On the graph of a function in two variables over a finite field

Simeon Ball* and Michel Lavrauw†

Departament de Matemàtica Aplicada IV,
Universitat Politècnica de Catalunya, Jordi Girona 1-3, Mòdul C3, Campus Nord,
08034 Barcelona, Spain
simeon@mat.upc.es, lavrauw@mat.upc.es

5 October 2004

Abstract

We show that if the number of directions not determined by a pointset $\mathcal{W}$ of $\mathrm{AG}(3,q)$, $q=p^h$, of size q^2 is at least $p^e q$ then every plane intersects $\mathcal{W}$ in 0 modulo p^{e+1} points and apply the result to ovoids of the generalised quadrangles $T_2(\mathcal{O})$ and $T_2^*(\mathcal{O})$.

1 Preliminaries

Let $\mathrm{AG}(n,q)$, respectively $\mathrm{PG}(n,q)$, denote the affine, respectively projective, n-dimensional space over the finite field $\mathrm{GF}(q)$ with q elements, where $q=p^h$ for some prime p. Let f be a function from $\mathrm{GF}(q)^2$ to $\mathrm{GF}(q)$ and let

$$\mathcal{W}_f := \{\langle a,b,f(a,b),1\rangle \ : \ a,b \in \mathrm{GF}(q)\},$$

be the set of points corresponding to the graph of the function f in $\mathrm{AG}(3,q)$. Let π be the plane with equation $X_3=0$, and put

$$\mathcal{D}(f) := \{\langle P,Q\rangle \cap \pi \ : \ P,Q \in \mathcal{W}_f, P \neq Q\}.$$

We call $\mathcal{D}(f)$ the *set of directions determined by* f. Often we will only refer to the set of affine points $\mathcal{W}_f$ and talk about the number of directions determined by $\mathcal{W}_f$ instead

*The author acknowledges the support of the Ministerio de Ciencia y Tecnologia, España.

†The author acknowledges the financial support provided through the European Community's Human Potential Programme under contract HPRN-CT-2002-00278, COMBSTRU.

of by f. Note that $|\mathcal{W}_f| = q^2$ and that for any set $\mathcal{W}$ of q^2 affine points in $\mathrm{PG}(3,q)$ one can define a function $f_{\mathcal{W}}$ provided that $\mathcal{W}$ does not determine every direction. The main result of this paper is that if the number of directions not determined by $\mathcal{W}$ is more than q then every plane of $\mathrm{PG}(3,q)$ intersects $\mathcal{W}$ in 0 modulo p points. After the proof of this result, we will prove two more theorems, by refining the hypotheses in one case and for $p = 2$ in the other case. In the last section we consider some consequences for ovoids of the generalised quadrangles $T_2(\mathcal{O})$ and $T_2^*(\mathcal{O})$, where $\mathcal{O}$ is an oval of $\mathrm{PG}(2,q)$.

In contrast to the main result of this article, Storme and Sziklai [8] prove that if the number of directions determined by $\mathcal{W}$ is less than $q(q+3)/2$ then every line is incident with exactly one point of $\mathcal{W}$ or 0 mod p points. If $p > 3$ they prove that $\mathcal{W}$ is $\mathrm{GF}(s)$-linear for some subfield $\mathrm{GF}(s)$ of $\mathrm{GF}(q)$. Their proof uses the main result in [5] which classifies those sets of q points in $\mathrm{AG}(2,q)$ that determine less than half the directions. This problem dates back to Rédei [7, pp. 226], who together with Megyesi solved the prime case, and has now been solved completely, for the most part in [5] and for characteristic two and three in [2]. The restriction $p > 3$ in [8] can been weakened to $p > 2$ as a result of [2].

2 The number of directions

We start with a lemma concerning the number of zeros of a polynomial over a finite field, which we will often refer to in what follows.

