Discrete Mathematics 311 (2011) 2253–2258

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

On sets without tangents and exterior sets of a conic

Geertrui Van de Voorde

Vakgroep Wiskunde, Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussel, Belgium

ARTICLE INFO

Article history:
Received 11 January 2011
Received in revised form 29 June 2011
Accepted 6 July 2011
Available online 3 August 2011

Keywords:
Set without tangents
Exterior set of a conic
LDPC code
Stopping sets

ABSTRACT

A set without tangents in PG(2, q) is a set of points $\mathcal{S}$ such that no line meets $\mathcal{S}$ in exactly one point. An exterior set of a conic $\mathcal{C}$ is a set of points $\mathcal{E}$ such that all secant lines of $\mathcal{E}$ are external lines of $\mathcal{C}$. In this paper, we first recall some known examples of sets without tangents and describe them in terms of determined directions of an affine pointset. We show that the smallest sets without tangents in PG(2, 5) are (up to projective equivalence) of two different types. We generalise the non-trivial type by giving an explicit construction of a set without tangents in PG(2, q), $q = p^h$, $p > 2$ prime, of size $q(q-1)/2 - r(q+1)/2$, for all $0 \leq r \leq (q-5)/2$. After that, a different description of the same set in PG(2, 5), using exterior sets of a conic, is given and we investigate in which ways a set of exterior points on an external line L of a conic in PG(2, q) can be extended with an extra point Q to a larger exterior set of $\mathcal{C}$. It turns out that if $q = 3 \bmod 4$, Q has to lie on L, whereas if $q = 1 \bmod 4$, there is a unique point Q not on L.

1. Introduction and preliminaries

Throughout this paper, $q = p^h$, where p is a prime, and the finite field of order q is denoted by $\mathbb{F}_q$. It is well known that $\mathbb{F}_q$, q odd, contains $(q+1)/2$ squares and $(q-1)/2$ non-squares. The projective plane of order q is denoted by PG(2, q). If $\mathcal{S}$ is a set of points in PG(2, q), then a line meeting $\mathcal{S}$ in exactly 1 point is called a *tangent* line (of $\mathcal{S}$), lines containing no points of $\mathcal{S}$ are called *external* (lines of $\mathcal{S}$) and lines containing at least 2 points are called *secant* (lines of $\mathcal{S}$). If $\mathcal{S}$ is a set such that no line of PG(2, q) is a tangent of $\mathcal{S}$, $\mathcal{S}$ is called a *set without tangents*.

Let $\mathcal{C}$ be an irreducible conic in PG(2, q), q odd, then $\mathcal{C}$ has $q+1$ points and a line of PG(2, q) meets $\mathcal{C}$ in 0, 1, or 2 points. The conic $\mathcal{C}$ has $q+1$ tangent lines, $q(q-1)/2$ external lines and $q(q+1)/2$ secant lines. The points, not on $\mathcal{C}$, that lie on a tangent line of $\mathcal{C}$, are called *exterior* (points of $\mathcal{C}$) and every exterior point lies on exactly two tangent lines of $\mathcal{C}$. The points not lying on a tangent line of $\mathcal{C}$, are called *interior* (points of $\mathcal{C}$). A *Desargues configuration* $\mathcal{D}$ in PG(2, q) is a set consisting of 10 points of PG(2, q), and 10 lines of PG(2, q), such that every line contains 3 points of $\mathcal{D}$ and through every point of $\mathcal{D}$ there are 3 lines.

1.1. Exterior sets of conics

An *exterior set* $\mathcal{E}$ of $\mathcal{C}$ is a set of points such that every secant line of $\mathcal{E}$ is an external line of $\mathcal{C}$.

If $\mathcal{S}$ is a set of $(q+1)/2$ exterior points forming an exterior set of the conic $\mathcal{C}$, then we have the following theorem by Blokhuis et al.

Theorem 1 ([4]). *Let $\mathcal{S}$ be a set of $(q+1)/2$ exterior points forming an exterior set of the conic $\mathcal{C}$. If $q = 1 \bmod 4$, $\mathcal{S}$ consists of the $(q+1)/2$ exterior points on an external line of $\mathcal{C}$. If $q = 3 \bmod 4$, there exist other examples (at least for $q = 7, 11, \ldots, 31$).*

It is conjectured by the authors of the same paper (and checked by computer for $q < 131$), that only for $q = 7, 11, \ldots, 31$, there exist other examples.

