ and $k \geq mq+m$. Furthermore*

- $k = mq+m$ if and only if $w_n(0) = 0$;
- $k \geq mq+n$ if and only if $w_n(0) \geq 1$.

Proof. Let r be an external line and let π be a plane passing through r . Being $|\pi \cap K| \leq q^2$, $|\pi \cap K| \in \{m, n\}$ and $m < n$, we have that $m \leq q^2$. By equation (4) we get $k = m(q+1) + (n-m)w_n(0)$. \square

Remark 4.4. *The lower bound in Corollary 4.3 is sharp. As a matter of fact, if we consider m lines of a spread of $PG(3, q)$ we get a two-intersection k -set with $k = m(q+1)$ having an external line for each $m \leq q^2$.*

Remark 4.5. *If $m \leq q$, then K has at least one external line. So $k \geq m(q+1)$.*

Proof. Let α be an m -plane and let P a point of $\alpha \setminus K$. If we consider the $q+1$ lines passing through P on the plane α , we have that at least $q+1-m \geq 1$ of them are external to K . \square

Corollary 4.6. *If $k < m(q+1)$, then $m \geq q+1$.*

The following result has a number of interesting consequences.

Theorem 4.7. *If there are a j_1 -line and a j_0 -line with $j_1 > j_0$, then $n-m$ divides $(j_1 - j_0)q > 0$.*

Proof. By equation (4) we get $(n-m)w_n(j_1) = k - m(q+1) + j_1q$ and $(n-m)w_n(j_0) = k - m(q+1) + j_0q$. Hence

$$(n-m)[w_n(j_1) - w_n(j_0)] = (j_1 - j_0)q > 0 \quad (5)$$

So $n-m$ divides $(j_1 - j_0)q > 0$. \square

All the following results are consequence of Theorem **4.7**.

Corollary 4.8. *If there are a j_1 -line and a j_0 -line with $j_1 > j_0$ such that p does not divide $j_1 - j_0$, then $n-m$ divides q .*

Corollary 4.9. *If K has at least one tangent line and at least one external line, then $n-m$ divides q .*

Corollary 4.10. *Let us suppose that there are a j_0 -line and a j_1 -line with $j_1 > j_0$.*

(1) *If $n - m < q$, then $n - m = p^s$ with $1 \leq s < h$ and*

$$(j_1 - j_0)p^{h-s} = w_n(j_1) - w_n(j_0) \leq q + 1 \tag{6}$$

Furthermore $j_1 - j_0 \leq p^s = n - m < q$, since p^{h-s} and $q + 1$ are coprime.

(2) *If $n - m > q$, then $n - m = qp^r$ with $1 \leq r \leq h$ and*

$$[w_n(j_1) - w_n(j_0)]p^r = j_1 - j_0 \leq q + 1 \tag{7}$$

Furthermore $j_1 - j_0 \leq q$, since p^r and $q + 1$ are coprime.

Corollary 4.11. *If $n - m > q$, then K has not both an external line and a tangent line.*

Corollary 4.12. *If K has both an external line and a contained line, then $n - m = q$.*

Remark 4.13. *Let us note that the converse of Corollary 4.12 is not true. As a matter of fact, if we consider the point-set of a maximal partial m -spread we get a set of type $(m, m + q)_2$ which contains lines but has no external line.*

Corollary 4.14. *Let j_0 and j_1 be respectively the minimum and the maximum number of points of K contained in a line. If $n - m = p^{h+r} = qp^r$ with $1 \leq r \leq h$, then $t \leq p^{h-r}$.*

Proof. By 2. of Corollary 4.10 we have $\sum_{i=0}^{t-1} (j_{i+1} - j_i) = j_t - j_0 \leq q$. By equation (7) we have $p^r \leq h_{i+1} - h_i$. So $tp^r \leq \sum_{i=0}^{t-1} (j_{i+1} - j_i)$. Finally from $tp^r \leq q = p^h$ we get the statement. \square

Corollary 4.15. *If $n - m = q^2$, then K is a plane (so $n = q^2 + q + 1$) or the complementary set of a plane (so $m = 0$).*