Lemma 2.1 *Let S be a subset of $\mathrm{GF}(q)^2$ and $\sigma \in \mathrm{GF}(q)[X,Y]$ be such that $\sigma(aY + b, Y) \equiv 0$, for all $(a,b) \in S$. If $|S| > deg(\sigma)$ then $\sigma(X,Y) \equiv 0$.*

Proof. If $\sigma(aY+b,Y) \equiv 0$ then $\sigma(X,Y) \equiv 0$ modulo $X - aY - b$, and hence

$$X - aY - b \mid \sigma(X,Y).$$

It follows that

$$\prod_{(a,b)\in S} (X - aY - b) \mid \sigma(X,Y).$$

Since the degree of the left hand side is $|S|$ the result follows. ■

Theorem 2.2 *Let $\mathcal{W} \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $q = p^h$, $|\mathcal{W}| = q^2$. If the number of directions not determined by $\mathcal{W}$ is at least q then every plane of $\mathrm{PG}(3,q)$ meets $\mathcal{W}$ in 0 modulo p points.*

Proof. Let π denote the plane $X_3 = 0$ in $\mathrm{PG}(3,q)$, $\mathcal{W}$ be contained in $\mathrm{PG}(3,q)\backslash\pi$, and $\mathcal{D}(\mathcal{W})$ denote the set of directions determined by $\mathcal{W}$. Choose a subset $\mathcal{U} \subset \pi \setminus \mathcal{D}(\mathcal{W})$

of size q. Without loss of generality we may assume that $\mathcal{U} = \{\langle 1, u_i, v_i, 0\rangle : i \in \{1, \ldots, q\}\}$. Consider the Rédei polynomial

$$R(T,X,Y) := \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + aX + bY + c) = \sum_{j=0}^{q^2} \sigma_j(X,Y) T^{q^2-j}.$$

Note that $deg(\sigma_j) \leq j$. Since every line intersecting π in a point of $\mathcal{U}$ contains at most one point of $\mathcal{W}$ and $|\mathcal{W}| = q^2$, every such line must intersect $\mathcal{W}$ in exactly one point. Consider

$$R(T, -u_iY - v_i, Y) = \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + a(-u_iY - v_i) + bY + c)$$

$$= \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + (b - au_i)Y + c - av_i).$$

The number of factors satisfying $b - au_i = r$ and $c - av_i = s$ is equal to the number of points of $\mathcal{W}$ on the line defined by the planes $X_1 - u_iX_0 = rX_3$ and $X_2 - v_iX_0 = sX_3$. Since this line is incident with the point $\langle 1, u_i, v_i, 0\rangle \in \mathcal{U}$, the number of such factors is one. Hence

$$R(T, -u_iY - v_i, Y) = \prod_{(r,s)\in \mathrm{GF}(q)^2} (T + rY + s) = \prod_{r \in \mathrm{GF}(q)} (T^q + rY^q - T - rY)$$

$$= T^{q^2} - ((Y^q - Y)^{q-1} + 1)T^q + (Y^q - Y)^{q-1}T,$$

for all $i \in \{1, \ldots, q\}$. It follows that $\sigma_j(-u_iY - v_i, Y) \equiv 0$ for all $i \in \{1, \ldots, q\}$, $0 < j < q^2 - q$. By the previous lemma, $\sigma_j(X,Y) \equiv 0$ for $0 < j < q$ since $deg(\sigma_j) \leq j$. This implies that

$$R(T,X,Y) = T^{q^2} + \sum_{j=q}^{q^2} \sigma_j(X,Y) T^{q^2-j}.$$

Differentiate the Rédei polynomial with respect to T

$$\frac{\partial R}{\partial T}(T,X,Y) = \sum_{\langle a,b,c,1\rangle \in \mathcal{W}} \frac{1}{(T + aX + bY + c)} R(T,X,Y).$$

Evaluate at $X = x \in \mathrm{GF}(q)$ and $Y = y \in \mathrm{GF}(q)$ and multiply through by $T^q - T$. Then we have a polynomial identity and the divisibility

$$R(T,x,y) \mid (T^q - T)\frac{\partial R}{\partial T}(T,x,y).$$

The left hand side has degree q^2 and the right hand side has degree less than q^2. Hence the right hand side is zero, in particular

$$\frac{\partial R}{\partial T}(T,x,y) \equiv 0,$$

for all $(x,y) \in \mathrm{GF}(q)^2$. This implies that $R(T,x,y)$ is a p-th power, for all $(x,y) \in \mathrm{GF}(q)^2$. It follows that every factor $T-t$, where $t=-ax-by-c$ for some $\langle a,b,c,1\rangle \in \mathcal{W}$ occurs a multiple of p times in $R(T,x,y)$. In other words, every plane with equation

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

$x,y,t \in \mathrm{GF}(q)$, intersects $\mathcal{W}$ in 0 modulo p points. These are all planes of $\mathrm{PG}(3,q)$ except those which have no X_2-term in their defining equation. But if we define the Rédei polynomial as

$$\prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + a + bX + cY),$$

respectively

$$\prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + aX + b + cY),$$

then exactly the same arguments as for $R(T,X,Y)$ can be applied and it follows that every plane of $\mathrm{PG}(3,q)$ intersects $\mathcal{W}$ in 0 modulo p points, except those planes which have no X_0-term, respectively X_1-term, in their defining equation. The only plane belonging to all of the above exceptional planes is the plane $X_3 = 0$, which intersects $\mathcal{W}$ in 0 points. ∎

The following example illustrates that the bound in Theorem 2.2 is sharp.