E-mail address: gvdevoor@vub.ac.be.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2011.07.010

1.2. Sets without tangents

A non-empty set without tangents in PG(2, q) is easily seen to have at least $q+2$ points. If q is even, this bound is sharp by the existence of hyperovals. If q is odd, no hyperovals exist and the determination of size of the smallest non-empty set without tangents in PG(2, q) remains an open problem, except for a few small values of q. Let u_q be the size of the smallest set without tangents in PG(2, q). In [3], Blokhuis et al. determined that $u_3 = 6$, $u_5 = 10$, $u_7 = 12$. We showed by computer that $u_9 = 15$, and $u_{11} = 18$.

It is easy to construct a set without tangents of size $2q$: let $\mathcal{S}$ be the set of points on two different lines L_1 and L_2, different from the intersection point $L_1 \cap L_2$. We call this example the *trivial* set without tangents.

1.3. Directions determined by a pointset

Let $\mathcal{S}$ be a set of points with coordinates $\langle(x, y, z)\rangle$ in PG(2, q), let L_∞ be the line with equation $z = 0$ of PG(2, q) and let PG(2, q) $\setminus L_\infty$ be the affine plane AG(2, q), obtained by removing the line L_∞. The pointset of $\mathcal{A} = \mathcal{S} \setminus L_\infty$ in AG(2, q) is called the *affine part* of $\mathcal{S}$ and consists of points with coordinates $\langle(x_i, y_i, 1)\rangle$, $i = 1, \ldots, |\mathcal{S}|$. The set of determined directions $\mathcal{D}$ is defined as

$$\mathcal{D} = \left\{ \frac{y_i - y_j}{x_i - x_j} \middle| 1 \leq i \neq j \leq |\mathcal{S}| \right\}.$$

We identify a direction d in $\mathcal{D}$ with the point $\langle(1, d, 0)\rangle$ on L. If $x_i = x_j$ for some $i \neq j$, then the determined direction is ∞, which is identified with the point $\langle(0, 1, 0)\rangle$ on L_∞.

1.4. Finite geometry codes and stopping sets

An $\mathbb{F}_p$-*linear code* C of length n is a vector subspace of $V(n, p)$. The vectors of C are called *codewords*. The *incidence matrix* of a projective plane Π of order $q = p^h$ is the matrix A where the columns are indexed by the points $P_1, \ldots, P_{q^2+q+1}$ of Π, the rows are indexed by the lines $L_1, \ldots, L_{q^2+q+1}$ of Π, and with entry $A_{ji} = 1$ if P_j lies on L_i, and entry 0 otherwise. The *code of* PG(2, q), denoted by $C(2, q)$ is the $\mathbb{F}_p$-span of the rows of A. The *dual code* $C^\perp$ of a code C of length n is the vector space consisting of all vectors v of $V(n, p)$ such that $v.c = 0$ for all $c \in C$. The *support* of a codeword is the set of coordinate positions for which the corresponding entry in the codeword is non-zero.

The minimum weight of $C(2, q)^\perp$ is only known in the case that q is even (then it is $q+2$), and the case that q is a prime p (then it is $2p$). It is not too hard to see that the set of points $\mathcal{S}$ defined by the support of a codeword of $C(2, q)^\perp$ is a set without tangents: a codeword has scalar product with all rows of A equal to zero. Since the rows of A correspond to the lines of Π, this implies that there cannot be lines containing exactly one point of $\mathcal{S}$. It should be noted that every codeword of $C(2, q)^\perp$ gives rise to a set without tangents, but the vice versa part is generally not true. As we have seen, the minimum weight of $C(2, p)^\perp$, p prime, is $2p$, but we will give an example of a set without tangents of weight $2p-2$ for $p > 5$. However, the smallest known example of a non-trivial set without tangents in PG(2, q), q not a prime, arises from the support of a codeword in $C(2, q)^\perp$.

The dual code of a projective plane is often considered as a so-called *LDPC-code* (see [11]), and the number of errors that can be decoded by using iterative decoding over a binary erasure channel is entirely defined by the size of the smallest *stopping set* (see [7]). In the case of the LDPC-code of a projective plane PG(2, q), these *stopping sets* are exactly the sets without tangents in PG(2, q), regardless whether q is even or odd. Hence, the problem of finding the smallest set without tangents in projective planes of odd order is of importance when studying the LDPC-codes of projective planes. This point of view on sets without tangents was used in the papers [10,14], where elementary bounds on the size of the smallest stopping sets are derived. However, the results are much weaker than the ones on sets without tangents obtained by Blokhuis et al. [3].

1.5. Arcs, conics, and $P\Gamma L(3, q)$

A k-*arc* in PG(2, q) is a set of k points in PG(2, q) such that no three of them are collinear. It is easy to see that a k-arc in PG(2, q), has at most $q+2$ points. If a $(q+2)$-arc (i.e. a hyperoval) exists, necessarily q is even. The pointset of an irreducible conic forms a $(q+1)$-arc in PG(2, q), and if q is odd, Segre showed that the converse also holds.