Proof. If $n - m = q^2$, then $r = h$. By Corollary 4.14 we have $t \leq 1$. So K is a set of class $[h_0, h_1]_1$. By 2. of Corollary 4.10 we get $q \leq h_1 - h_0 \leq q$. So $h_1 - h_0 = q$. Hence K is of class $[1, q + 1]_1$ (i.e. K is a plane) or K is of class $[0, q]_1$ (i.e. K is the complementary set of a plane). \square

Corollary 4.16. *If $1 \leq m < n \leq q^2 + q$, then $n - m \leq q^2/p$.*

Remark 4.17. *If we do not consider the trivial two-intersection sets, then by 1. of Result 2.1 we have that $1 \leq m < n \leq q^2 + q$. Furthermore, by Remark 4.1 and Corollary 4.16, we also have that $p \leq n - m \leq q^2/p$.*

Corollary 4.18. *If K is not a trivial two-intersection set and q is a prime, then $n - m = q$.*

5. New bounds for k

If we put $x := n$ and $y := k$, then equation (1) can be rewritten in the following way

$$\mathcal{C} : \quad Bxy + Cy^2 + Dx + Ey = 0 \tag{8}$$

where

- $B = q^2 + q + 1$
- $C = -(q + 1)$
- $D = -m(q + 1)(q^2 + 1)$
- $E = m(q^2 + q + 1) - q^2$

Remark 5.1. *It is easy to see that*

- \mathcal{C} is a hyperbole;
- if $C(x_C, y_C)$ is the centre of the hyperbole, then $y_C = mq + m/(q^2 + q + 1) < mq + 1$;
- the line $y = y_C$ is a horizontal asymptote; so we are interested only to the "right side" of \mathcal{C} , since $y = k \geq mq + 1 > y_C$;
- the vertical line $x = n = m + q$ meets \mathcal{C} in the points $P_{01}(m + q, k_{01})$ and $P_{02}(m + q, k_{02})$, where $k_{01} = m(q + 1)$ and $k_{02} = (m + q)(q^2 + 1)/(q + 1)$;
- $k_{01} < k_{02}$ if and only if $m < (q^2 + 1)/2$; in this case P_{01} is under P_{02} ;
- $k_{01} > k_{02}$ if and only if $m > (q^2 + 1)/2$; in this case P_{02} is under P_{01} ;
- $k_{01} = k_{02}$ if and only if $m = (q^2 + 1)/2$; in this case the line $x = n = m + q$ is tangent to \mathcal{C} , so there are no points having $x = n < m + q$;

As an immediate consequence of the previous Remark we have new bounds for k as we can see in the following

Lemma 5.2. *Let $P(n, k)$ be a point of \mathcal{C} .*

- (1) *If $m < (q^2 + 1)/2$, then*
 - $n < m + q$ implies $k > m(q + 1)$;
 - $n > m + q$ implies $k > k_{02}$ or $mq + 1 < k < m(q + 1)$ (let us note that in the last case by Corollary 4.6 it is also $m \geq q + 1$).
- (2) *If $m > (q^2 + 1)/2$, then*
 - $n < m + q$ implies $k > k_{02}$;
 - $n > m + q$ implies $mq + 1 < k < k_{02}$ or $k > m(q + 1)$;
- (3) *If q is odd and $m = (q^2 + 1)/2$, then $n - m \geq q$.*

6. An useful integer c

Let K be a k -set of type $(m, n)_2$ in $PG(3, q)$ with $q = p^h$.

Lemma 6.1. $n - m$ divides $k - m$ and $k - n$.

Proof. By 6. of Result 2.1 there is an integer s with $0 \leq s \leq 2h$ such that $n - m = p^s$. By 5. of Result 2.1, we get $p^s u_n = (k - m)(p^h + 1) - mp^{2h}$. Being p^s and $p^h + 1$ coprime, we have that $n - m = p^s$ divides $k - m$. Finally $n - m$ divides $(k - m) - (n - m) = k - n$. \square