Example 2.3 *Let π and π' be two planes of $\mathrm{PG}(3,q)$, $q=p^h$, intersecting in the line L. Suppose P is a point of $\pi \setminus L$, Q a point of $\pi' \setminus L$ and R a point on L. Define $\mathcal{W}$ as the set of points on $\pi' \setminus L$ but not on the line $\langle Q,R\rangle$, together with the points on the line $\langle P,Q\rangle$ different from P. Then $\mathcal{W}$ has size q^2, $\mathcal{W}$ determines q^2+2 directions, the points on the line $\langle R,P\rangle \setminus \{R,P\}$ are not determined by $\mathcal{W}$, and not every plane intersects $\mathcal{W}$ in 0 modulo p points.*

In fact we can show that as the number of directions determined by $\mathcal{W}$ becomes smaller, the restriction on the intersection number with planes of $\mathrm{PG}(3,q)$ becomes stronger.

Theorem 2.4 *Let $\mathcal{W} \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $q=p^h$, $|\mathcal{W}| = q^2$. If there are more than $p^e q$ directions not determined by $\mathcal{W}$ for some $e \in \{0,1,2,\ldots,h-1\}$ then every plane of $\mathrm{PG}(3,q)$ meets $\mathcal{W}$ in 0 modulo p^{e+1} points.*

Proof. The case $e=0$ was proven in Theorem 2.2 so assume that $e \geq 1$ and as in the proof of Theorem 2.2 let π denote the plane $X_3=0$ in $\mathrm{PG}(3,q)$, $\mathcal{W}$ be contained in $\mathrm{PG}(3,q) \setminus \pi$, and $\mathcal{D}(\mathcal{W})$ denote the set of directions determined by $\mathcal{W}$. Without loss of generality we may assume that $\langle 0,0,1,0\rangle \in \mathcal{D}(\mathcal{W})$ and by hypothesis there is a set

$\mathcal{U} \subset \pi \setminus \mathcal{D}(\mathcal{W})$ of size $p^e q$. Put $\mathcal{U} = \{\langle 1, u_i, v_i, 0\rangle : i \in \{1, \ldots, p^e q - k\}\} \cup \{\langle 0, 1, t_i, 0\rangle : i \in \{1, \ldots, k\}\}$. Consider the Rédei polynomial

$$R(T, X, Y, Z) := \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + aX + bY + cZ) = \sum_{j=0}^{q^2} \sigma_j(X, Y, Z) T^{q^2 - j}.$$

Repeating the exact same arguments as in the proof of Theorem 2.2 but using the homogeneous polynomials $\sigma_j(X, Y, Z)$ we have that

$$\sigma_j(-u_i Y - v_i Z, Y, Z) \equiv 0,$$

for all i and $0 < j < q^2 - q$. Hence

$$\prod_{i=1}^{p^e q - k} (X + u_i Y + v_i Z) \mid \sigma_j(X, Y, Z)$$

for $0 < j < q^2 - q$. Consider

$$R(T, 1, -t_i Z, Z) = \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + (c - t_i b)Z + a).$$

The number of factors satisfying $c - t_i b = r$ and $a = s$ is equal to the number of points of $\mathcal{W}$ on the line defined by the planes $X_2 - t_i X_1 = r X_3$ and $X_0 = s X_3$. Since this line is incident with the point $\langle 0, 1, t_i, 0\rangle$ the number of such factors is one. Hence

$$R(T, 1, -t_i Z, Z) = \prod_{(r,s) \in \mathrm{GF}(q)^2} (T + rZ + s)$$

$$= T^{q^2} - ((Z^q - Z)^{q-1} + 1)T^q + (Z^q - Z)^{q-1} T,$$

for all $i \in \{1, \ldots, k\}$. It follows that $\sigma_j(1, -t_i Z, Z) \equiv 0$ for all $i \in \{1, \ldots, k\}$ and $0 < j < q^2 - q$. As in lemma 2.1