Theorem 2 (*[13]*). *A $(q+1)$-arc in* PG(2, q), *q odd, is an irreducible conic.*

The following well-known lemmas will be used in the proof of Theorem 15. The collineation group of PG(2, q) is denoted by $P\Gamma L(3, q)$ and consists of all semi-linear transformations.

Lemma 3. (1) *(See e.g.* [9, *Theorem 2.36*]*). The group* PGL(3, q) *acts transitively on the non-empty irreducible conics of* PG(2, q).

(2) *(See e.g.* [8, *Theorem 22.6.6*]*). Let $\mathcal{C}$ be an irreducible conic in* PG(2, q), *q odd. The stabiliser of $\mathcal{C}$ in $P\Gamma L(3, q)$, acts transitively on the external lines of $\mathcal{C}$.*

Remark 4. Recall that an irreducible conic in PG(2, q), q odd, is always non-empty.

2. Sets without tangents in PG(2, q)

2.1. A lower bound and some old examples

If q is odd, the following theorem of Blokhuis et al. gives a lower bound on the size of a set without tangents in PG(2, q).

Theorem 5 ([3]). *A non-empty set without tangents in* PG(2, q), q *odd, has at least* $q + \frac{1}{4}\sqrt{2q} + 2$ *points.*

Unfortunately, the bound of Theorem 5 is probably not sharp and the known examples of sets without tangents have size substantially larger than this lower bound. As we have already seen, the trivial set without tangents in PG(2, q) contains $2q$ points. In [3], the authors present another example of a set without tangents in PG(2, q), $q > 5$. It has size $2(q-1)$ and arises from two conics: let $\mathcal{C}_1$ be the conic with equation $Z^2 = XY$ and let $\mathcal{C}_2$ be the conic with equation $Z^2 = aXY$, with a in $\mathbb{F}_q$ such that $1-a$ and $a(a-1)$ are both squares. The points that lie on $\mathcal{C}_1$ or $\mathcal{C}_2$, but not on both, can be shown to be a set without tangents. For q prime, this example is the best known. If q is not prime, the following construction giving rise to a codeword in $C(2, q)^{\perp}$ by Lavrauw et al. (see also [6]) improves this bound and is up to our knowledge the smallest known.

Theorem 6 ([12]). *Let* $\mathcal{A}$ *be the set of points of the form* $\{\langle(1, x, x^p)\rangle | x \in \mathbb{F}_q\}$ *and let* $\mathcal{N}$ *be the set of points on the line* $x = 0$ *that are not of the form* $\langle(0, x, x^p)\rangle$, *then* $\mathcal{A} \cup \mathcal{N}$ *is a set without tangents of size* $q + (q-p)/(p-1)$.

The set $\mathcal{A}$ in the previous theorem is a set of q affine points and the set $\mathcal{N}$ is the set of non-determined directions of $\mathcal{A}$. This example is the example of smallest size of the following, more general construction.

Theorem 7. *Let* $\mathcal{A}$ *be a set of* q *affine points in* PG(2, q), $p > 2$, *and let* $\mathcal{D}$ *be the set of determined directions of* $\mathcal{A}$, *lying on* L_∞. *If* $|\mathcal{D}| < (q+3)/2$, *then* $\mathcal{A}$, *together with the complement of* $\mathcal{D}$ *in* L_∞, *is a set without tangents. Vice versa, if* $\mathcal{S}$ *is a set without tangents of size* $q + k$ *and suppose that there exists a line* L_∞ *with* k *points of* $\mathcal{S}$. *Then the* k *points on* L_∞ *are the non-determined directions of the set* $\mathcal{A} = \mathcal{S} \setminus L_\infty$.

Proof. If $|\mathcal{D}| < (q+3)/2$, then the main theorem of [5] implies that every line meets $\mathcal{A} \cup \mathcal{D}$ in 1 mod p points. Denote the complement of $\mathcal{D}$ in L_∞ by $\mathcal{N}$ and let N be a point of $\mathcal{N}$. Since N is a non-determined direction, and $|\mathcal{A}| = q$, every line through N meets $\mathcal{A}$ in exactly one point. Let P be a point of $\mathcal{A}$, and let L be a line through P, not through a non-determined direction, then, since L meets $\mathcal{A} \cup \mathcal{D}$ in 1 mod p points, there are at least $p > 2$ points of $\mathcal{A}$ in L. Hence, $\mathcal{A} \cup \mathcal{N}$ is a set without tangents.