Theorem 6.2. *There is an integer s with $s \leq 2h$ such that for each $d \leq s$ we have that*

$$m \equiv n \equiv k \pmod{p^d} \quad (9)$$

Corollary 6.3. *If $s \geq h$, i.e. $n - m \geq q$, then*

$$m \equiv n \equiv k \pmod{q} \quad (10)$$

Lemma 6.4. *If $m \equiv j \pmod{q}$ with $0 \leq j < q$, then there is an integer c such that*

$$k = m + (m - j)q + c(n - m) \tag{11}$$

Proof. Being $m \equiv j \pmod{q}$, we have that q^2 divides $(m - j)q$. Hence $n - m$ divides $(m - j)q$, since $n - m$ divides q^2 . By Lemma 6.1 $n - m$ divides $k - m$. Now if we consider the following integer

$$c := \frac{k - m}{n - m} - \frac{(m - j)q}{n - m} \tag{12}$$

then we have the statement. □

Remark 6.5. *If there is a j -line r , then $c = w_n(j)$, see equation (4), i.e. c is the number of the n -planes passing through a j -line. But let us explicitly note that the existence of the integer c does not depend from the existence of a j -line.*

7. The case $n - m \leq q$

In this Section K will ever be a non-trivial k -set of type $(m, n)_2$ in $PG(3, q)$ (i.e. $1 \leq m < n \leq q^2 + q$) with $p^s = n - m \leq q = p^h$. So $1 \leq s \leq h$. Let j be the integer such that $m \equiv j \pmod{q}$ and $0 \leq j < q$. Finally let c be the integer as in (12).

Remark 7.1. *We have*

- (1) $c \equiv \frac{k-m}{n-m} \pmod{qp^{h-s}}$;
- (2) $m^* \equiv \frac{k-m}{n-m} \pmod{q}$;
- (3) $m^* \equiv c \pmod{q}$.

Proof. By equation (12) we have $c = \frac{k-m}{n-m} - (m - j)p^{h-s}$. Hence we have (1), since $m - j \equiv 0 \pmod{q}$. Now by 6. and 7. of Result 2.1 we get $m^* = \frac{k-m}{n-m} + [\frac{k-m}{n-m} - mp^{h-s}]q$. So we have (2). Finally, by (1) and (2) we immediately get (3). □

Lemma 7.2. *If $p^s = n - m \leq q$ and there is an integer $b \leq s$ such that $j \equiv 0, 1 \pmod{p^b}$, then $c \equiv 0, 1 \pmod{p^{2(h-s)+b}}$.*

Proof. Equation (1) can be rewritten in the following way

$$(k - m)(k - n)(q + 1) = q^2[k(m - 1) + n(k - m) - mnq] \tag{13}$$

Now let us note that by hypothesis $p^b \leq p^s = n - m \leq p^h = q$.

Being $m \equiv j \pmod{q}$ and $p^s \leq p^h = q$, then by Theorem 6.2 we have that $m \equiv n \equiv k \equiv j \pmod{p^s}$ and $k(m - 1) \equiv j(j - 1) \pmod{p^s}$. So $k(m - 1) \equiv 0 \pmod{p^b}$, since $p^b \leq p^s$. Furthermore p^b divides both q and $k - m$ (since $p^s = n - m$ divides $k - m$). Finally $p^b q^2$ divides the right side of equation (13). So p^{2h+b} divides $(k - m)(k - n)$.

Now let α be the integer such that $m = \alpha q + j$ with $0 \leq j < q$. By Lemma 6.4 we get $k = \alpha q(q + 1) + cp^s + j$. Being $n = m + p^s = \alpha q + p^s + j$ we get

$$(k - m)(k - n) = \alpha^2 p^{4h} + \alpha(2c - 1)p^{2h+s} + c(c - 1)p^{2s} \tag{14}$$

where $p^{4h} > p^{2h+s} > p^{2s}$, since $s \leq h$.

So p^{2h+b} divides $c(c - 1)p^{2s}$ and we have the statement. □

Corollary 7.3. *If $p^s = n - m \leq q$, then $c \equiv 0, 1 \pmod{p^{2(h-s)}}$.*

Corollary 7.4. *If $p^s = n - m \leq q$ and $j \equiv 0, 1 \pmod{p^s}$, then $c \equiv 0, 1 \pmod{p^{2h-s}}$. So q^2 divides $c(c-1)(n-m)$.*

Theorem 7.5. *Let K be a k -set of type $(m, n)_2$ of $PG(3, q)$ with*

- $1 \leq m \leq (q^2 + 1)/2$;
- $a := n - m \leq q$;
- $m \equiv j \pmod{q}$ with $0 \leq j < q$;
- $j \equiv 0, 1 \pmod{a}$.