$$\prod_{i=1}^{k} (Y + t_i Z) \mid \sigma_j(X, Y, Z)$$

and so

$$\prod_{i=1}^{k} (Y + t_i Z) \prod_{i=1}^{p^e q - k} (X + u_i Y + v_i Z) \mid \sigma_j(X, Y, Z)$$

for $0 < j < q^2 - q$. Now if $j < p^e q$ then the degree of $\sigma_j(X, Y, Z)$ is less than $p^e q$ and so $\sigma_j(X, Y, Z) \equiv 0$. Therefore

$$R(T, X, Y, 1) = T^{q^2} + \sum_{j=p^e q}^{q^2} \sigma_j(X, Y, 1) T^{q^2 - j}.$$

and we can follow the proof of Theorem 2.2 and conclude that $R(T,x,y,1)$ is a p-th power, for all $(x,y) \in \mathrm{GF}(q)^2$. Now fix an $(x,y) \in \mathrm{GF}(q)^2$ and take the p-th root of $R(T,x,y,1)$, i.e.,

$$R_1(T) := R(T,x,y,1)^{1/p} = T^{q^2/p} + G(T),$$

for some $G \in \mathrm{GF}(q)[T]$, with $deg(G) \leq (q^2 - p^e q)/p$. Again as in the proof of Theorem 2.2 we have that

$$R_1(T) \mid (T^q - T)\frac{\partial R_1}{\partial T}(T).$$

The left hand side has degree q^2/p and the right hand side has degree at most $q^2/p + q - p^e q/p - 2 < q^2/p$. Hence the right hand side is zero, in particular

$$\frac{\partial R_1}{\partial T}(T) \equiv 0.$$

This implies that $R_1(T)$ is a p-th power and $R(T,x,y,1)$ is a p^2-th power for all $(x,y) \in \mathrm{GF}(q)^2$. We can continue this process by defining $R_l(T)$ as the p^l-th root of $R(T,x,y)$ for any fixed $(x,y) \in \mathrm{GF}(q)^2$, consider the divisibility

$$R_l(T) \mid (T^q - T)\frac{\partial R_l}{\partial T}(T),$$

and obtain that $R_l(T)$ is a p-th power, as long as the degree of the right hand side is less than q^2/p^l. This is the case as long as $l < e+1$, which implies that $R(T,x,y,1)$ is a p^{e+1}-th power, for all $(x,y) \in \mathrm{GF}(q)^2$. It follows that every factor $T - t$, where $t = -ax - by - c$ for some $\langle a,b,c,1\rangle \in \mathcal{W}$, occurs a multiple of p^{e+1} times in $R(T,x,y,1)$. In other words, every plane with equation

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

$x,y,t \in \mathrm{GF}(q)$, intersects $\mathcal{W}$ in 0 modulo p^{e+1} points. These are all planes of $\mathrm{PG}(3,q)$ except those which have no X_2-term in their defining equation. However we can redefine the Rédei polynomial as in Theorem 2.2, by permuting the coordinates, and conclude that all planes intersect $\mathcal{W}$ in 0 modulo p^{e+1} points. ■

The following theorem says we can deduce more in the case when q is even.

Theorem 2.5 *Let $\mathcal{W} \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $q = 2^h$, $|\mathcal{W}| = q^2$. Suppose that there are at least $2^e q$ directions not determined by $\mathcal{W}$ for some $e \in \{0,1,\ldots,h-1\}$. Then two parallel planes intersect $\mathcal{W}$ in the same number of points modulo 2^{e+2}.*

Proof. Put $\pi := \mathrm{PG}(3,q) \setminus \mathrm{AG}(3,q)$ and suppose that π_1 and π_2 are two parallel planes intersecting π in the same line determined by the equations $X_3 = 0$ and $xX_0 + yX_1 + X_2 = 0$ for some $x,y \in \mathrm{GF}(q)$. We assume that the planes π_1 and π_2 do not contain the point $\langle 0,0,1,0\rangle$, but as before we can permutate the coordinates and consider planes that do not contain the point $\langle 1,0,0,0\rangle$ and the point $\langle 0,1,0,0\rangle$. Let

$$\pi_1 : xX_0 + yX_1 + X_2 + t_1X_3 = 0$$

and

$$\pi_2 : xX_0 + yX_1 + X_2 + t_2X_3 = 0.$$

Theorem 2.4 implies that planes intersect $\mathcal{W}$ in zero modulo 2^{e+1} points.