Suppose now that $\mathcal{S}$ is a set without tangents of size $q + k$ and suppose that there exists a line L_∞ with k points of $\mathcal{S}$. If Q is a point of L_∞, not in $\mathcal{S}$, then every line through Q and a point of $\mathcal{A} = \mathcal{S} \setminus L_\infty$, has to contain another point of $\mathcal{A}$, hence, Q is a direction, determined by the points of $\mathcal{A}$. If Q is a point of L_∞ in $\mathcal{S}$, then all q lines through Q have to contain a point of $\mathcal{S}$. Since $|A| = q$, every line through Q contains exactly one point of $\mathcal{A}$, and hence Q is a non-determined direction. □

Remark 8. If $q = p$ prime, the set without tangents constructed in the previous lemma is the trivial set without tangents. It also follows that a set without tangents $\mathcal{S}$ in PG(2, p) of size $\leq 2p$, that contains a line with p points of $\mathcal{S}$, is the trivial set without tangents. For example, this shows that a set without tangents $\mathcal{S}$ in PG(2, 3) of size 6 is trivial: let P be a point of $\mathcal{S}$. Since there are 4 lines through P and 5 points of $\mathcal{S}$ left, there is a 3-secant L through P.

Remark 9. If we take $\mathcal{A} = \{\langle(1, x, Tr(x))\rangle\}$, then we obtain the set without tangents of size $2q - q/p$, constructed in [5].

2.2. The prime case

We can exploit the link with determined directions a little bit further to prove that in PG(2, p), p prime, a set without tangents $\mathcal{S}$, having a secant with 'many' points of $\mathcal{S}$, is trivial. For this, we need the following proposition of Ball, which uses the techniques developed by Blokhuis in [2].

Theorem 10 ([1, Corollary 4.4]). *Let* AG(2, p) = PG(2, p) $\setminus L_\infty$, *and* p *prime. Let* $\mathcal{A}$ *be a set of points of* AG(2, p). *If there are at least* $|\mathcal{A}| - (p-1)/2$ *and at most* $p-1$ *points* P *on* L_∞ *for which the lines through* P *are all incident with at least one point of* $\mathcal{A}$, *then* $\mathcal{A}$ *contains all the points of a line of* AG(2, p).

Theorem 11. *Let* $\mathcal{S}$ *be a set without tangents in* PG(2, p), p *prime, with* $|\mathcal{S}| \leq 2p$. *If there is a line* L_∞ *containing* x *points of* $\mathcal{S}$, *and* $x \geq |\mathcal{S}|/2 - (p-1)/4$, *then* $\mathcal{S}$ *is trivial.*

Proof. Let L_∞ be the line containing x points of $\mathcal{S}$, with $x \geq |\mathcal{S}|/2 - (p-1)/4$. For every point N in $\mathcal{S} \cap L_\infty$, the p lines through N, different from L_∞, contain a point of $\mathcal{S}$. The affine part $\mathcal{A} = \mathcal{S} \setminus L_\infty$, contains $|\mathcal{S}| - x$ points. If $x = p+1$, then it easily follows that $|\mathcal{S}| \geq 2p+1$ which is a contradiction. If $x = p$, then by Remark 8, $\mathcal{S}$ is trivial. Hence, suppose that $x \leq p-1$. Since $x \geq |\mathcal{S}| - x - (p-1)/2$, we may apply Theorem 10, and obtain that the affine part of $\mathcal{S}$ contains an affine line. It follows again from Remark 8 that $\mathcal{S}$ is trivial. □

Corollary 12. *If* $\mathcal{S}$ *is a set without tangents in* PG(2, p), *and* $|\mathcal{S}| < 2p$, *then a line has at most* $|\mathcal{S}|/2 - (p-5)/4$ *points of* $\mathcal{S}$.

2.3. A new construction

Lemma 13. *The set of interior points of an irreducible conic $\mathcal{C}$ in* PG$(2, q)$, *q odd, $q \geq 5$ is a set without tangents of size $q(q-1)/2$.*

Proof. Let $\mathcal{S}$ be the set of interior points of $\mathcal{C}$. The point P of $\mathcal{S}$ lies only on secant lines and external lines to $\mathcal{C}$. As a secant line contains $(q-1)/2$ interior points and an external line contains $(q+1)/2$ interior points, every line through P contains at least $(q-3)/2$ other points of $\mathcal{S}$. Since $q \geq 5$, $\mathcal{S}$ is a set without tangents. □

As we will see in the next subsection, this example, together with the trivial example, is the best possible for PG$(2, 5)$. When $q > 5$, we can find examples of smaller size using the same idea.