Then $n - m = q$.

Proof. By 3. of Lemma 5.2 if q is odd and $m = (q^2 + 1)/2$, then $n - m \geq q$. So $n - m = q$. Now let us consider the case $m < (q^2 + 1)/2$. We have to prove that $n - m = q$. On the contrary let us suppose that $a = n - m < q$ and let $b \geq p$ the integer such that $q = ab$. By the last assumption in Theorem 7.5 there are two non-negative integers v and $u \in \{0, 1\}$ such that $j = u + av$. If $b \leq v$, then $q \leq u + q = u + ab \leq u + av = j < q$ a contradiction. So $v \leq b - 1$ and hence $j = u + av \leq u + ab - a = u + q - a \leq 1 + q - a$. Finally we get $a + j - 1 \leq q$. Now, by Lemma 6.4, there is an integer c such that $k = m + (m - j)q + ca$. Being $m \leq q^2 - 1$, by 4. of Result 2.1 we have that

$$m + (m - j)q + ca = k \leq nq - \frac{q^2 - m}{q + 1} = (m + a)q - \frac{q^2 - m}{q + 1}$$

from which we obtain $ac \leq (a + j - 1)q - \frac{m - 1}{q + 1}$. So $ac \leq q^2 - \frac{m - 1}{q + 1}$.

Now, being $m < (q^2 + 1)/2$ and $n = m + a < m + q$, by 1. of Lemma 5.2 it is $m + (m - j)q + ca = k > m(q + 1)$. So $ca > jq \geq 0$ and hence $c > 0$. Furthermore let us note that if $c = 1$, then $j = 0$ necessarily, since $a < q$. In such a case $m = dq$ with $d > 0$ and $k = dq(q + 1) + a$. By equation (1) with $m = dq$, $n = dq + a$ and $k = dq(q + 1) + a$ we get $a = 1 + d[(b - 1)q + b + 1]$. So $a \geq 1 + (b - 1)q + b + 1 \geq (p - 1)q + p + 2 > q$, a contradiction. Thus $c > 1$. Now, by Corollary 7.4, we have that q^2 divides $ac(c - 1) > 0$. Being c and $c - 1$ coprime, q^2 divides ac or $a(c - 1)$. In each case we get $q^2 \leq ac$. So we have that $q^2 \leq ac \leq q^2 - \frac{m - 1}{q + 1}$ and hence $m = 1$ and $ac = q^2$ necessarily. Now by equation (1) with $m = 1$ and $k = m + (m - j)q + ca = 1 + q^2$ we get $n = q + 1$ and hence $n - m = q$, a contradiction. So $n - m = q$. \square

Corollary 7.6. *Let K be a k -set of type $(m, n)_2$ of $PG(3, q)$ such that*

- $1 \leq m \leq (q^2 + 1)/2$;
- $n - m \leq q$;
- $m \equiv 0, 1 \pmod{q}$.

Then $n - m = q$.

8. On sets of type $(q, n)_2$ and sets of type $(q + 1, n)_2$

Durante *et al.* (2016a,b) studied the cases $m = q$ and $m = q + 1$. They also conjectured that in such cases it is $n = m + q$ (if K is not a plane). Here we prove their conjectures.

Remark 8.1. *If $m \leq q + 1$, then K has at least one tangent line.*

Proof. Let α be an m -plane and let P a point of $K \cap \alpha$. If we consider the $q + 1$ lines passing through P on the plane α , we have that at least $q + 1 - (m - 1) = q - m + 2 \geq 1$ of them are tangent to K . \square

Durante *et al.* (2016b) proved, among other things, the following

Result 8.2. *If $m = q + 1$ and K is not a plane, then K has at least one external line.*

By Remark 8.1, Result 8.2, Remark 4.5, and Corollary 4.9 we have the following

Theorem 8.3. *If $m \leq q + 1$ and K is not a plane, then $n - m$ divides q .*

By Theorem 8.3 and Corollary 7.6 we immediately have the following results

Corollary 8.4. *If K is a k -set of type $(q, n)_2$, then $n = 2q$.*

Corollary 8.5. *If K is a k -set of type $(q + 1, n)_2$ and K is not a plane, then $n = 2q + 1$.*

So the two conjectures of Durante, Napolitano and Olanda are true.