Suppose π_1 intersects $\mathcal{W}$ in 2^{e+1} mod 2^{e+2} points. Then, as in the proof of Theorem 2.4, it follows that t_1 is a root of $R(T,x,y,1)$, where $R(T,X,Y,Z)$ is the Rédei polynomial corresponding to $\mathcal{W}$, of multiplicity 2^{e+1} mod 2^{e+2}, and we obtain $R(T,x,y,1) \in \mathrm{GF}(q)[T^{2^{e+1}}] \setminus \mathrm{GF}(q)[T^{2^{e+2}}]$. We will show that also π_2 intersects $\mathcal{W}$ in 2^{e+1} mod 2^{e+2} points. We may write

$$R(T,x,y,1)^{1/2^{e+1}} = T^{q^2/2^{e+1}} + g(T),$$

where $g \in \mathrm{GF}(q)[T]$ is of degree at most $q^2/2^{e+1} - q/2$ and $g'(T)$ is not identically zero. The product of the distinct linear factors of $R(T,x,y,1)^{1/2^{e+1}}$ divides $T^q + T$ and the repeated factors divide its derivative, hence

$$T^{q^2/2^{e+1}} + g(T) \mid (T^q + T)g'(T).$$

The degree of the quotient $m(T)$ is at most $q/2 - 2$ and differentiating the identity

$$(T^{q^2/2^{e+1}} + g(T))m(T) = (T^q + T)g'(T),$$

we get

$$T^{q^2/2^{e+1}}m'(T) + (g(T)m(T))' = g'(T).$$

The degree of $g(T)m(T)$ is at most $q^2/2^{e+1} - 2$ so we must have that $m'(T) = 0$. The last equation then becomes $m(T)g'(T) = g'(T)$ and hence $m(T) = 1$. Therefore

$$R(T,x,y,1) = (T^q + T)^{2^{e+1}} h(T)^{2^{e+2}},$$

where $h(T)^2 = g'(T)$. It follows that every root of $R(T,x,y,1)$, in particular t_2, is a root with multiplicity 2^{e+1} mod 2^{e+2}, which implies that π_2 intersects $\mathcal{W}$ in 2^{e+1} mod 2^{e+2} points. We have shown that the number of points in the intersection of a plane with $\mathcal{W}$ modulo 2^{e+2} only depends on the plane's intersection with π. ■

3 Ovoids of the generalised quadrangles $T_2(\mathcal{O})$ and $T_2^*(\mathcal{O})$

Let $\mathcal{O}$ be an oval in $\mathrm{PG}(2,q) \subset \mathrm{PG}(3,q)$, i.e., a set of $q+1$ points no three collinear, where $q = p^h$. Consider the following incidence structure $T_2(\mathcal{O})$. We define three types of points: (i) the points of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$; (ii) The planes of $\mathrm{PG}(3,q)$ which meet $\mathrm{PG}(2,q)$ in a tangent line to $\mathcal{O}$; (iii) a point (∞). We define two type of lines:

(a) the points of $\mathcal{O}$; (b) the lines of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$ which meet $\mathrm{PG}(2,q)$ in a point of $\mathcal{O}$. Incidence is symmetric containment in $\mathrm{PG}(3,q)$ and the point (∞) is incident with every line of type (a). The incidence structure $T_2(\mathcal{O})$ is a generalised quadrangle of order q, see [6, 3.1.2]. An *ovoid* Ω of a generalised quadrangle $\mathcal{S}$ is a set of points of $\mathcal{S}$ such that every line of $\mathcal{S}$ is incident with exactly one point of Ω. If the generalised quadrangle $\mathcal{S}$ has order (s,t) then an ovoid of $\mathcal{S}$ has $st+1$ points, again see [6]. Theorem 2.2 and Theorem 2.5 have the following immediate corollary.

Corollary 3.1 *If Ω is an ovoid of $T_2(\mathcal{O})$ containing the point (∞), then every plane of $\mathrm{PG}(3,q)$ meets Ω in zero modulo p points. Moreover if q is even, two planes meeting $\mathrm{PG}(3,q) \setminus \mathrm{AG}(3,q)$ in the same line intersect Ω either both in 0 modulo 4 points or both in 2 modulo 4 points.*

Proof. Note that an ovoid of $T_2(\mathcal{O})$ contains q^2+1 points. The fact that no two points of $\mathcal{W} := \Omega \setminus \{(\infty)\}$ are collinear means that the points of $\mathcal{O}$ are not contained in the set of directions determined by $\mathcal{W}$. Since $|\mathcal{W}| = q^2$ and $|\mathcal{O}| = q+1$, we can apply Theorem 2.2 and the first part of the corollary follows. The second part of the corollary follows directly from Theorem 2.5. ■