Theorem 14. *There exists a set without tangents $\mathcal{S}$ in* PG$(2, q)$, *q odd, of size $q(q-1)/2 - r(q+1)/2$, for all $0 \leq r \leq (q-5)/2$.*

Proof. Let $\mathcal{C}$ be an irreducible conic in PG$(2, q)$, q odd, and let Q be an exterior point of $\mathcal{C}$. Let $\mathcal{R}$ be a set of r external lines through Q to $\mathcal{C}$, where $0 \leq r \leq (q-5)/2$. Let $\mathcal{S}$ be the set of internal points to $\mathcal{C}$, not contained in the lines of $\mathcal{R}$. Then $|\mathcal{S}| = q(q-1)/2 - r(q+1)/2$, and every line through a point of P contains at least $(q-3)/2 - (q-5)/2 = 1$ other point of $\mathcal{S}$. □

2.4. The case PG$(2, 5)$

Recall from Section 1.2 that $u_5 = 10$. In this section, we show that every set without tangents in PG$(2, 5)$ of size 10 is either trivial or arises from the example of Lemma 13.

Theorem. *Up to projective equivalence, there exist exactly* 2 *sets without tangents of size* 10 *in* PG$(2, 5)$*:*

(i) *The set of points on two lines L_1 and L_2, different from $L_1 \cap L_2$.*
(ii) *The points on a Desargues configuration, which is the set of internal points of a conic in* PG$(2, 5)$.

Proof. Let $\mathcal{S}$ be a set without tangents of size 10 in PG$(2, 5)$. There is no 6-secant of $\mathcal{S}$, since otherwise the number of points in $\mathcal{S}$ would be at least 11. If $\mathcal{S}$ has a 5-secant, then by Remark 8, $\mathcal{S}$ is trivial. So now assume that $\mathcal{S}$ has no 5-secants. Let x_i be the number of lines that meet $\mathcal{S}$ in i points. Note that by definition, $x_1 = 0$. We count the number of lines in PG$(2, 5)$, the number of couples (P, L) where L is a line through the point P of $\mathcal{S}$, and the number of triples (P_1, P_2, L), where L is a line through the points P_1 and P_2 of $\mathcal{S}$. This yields

$$x_0 + x_2 + x_3 + x_4 = 31$$
$$2x_2 + 3x_3 + 4x_4 = 60$$
$$2x_2 + 6x_3 + 12x_4 = 90.$$

It is easy to check that there are only 2 solutions (x_0, x_2, x_3, x_4) for this system of equations with $x_i \in \mathbb{N}$; they are $(5, 21, 2, 3)$ and $(6, 15, 10, 0)$. Let us assume that we have $x_0 = 5, x_2 = 21, x_3 = 2$, and that $x_4 = 3$. Let L_1, L_2, L_3 be the 4-secants of $\mathcal{S}$. If two of these lines, say L_1 and L_2 meet in a point P of $\mathcal{S}$, then there are 4 other lines through P that have to contain a point of $\mathcal{S}$, so $|\mathcal{S}| \geq 11$. Hence, L_1 and L_2 meet in a point Q, not in $\mathcal{S}$. The points P_1, P_2, P_3, P_4 on L_3 all have to be different from the points of $\mathcal{S}$ in L_1 and L_2, which forces $\mathcal{S}$ to have at least 12 points, a contradiction.

We conclude that $x_0 = 6, x_2 = 15, x_3 = 10, x_4 = 0$. Let $L_1, \ldots, L_6$ be the 6 lines, skew to $\mathcal{S}$. If three of the lines $L_1, \ldots, L_6$ are concurrent in a point Q, then the 10 points of $\mathcal{S}$ have to lie on the three remaining lines through Q. Hence, there is a line through Q with at least 4 points of $\mathcal{S}$ which is a contradiction. This implies that $L_1, \ldots, L_6$ forms a dual $(q+1)$-arc, and thus, by Theorem 2, a dual conic. Since there are $6.7/2 = 21$ points of PG$(2, 5)$ that lie on one of the lines of $\{L_1, \ldots, L_6\}$, the 10 points of $\mathcal{S}$ are the 31–21 points, not on one of those lines. The complement of the points on a dual conic, is clearly the set of interior points of that conic. Lemma 13 shows that the set of interior points of a conic is a set without tangents, and since all conics in PG$(2, q)$, q odd, are projectively equivalent (see Lemma 3(1)), all sets of interior points to a conic are projectively equivalent. It is easy to see that the 10 points of a Desargues configuration form a set without tangents in PG$(2, 5)$. The statement follows by noticing that this set is not the trivial set without tangents, since no line meets the points of a Desargues configuration in 4 points. □