9. Few words on the case $n - m > q$

Let K be a non-trivial k -set of type $(m, n)_2$ in $PG(3, q)$ with $n - m > q$. So by Corollary 4.18 $h \geq 2$ and by Corollary 4.16 there is an integer r with $1 \leq r < h$ such that $n - m = qp^r$. If we put $s := h - r$, then $1 \leq s < h$. By Remark 3.4 there is a non-trivial k^* -set K^* of type $(m^*, n^*)_2$ in the dual space $PG(3, q)^*$ with $n^* - m^* = q^2 / (n - m) = q / p^r = p^s < q$. Now by Remark 7.1 we have that $m = (m^*)^* \equiv c^* \pmod{p^h}$. Being $2(h - s) = 2r$, by Corollary 7.3 we have that $c^* \equiv 0, 1 \pmod{p^{2r}}$. If we put $e := \min\{2r, h\}$, then $p^e < qp^r = n - m$, since $r < h$. So by (6.2) we have the following

Theorem 9.1. *Let K be a non-trivial k -set of type $(m, n)_2$ in $PG(3, q)$ with $n - m = qp^r > q$. If $e := \min\{2r, h\} \geq 2$, then $m \equiv n \equiv k \equiv 0, 1 \pmod{p^e}$.*

Remark 9.2. *Let us explicitly note that (differently from the case $n - m > q$) if $p^s = n - m < q$ with $s \geq 1$, then there are admissible triple (k, n, m) such that $k \equiv n \equiv m \equiv j \pmod{p^s}$ and p does not divide $j(j - 1)$. We recall that the triple (k^c, n^c, m^c) has $n^c - m^c = n - m < q$. Furthermore, being $m^c = q^2 + q + 1 - n$, if we denote by j^c the integer such that $0 \leq j^c \leq q$ and $m^c \equiv j^c \pmod{p}$, then $j^c \equiv 1 - j \pmod{p}$.*

Example 9.3. *Let us consider a non-standard admissible triple as in Example 3.13 with $h = 1$. It is easy to see that $m \equiv \frac{p+1}{2} \pmod{p}$. So $j = \frac{p+1}{2} = j^c$.*

Example 9.4. *If $q = 343$, then $(m, n, k) = (62, 111, 21720)$ is a non-standard admissible triple. We have $j = 6$ and $j^c = 2$.*

References

- Biliotti, M. and Francot, E. (1999). "Parameters for Sets of Type (m, n) in Projective Planes of Prime Power Order". *Journal of Combinatorial Theory, Series A* **86**(2), 395–400. DOI: [10.1006/jcta.1998.2935](https://doi.org/10.1006/jcta.1998.2935).
- Blokhuis, A. and Lavrauw, M. (2000). "Scattered spaces with respect to a spread in $PG(n, q)$ ". *Geometriae Dedicata* **81**(1-3), 231–243. DOI: [10.1023/A:1005283806897](https://doi.org/10.1023/A:1005283806897).
- Blokhuis, A. and Lavrauw, M. (2002). "On Two-intersection Sets with Respect to Hyperplanes in Projective Spaces". *Journal of Combinatorial Theory, Series A* **99**(9), 377–382. DOI: [10.1006/jcta.2002.3289](https://doi.org/10.1006/jcta.2002.3289).
- Calderbank, R. and Kantor, W. M. (1986). "The geometry of two-weight codes". *Bulletin of the London Mathematical Society* **18**(2), 97–122. DOI: [10.1112/blms/18.2.97](https://doi.org/10.1112/blms/18.2.97).