If q is even then the oval $\mathcal{O}$ has a nucleus N, i.e., a point which is incident with every tangent line to $\mathcal{O}$. Consider the following incidence structure $T_2^*(\mathcal{O})$. The points are the points of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$, the lines are the lines of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$ which meet $\mathrm{PG}(2,q)$ in a point of $\mathcal{O} \cup \{N\}$, and incidence is that inherited from $\mathrm{PG}(3,q)$. $T_2^*(\mathcal{O})$ is a generalised quadrangle of order $(q-1,q+1)$, see [6, 3.1.3]. Again we can apply Theorem 2.2 and Theorem 2.5 to obtain the following corollary for ovoids of $T_2^*(\mathcal{O})$.

Corollary 3.2 *If Ω is an ovoid of $T_2^*(\mathcal{O})$, then every plane of $\mathrm{PG}(3,q)$ meets Ω in an even number of points. Moreover two planes meeting $\mathrm{PG}(3,q) \setminus \mathrm{AG}(3,q)$ in the same line intersect Ω either both in 0 modulo 4 points or both in 2 modulo 4 points.*

Proof. Note that an ovoid of $T_2^*(\mathcal{O})$ has $(q-1)(q+1)+1 = q^2$ points. The fact that no two points of $\mathcal{W} := \Omega$ are collinear implies that the points of $\mathcal{O} \cup \{N\}$ are not contained in the set of directions determined by $\mathcal{W}$. Since $|\mathcal{W}| = q^2$ and $|\mathcal{O} \cup \{N\}| = q+2$, we can apply Theorem 2.2 and the first part of the corollary follows. The second part of the corollary follows directly from Theorem 2.5. ■

Motivated by the desire to know the possible intersection numbers that planes have with an ovoid of $T_2(\mathcal{O})$, where (∞) is not a point of the ovoid we prove the following theorem which would seem artificial were it not for the immediate corollary.

Theorem 3.3 *Let $\mathcal{W} \subset \mathrm{AG}(3,q) \subset \mathrm{PG}(3,q)$, $q = p^h$, be a set of $q^2 - q$ points that does not determine a set of directions $\mathcal{U} \subset \pi \setminus \mathcal{D}(\mathcal{W})$, where $\pi := \mathrm{PG}(3,q) \setminus \mathrm{AG}(3,q)$, which has the property that for each point $P \in \mathcal{U}$ the q affine lines incident with P but skew from $\mathcal{W}$ are coplanar.*

(i) If $|\mathcal{U}| \geq q-1$ then two planes that meet π in the same line are either both incident with a point of $\mathcal{W}$ or they are both incident with 0 modulo p points of $\mathcal{W}$.

(ii) If $\mathcal{U}$ is of size q and has the property that the skew planes are incident with a common point Q of π then every plane not incident with Q is incident with a point of $\mathcal{W}$ and those incident with Q are incident with 0 modulo p points of $\mathcal{W}$. Moreover if q is even then every plane not incident with Q is incident with an odd number of points of $\mathcal{W}$.

Proof. As before let π denote the plane $X_3 = 0$ in $\mathrm{PG}(3,q)$, $\mathcal{W}$ be contained in $\mathrm{PG}(3,q) \setminus \pi$, and $\mathcal{D}(\mathcal{W})$ denote the set of directions determined by $\mathcal{W}$. Choose a subset $\mathcal{U} \subset \pi \setminus \mathcal{D}(\mathcal{W})$ of size $q-1$. Without loss of generality we may assume that $\mathcal{U} = \{\langle 1, u_i, v_i, 0\rangle : i \in \{1, \dots, q-1\}\}$. Define the Rédei polynomial

$$R(T,X,Y) := \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + aX + bY + c) = \sum_{j=0}^{q^2-q} \sigma_j(X,Y) T^{q^2-q-j}.$$

Consider

$$R(T, -u_iY - v_i, Y) = \prod_{\langle a,b,c,1\rangle \in \mathcal{W}} (T + (b - au_i)Y + c - av_i).$$