3. Exterior sets in PG$(2, q)$

If $q = 7$ and $q = 11$, there are examples of a set without tangents of size 12 and 18 respectively, obtained in the following way: take the $q+1$ points of an irreducible conic, together with $(q+1)/2$ exterior points, no. 3 on a line, forming an exterior set (see [4]). This construction was the starting point of the investigation of exterior sets of a conic. In the same paper, Blokhuis et al. conjecture that if $q > 31$, there are no exterior sets consisting of $(q+1)/2$ non-collinear exterior points in PG$(2, q)$, and they found by computer that for $11 < q \leq 31$, all exterior sets consisting of $(q+1)/2$ exterior points contain a line with at least 3 points of this set. Hence, the cases $q = 7$ and $q = 11$ are conjectured to be the only cases for which a conic $\mathcal{C}$ and $(q+1)/2$ exterior points of $\mathcal{C}$ form a set without tangents.

We now give a third point of view on the non-trivial set without tangents of size 10 in PG(2, 5). Let $\mathcal{C}$ be a conic in PG(2, 5) and let L be an external line of $\mathcal{C}$. Let P_1, P_2, P_3 be the exterior points on L, and denote the external line, different from L, through P_i by M_i, $i = 1, 2, 3$. It turns out (as we will see in this section) that M_1, M_2, M_3 are concurrent, say in Q. From this, it easily follows that the points of $\mathcal{C}$, together with P_1, P_2, P_3, and Q form a set without tangents of size 10.

In this section, we check whether we can extend this example to a construction of a non-trivial set without tangents of size $2q$ for other values of q. For this, as a first step, we need to find a point Q such that Q together with the exterior points on an external line L is an exterior set. As we will see, if $q = 3 \bmod 4$, this point Q is always contained in the line L, and hence, we can never get a set without tangents in this way. If $q = 1 \bmod 4$ on the other hand, there is a unique point Q satisfying the required condition, not contained in L. It follows that we cannot extend this set with other points to find a set without tangents of size $2q$ if $q > 5$.

Theorem 15. *Let $\mathcal{C}$ be an irreducible conic in* PG(2, q) *and let L be an external line of $\mathcal{C}$. Let $\mathcal{S}$ be the set of $(q+1)/2$ exterior points on L. If $q = 3 \bmod 4$, then each point Q such that $\mathcal{S} \cup \{Q\}$ is an exterior set, lies on L. If $q = 1 \bmod 4$, there is a unique point Q, not on L, such that $\mathcal{S} \cup \{Q\}$ is an exterior set.*

Proof. By Lemma 3(1), we may fix $\mathcal{C}$ to be the points $\langle (X, Y, Z)\rangle$ satisfying the equation $Y^2 = XZ$. A line with equation $Z = aX$ is external if and only if $Y^2 = aX^2$ has no non-zero solution, hence, if and only if a is a non-square in $\mathbb{F}_q$. By Lemma 3(2), we may fix an external line L to be the line with equation $Z = aX$, where a is a fixed non-square in $\mathbb{F}_q$.

The tangent lines of $\mathcal{C}$ are the line $X = 0$, together with the lines with equation $\mu^2 X - 2\mu Y + Z = 0$, where $\mu \in \mathbb{F}_q$. The point $P = \langle (0, 1, 0)\rangle$ lies on L and on the line $X = 0$, hence, it is an exterior point of $\mathcal{C}$. The points on L, different from P, have the form $\langle (1, \xi, a)\rangle$, for some $\xi \in \mathbb{F}_q$. Such a point is exterior if and only if it lies on one of the tangent lines of $\mathcal{C}$, hence, if and only if the equation $\mu^2 - 2\xi\mu + a = 0$ has a solution, which is the case if and only if $\xi^2 - a$ is a square.

The lines through P have equation $Z = \lambda X$, and, as before, we see that this line is an external line of $\mathcal{C}$ if and only if λ is a non-square. A point Q on the line $Z = \lambda X$ has coordinates $\langle (1, \alpha, \lambda)\rangle$.

The point Q extends $\mathcal{S}$ to an exterior set if and only if the lines connecting Q with the points of $\mathcal{S}$ are external lines. It is clear that if Q is a point on $L \setminus \mathcal{S}$, we find such a set. Hence, we assume that Q does not lie on L, so $\lambda \neq a$.

The line M through $\langle (1, \alpha, \lambda)\rangle$ and $\langle (1, \xi, a)\rangle$ has equation

$$(\alpha a - \xi\lambda)X + (\lambda - a)Y + (\xi - \alpha)Z = 0.$$

We see that the line M is external if and only if $(\lambda - a)^2 - 4(\alpha a - \xi\lambda)(\xi - \alpha)$ is a non-square.