- Cossidente, A. and Van Maldeghem, H. (2007). “The simple exceptional group $G_2(q)$, q even, and two-character sets”. *Journal of Combinatorial Theory, Series A* **114**(5), 964–969. DOI: [10.1016/j.jcta.2006.09.006](https://doi.org/10.1016/j.jcta.2006.09.006).
- De Finis, M. (1986). “On k -sets of type (m, n) in $PG(3, q)$ with respect to planes”. *Ars Combinatoria* **21**, 119–136.
- De Resmini, M. J. (1987). “A 35-Set of type $(2, 5)$ in $PG(2, 9)$ ”. *Journal of Combinatorial Theory, Series A* **45**(1), 303–305. DOI: [10.1016/0097-3165\(87\)90021-5](https://doi.org/10.1016/0097-3165(87)90021-5).
- De Resmini, M. J. (1988). “On admissible sets with two intersection numbers in a projective plane”. *Annals of Discrete Mathematics* **37**, 137–146. DOI: [10.1016/S0167-5060\(08\)70232-2](https://doi.org/10.1016/S0167-5060(08)70232-2).
- Durante, N., Napolitano, V., and Olanda, D. (2016a). “Sets of type (q, n) in $PG(3, q)$ ”. *Ricerche di Matematica* **65**(1), 65–70. DOI: [10.1007/s11587-015-0252-x](https://doi.org/10.1007/s11587-015-0252-x).
- Durante, N., Napolitano, V., and Olanda, D. (2016b). “Sets of type $(q + 1, n)$ in $PG(3, q)$ ”. *Journal of Geometry* **107**(1), 9–18. DOI: [10.1007/s00022-015-0271-5](https://doi.org/10.1007/s00022-015-0271-5).
- Hamilton, N. and Penttila, T. (2001). “Sets of type (a, b) from subgroups of $\Gamma L(1, p^r)$ ”. *Journal of Algebraic Combinatorics* **13**(1), 67–76. DOI: [10.1023/A:1008775818040](https://doi.org/10.1023/A:1008775818040).
- Hirschfeld, J. W. P. (1985). *Finite Projective Spaces of Three Dimensions*. Oxford Mathematical Monographs. Oxford University Press.
- Innamorati, S. and Zuanni, F. (2015). “In $AG(3, q)$ any q^2 -set of class $[1, m, n]_2$ is a cap”. *Discrete Mathematics* **338**(1), 863–865. DOI: [10.1016/j.disc.2015.01.011](https://doi.org/10.1016/j.disc.2015.01.011).
- Innamorati, S. and Zuanni, F. (2017). “In $AG(3, q)$ any q^2 -set of class $[0, m, n]_2$ containing a line is a cylinder”. *Journal of Geometry* **108**(2), 457–462. DOI: [10.1007/s00022-016-0351-1](https://doi.org/10.1007/s00022-016-0351-1).
- Jungnickel, D. (2011). “Characterizing geometric designs, II”. *Journal of Combinatorial Theory, Series A* **118**(2), 623–633. DOI: [10.1016/j.jcta.2010.05.004](https://doi.org/10.1016/j.jcta.2010.05.004).
- Kiermaier, M. (2013). MR2999552. Mathematical Reviews.
- Penttila, T. and Royle, G. F. (1995). “Sets of type (m, n) in the affine and projective planes of order nine”. *Designs, Codes and Cryptography* **6**(3), 229–245. DOI: [10.1007/BF01388477](https://doi.org/10.1007/BF01388477).
- Tallini Scafati, M. (1976). “Sui k -insiemi di uno spazio di Galois $S_{r,q}$ a due soli caratteri nella dimensione d ”. *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8* **60**(6), 782–788.
- Tallini, G. (1987). “Some new results on sets of type (m, n) in projective planes”. *Journal of Geometry* **29**(2), 191–199. DOI: [10.1007/BF01225209](https://doi.org/10.1007/BF01225209).
- Thas, J. A. (1973). “A combinatorial problem”. *Geometriae Dedicata* **1**(2), 236–240. DOI: [10.1007/BF00147522](https://doi.org/10.1007/BF00147522).

^a Università degli Studi dell’Aquila
Dipartimento di Ingegneria industriale e dell’informazione e di economia
Via Giovanni Gronchi 18, I-67100 L’Aquila, Italy

* To whom correspondence should be addressed | email: stefano.innamorati@univaq.it