The number of factors satisfying $b - au_i = r$ and $c - av_i = s$ is equal to the number of points of $\mathcal{W}$ on the line defined by the planes $X_1 - u_iX_0 = rX_3$ and $X_2 - v_iX_0 = sX_3$. Since this line is incident with the point $\langle 1, u_i, v_i, 0\rangle \in \mathcal{U}$, the number of such factors is one unless the line is contained in the plane π_i skew to $\mathcal{W}$ at $\langle 1, u_i, v_i, 0\rangle$. There is a point on the line $X_3 = X_0 = 0$ that is not incident with any π_i and without loss of generality we may assume that this point is $\langle 0,0,1,0\rangle$. So for some α_i, β_i the skew plane π_i at $\langle 1, u_i, v_i, 0\rangle$ is defined by the equation

$$-(v_i + \beta_i u_i)X_0 + \beta_i X_1 + X_2 + \alpha_i X_3 = 0.$$

This plane contains the line defined by the equations $X_1 - u_iX_0 = rX_3$ and $X_2 - v_iX_0 = sX_3$ if and only if $s = -(\alpha_i + \beta_i r)$. Hence

$$R(T, -u_iY - v_i, Y) = \prod_{(r,s)\in \mathrm{GF}(q)^2} (T + rY + s) / \prod_{r \in \mathrm{GF}(q)} (T + rY - (\alpha_i + \beta_i r)),$$

$$= [T^{q^2} - ((Y^q - Y)^{q-1} + 1)T^q + (Y^q - Y)^{q-1}T]/[T^q - (Y - \beta_i)^{q-1}T - \alpha_i],$$

for all $i \in \{1, 2, \ldots, q-1\}$. The second highest degree term in T on the right hand side is of degree $q^2 - 2q + 1$ so $\sigma_j(-u_iY - v_i, Y) \equiv 0$ for all $j \in \{1, 2, \ldots, q-2\}$ and $i \in \{1, 2, \ldots, q-1\}$. By Lemma 2.1 the polynomials $\sigma_j(X, Y) \equiv 0$ for all $j \in \{1, 2, \ldots, q-2\}$. So

$$R(T, X, Y) = T^{q^2-q} + \sum_{j=q-1}^{q^2-q} \sigma_j(X, Y) T^{q^2-q-j}.$$

As in the previous theorems for all $x, y \in \mathrm{GF}(q)$ we have the divisibility

$$R(T, x, y) \mid (T^q - T) \frac{\partial R}{\partial T}(T, x, y).$$

The left hand side has degree $q^2 - q$ and the right hand side has degree less than or equal to $q^2 - q$. The leading coefficient on the right hand side is $\sigma_{q-1}(x, y)$.

If $\sigma_{q-1}(x, y)$ is zero then the right hand side has degree less than the left hand side and is identically zero. In this case

$$\frac{\partial R}{\partial T}(T, x, y) \equiv 0,$$

and $R(T, x, y)$ is a p-th power and it follows that every factor $T - t$, where $t = -ax - by - c$ for some $\langle a, b, c, 1\rangle \in \mathcal{W}$ occurs a multiple of p times in $R(T, x, y)$. In other words, every plane with equation

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

$x, y, t \in \mathrm{GF}(q)$, intersects $\mathcal{W}$ in 0 modulo p points. These are the planes sharing the common line of π defined by the equations $X_3 = 0$ and $xX_0 + yX_1 + X_2 = 0$.

If $\sigma_{q-1}(x, y)$ is not zero then we have the equality

$$R(T, x, y) = \sigma_{q-1}(x, y)^{-1} (T^q - T) \frac{\partial R}{\partial T}(T, x, y).$$

and it follows that every factor $T - t$, where $t = -ax - by - c$ for some $\langle a, b, c, 1\rangle \in \mathcal{W}$ occurs at least once in $R(T, x, y)$. In other words, every plane with equation

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

$x, y, t \in \mathrm{GF}(q)$, intersects $\mathcal{W}$ in at least a point. Again these planes share the common line of π defined by the equations $X_3 = 0$ and $xX_0 + yX_1 + X_2 = 0$ and so we have proved the first part of the theorem for all lines which have an X_2 term in their defining equation. As in the previous theorems, redefining the Rédei polynomial by permuting the coordinates and going through the same arguments suffices for lines of π defined by equations of the form $xX_0 + X_1 + yX_2 = 0$ and $X_0 + xX_1 + yX_2 = 0$.