Suppose there exists a point $Q = \langle (1, \alpha, \lambda)\rangle$, not on L extending the set $\mathcal{S}$ to an exterior set, (hence $\lambda \neq a$ is a non-square). Then, for all ξ with $\xi^2 - a$ a square $(*)$, it holds that $(\lambda - a)^2 - 4(\xi - \alpha)(\alpha a - \xi\lambda)$ is a non-square $(**)$. Since $(*)$ is satisfied if and only if the point $\langle (1, \xi, a)\rangle$ is an exterior point on L, and there are $(q+1)/2$ exterior points on L, and $\langle (0, 1, 0)\rangle$ is one of them, the number of elements ξ for which $(*)$ holds is $(q-1)/2$. The condition $(**)$ is satisfied if and only if the line connecting $\langle (1, \alpha, \lambda)\rangle$ with $\langle (1, \xi, a)\rangle$ is an external line. A point $\langle (1, \alpha, \lambda)\rangle$ lies on at most $(q+1)/2$ external lines, of which the line $Z = \lambda X$, through $\langle (0, 1, 0)\rangle$ is one. Hence, at most $(q-1)/2$ elements of $\mathbb{F}_q$ satisfy condition $(**)$, and from our assumption, we get that the $(q-1)/2$ elements of $\mathbb{F}_q$ satisfying condition $(*)$ are exactly those for which $(**)$ holds. If x is an element of $\mathbb{F}_q$ for which $(*)$ holds, then also $-x$ satisfies $(*)$ and if y is an element of $\mathbb{F}_q$ for which $(**)$ holds, then $\frac{\alpha(a+\lambda)}{\lambda} - y$ also satisfies $(**)$. Since the elements satisfying $(*)$ and $(**)$ are the same, we get that the (not necessarily distinct) values

$$\begin{array}{llll} x, & -x & & \\ \dfrac{\alpha(a+\lambda)}{\lambda} - x, & & x - \dfrac{\alpha(a+\lambda)}{\lambda}, & \\ \dfrac{2\alpha(a+\lambda)}{\lambda} - x, & & x - \dfrac{2\alpha(a+\lambda)}{\lambda}, & \\ \dfrac{3\alpha(a+\lambda)}{\lambda} - x, & & x - \dfrac{3\alpha(a+\lambda)}{\lambda}, & \ldots, \\ \dfrac{(p-1)\alpha(a+\lambda)}{\lambda} - x, & & x - \dfrac{(p-1)\alpha(a+\lambda)}{\lambda} & \end{array}$$

are satisfying $(*)$. Suppose that two of the above $2p$ values coincide, then either $x = 0$ or $\frac{\alpha(a+\lambda)}{\lambda} = 0$. If $x = 0$ and $\frac{\alpha(a+\lambda)}{\lambda} \neq 0$, the number of different values is p. The above argument holds for every solution x of $(*)$. Hence, if $\frac{\alpha(a+\lambda)}{\lambda} \neq 0$, the number of different values for which $(*)$ holds is a multiple of p, but $(p^h - 1)/2$ is not a multiple of p which is a contradiction. We conclude that $\frac{\alpha(a+\lambda)}{\lambda} = 0$, so either $\alpha = 0$ or $\lambda = -a$.

First assume that $q = 3 \bmod 4$, then -1 is a non-square. This implies that $-a$ is a square, so if $\lambda = -a$, λ is a non-square, and we obtain a contradiction. If $\alpha = 0$ then the line $Y = 0$ through $\langle (1, 0, \lambda)\rangle$ and the exterior point $\langle (1, 0, a)\rangle$ on L meets $\mathcal{C}$ in $\langle (1, 0, 0)\rangle$ and $\langle (0, 0, 1)\rangle$, hence it is not an external line. This proves the theorem in the case that $q = 3 \bmod 4$.

If $q = 1 \bmod 4$, then -1 is a square. First note that $Q = \langle (1, 0, -a)\rangle$ extends $\mathcal{S}$ to a larger exterior set since $\xi^2 - a$ is a square if and only if $4a(a - \xi^2)$ is a non-square. We will now show that the point $Q = \langle (1, 0, -a)\rangle$ is the unique point satisfying this condition. By the previous argument, we only need to check the points of the form $\langle (1, \alpha, -a)\rangle$ and $\langle (1, 0, \lambda)\rangle$.