By hypothesis in the final part of the theorem we have a subset of $\mathcal{U} \subset \pi \setminus \mathcal{D}(\mathcal{W})$ of size q with the property that the planes skew to $\mathcal{W}$ are incident with a common point Q of π. Then every plane not incident with Q is incident with a point of $\mathcal{W}$. Without loss of generality let Q be the point $\langle 0,1,0,0\rangle$ and apply a collineation that fixes Q and maps the line $X_0 = 0$ skew to $\mathcal{U}$. Following the proof as in part (i), but with $\beta_i = 0$ for all $i \in \{1, 2, \ldots, q\}$ we have

$$R(T, -u_iY - v_i, Y) = (T^{q^2} - ((Y^q - Y)^{q-1} + 1)T^q + (Y^q - Y)^{q-1}T)/(T^q - Y^{q-1}T - \alpha_i),$$

for all $i \in \{1, 2, \ldots, q\}$. Hence $\sigma_{q-1}(-u_iY - v_i, Y) \equiv Y^{q-1}$ and by Lemma 2.1 $\sigma_{q-1}(X, Y) - Y^{q-1} \equiv 0$. Continuing along the arguments as before we now have that if $y \neq 0$ then the every plane with equation

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

$x, t \in \mathrm{GF}(q)$, intersects $\mathcal{W}$ in at least a point and if $y = 0$ then the planes defined by an equation of the form

$$xX_0 + X_2 + tX_3 = 0,$$

those incident with Q, intersect $\mathcal{W}$ in 0 modulo p points. Moreover, if q is even and $y \neq 0$ then

$$R(T, x, y) = \sigma_{q-1}(x, y)^{-1}(T^q - T)\frac{\partial R}{\partial T}(T, x, y).$$

Since $\frac{\partial R}{\partial T}(T, x, y)$ is a square in T every factor $T - t$ occurs an odd number of times and the planes defined by an equation of the form

$$xX_0 + yX_1 + X_2 + tX_3 = 0$$

intersect $\mathcal{W}$ in an odd number of points. ■

Corollary 3.4 *Let Ω be an ovoid of $T_2(\mathcal{O})$ that does not contain the point (∞). Every plane of $PG(3, q)$ that is not incident with a point of $\mathcal{O}$ is incident with 1 modulo p points of Ω.*

Proof. If q is even then all the hypotheses of Theorem 3.3 are satisfied and we can apply the last part of the theorem to obtain the corollary. If q is odd then $\mathcal{O}$ is a conic and $T_2(\mathcal{O})$ is isomorphic to $Q(4, q)$. The planes of $PG(3, q)$ that are not incident with a point of $\mathcal{O}$ correspond to elliptic quadrics in the $Q(4, q)$ model. Corollary 3.1 implies that elliptic quadrics are incident with no points of an ovoid of $Q(4, q)$ or 1 modulo p points. However Theorem 3.3 shows that the planes containing the line $\pi' \cap \pi$. where π' is a plane skew to the ovoid, are all skew to the ovoid, which is clearly nonsense. Hence an elliptic quadric is incident with 1 modulo p points of an ovoid of $Q(4, q)$.
■

In the case when q is odd, the previous corollary was first proven in [3]. It was proven again in [4] where it was also shown that ovoids of $Q(4, p)$, p prime, are elliptic quadrics.

In the case where q is even and $\mathcal{O}$ is a conic, so $T_2(\mathcal{O})$ is isomorphic to $Q(4,q)$, the previous corollary was first proven by Bagchi and Sastry [1]. Moreover it was shown in [4] that every elliptic quadric is either incident with 1 modulo 4 points of an ovoid of $Q(4,q)$ or every elliptic quadric is incident with 3 modulo 4 points of an ovoid of $Q(4,q)$.

References

[1] B. Bagchi and N. S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes, *Geom. Dedicata*, **22** (1987) 137–147.

[2] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, **104** (2003) 341–350.

[3] S. Ball, On ovoids of $O(5,q)$, *Adv. Geom.*, **4** (2004) 1–7.

[4] S. Ball, P. Govaerts and L. Storme, On ovoids of parabolic quadrics, submitted.

[5] A. Blokhuis, S. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes of the graph of a function defined over a finite field, *J. Combin. Theory Ser. A*, **86** (1999) 187–196.

[6] S. E. Payne, J. A. Thas, *Finite generalized quadrangles*. Research Notes in Mathematics, 110. Pitman (Advanced Publishing Program), Boston, MA, 1984. vi+312 pp. ISBN 0-273-08655-3

[7] L. Rédei, *Lacunary polynomials over finite fields*, North-Holland, Amsterdam, 1973.

[8] L. Storme and P. Sziklai, Linear point sets and Rédei type k-blocking sets in $PG(n,q)$, *J. Algebraic Combin.*, **14** (2001) 221–228.