Suppose that the point $Q = \langle(1, \alpha, -a)\rangle$, with $\alpha \neq 0$ extends $\mathcal{S}$ to a larger exterior set. Then $\xi^2 - a$ is a square if and only if $4a(a - \xi^2 + \alpha^2)$ is a non-square, hence, if and only if $(\xi^2 - a - \alpha^2)$ is a square. It also follows that $\xi^2 - a$ is a non-square if and only if $(\xi^2 - a - \alpha^2)$ is a non-square, hence, $(\xi - a)(\xi^2 - a - \alpha^2)$ is always a square. There are $(q + 1)/2$ squares in $\mathbb{F}_q$, so there are $(q + 1)/2$ values x for which $\xi^2 - a = x$. We claim that $X(X - \alpha^2) = \nu Z^2$ $(***)$ with ν a non-square has $(q + 1)/2$ different solutions for X. The number of solutions X to $(***)$ is the number of X's for which $\langle(X, 1, Z)\rangle$ is a solution of $X^2 - \alpha^2 XY - \nu Z^2 = 0$. If $\alpha \neq 0$, the last equation is the equation of an irreducible conic $\mathcal{C}'$, and it is clear that none of the $q + 1$ points on $\mathcal{C}'$ has $Y = 0$, so we may take $Y = 1$. Since a fixed value of X occurs in at most 2 points, there are at least $(q + 1)/2$ different solutions for X. Hence, there is at least one x for which $\xi^2 - a = x$, and $x(x - \alpha^2) = \nu z^2$ for some z, so $(\xi^2 - a)(\xi^2 - a - \alpha^2)$ is a non-square, a contradiction. We conclude that $\alpha = 0$.

Now suppose that the point $Q = \langle(1, 0, \lambda)\rangle$, with $\lambda \neq -a$ extends the set of exterior points on the line L to a larger exterior set, then $\xi^2 - a$ is a square if and only if $(\lambda - a)^2 + 4\lambda\xi^2$ is a non-square and vice versa. Hence, $(\xi^2 - a)((\lambda - a)^2 + 4\lambda\xi^2)$ is a non-square. There are $(q + 1)/2$ different values for $X = \xi^2$, and with a similar argument as before, we get that $(X - a)((\lambda - a)^2 + 4\lambda X) = Z^2$ has $(q + 1)/2$ different solutions for X, since $(X - aY)((\lambda - a)^2 Y + 4\lambda X) = Z^2$ is the equation of an irreducible conic if and only if $\lambda \neq -a$. So we conclude that $\lambda = -a$, which implies that the point $Q = \langle(1, 0, -a)\rangle$ extending $\mathcal{S}$ to a larger exterior set is unique. □

Acknowledgments

The author would like to thank the anonymous referees for their helpful suggestions.

References

[1] S. Ball, The polynomial method in Galois geometries, in: J. De Beule, L. Storme (Eds.), Current Research Topics in Galois Geometry, Nova Sci. Publ. (2011), Chapter.
[2] A. Blokhuis, On the size of a blocking set in PG(2, p), Combinatorica 14 (1994) 111–114.
[3] A. Blokhuis, Á. Seress, H. Wilbrink, On sets of points in PG(2, q) without tangents, Mitt. Math. Sem. Giessen (1991) 39–44.
[4] A. Blokhuis, Á. Seress, H. Wilbrink, Characterization of complete exterior sets of conics, Combinatorica 12 (1992) 143–147.
[5] A. Blokhuis, A. Brouwer, T. Szőnyi, The number of directions determined by a function f on a finite field, J. Combin. Theory Ser. A 70 (2) (1995) 349–353.
[6] N.J. Calkin, J.D. Key, M.J. de Resmini, Minimum weight and dimension formulas for some geometric codes, Des. Codes Cryptogr. 17 (1) (1999) 105–120.
[7] C. Di, D. Proietti, I.E. Telatar, T.J. Richardson, R.L. Urbanke, Finite-length analysis of low-density parity-check codes on the binary erasure channel, IEEE Trans. Inf. Theory 48 (6) (2002) 1570–1579.
[8] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford University Press, Oxford, 1991.
[9] D.R. Hughes, F.C. Piper, Projective Planes, Springer-Verlag, New York, 1973.
[10] N. Kashyap, A. Vardy, Stopping sets in codes from designs, in: IEEE International Symposium on Information Theory, 2003. Proceedings, 2003, p. 122.
[11] Y. Kou, S. Lin, M.P.C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results, IEEE Trans. Inform. Theory 47 (7) (2001) 2711–2736.
[12] M. Lavrauw, L. Storme, G. Van de Voorde, On the code generated by the incidence matrix of points and hyperplanes in PG(n, q) and its dual, Des. Codes Cryptogr. 48 (3) (2008) 231–245.
[13] B. Segre, Sulle ovali nei piani lineari finiti, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. 17 (8) (1954) 141–142.
[14] S. Xia, F. Fu, On the stopping distance of finite geometry LDPC codes, IEEE Commun. Lett. 10 (5) (2006) 381–383.