On the number of slopes of the graph of a function defined on a finite field

A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme and T. Szőnyi

Abstract

Given a set U of size q in an affine plane of order q, we determine the possibilities for the number of directions of secants of U, and in many cases characterize the sets U with given number of secant directions.

1 Introduction and Results

Let $K = GF(q)$ be the finite field with q elements, where $q = p^n$, p prime. Let U be a set of q points in K^2, and let, with $u = (u_1, u_2)$,

$$D = \left\{ \frac{u_2 - v_2}{u_1 - v_1} \;\middle|\; u \neq v,\, u, v \in U \right\} \subseteq K \cup \{\infty\}$$

be the set of directions determined by the set U. Rédei [4] proves the following bounds for the size N of D: Either $N \geq (q+1)/2$ or $(q+p^e)/(p^e+1) \leq N \leq (q-1)/(p^e-1)$ for some integer $e \leq n/2$, or $N = 1$. In [2] his proof was simplified and the results were improved. It was conjectured that the truth is that $N \geq (q+3)/2$ or $q/p^e + 1 \leq N \leq (q-1)/(p^e-1)$ for some divisor e of n, or $N = 1$. The aim of this note is to prove this and to determine the sets U with $N < (q+3)/2$.

The problem has been studied in recent years by several people, independently of each other, using different points of view. The geometric point of view asks for the number of difference quotients $(f(x)-f(y))/(x-y)$ that can occur for a function $f \in GF(q)[X]$ [4, 2]. The permutation polynomial point of view asks for the possible numbers of $c \in GF(q)$ such that $f(X) + cX$ is a permutation polynomial [3]. Since $f(X)+cX$ is a permutation polynomial precisely if $-c$ does not occur as a difference quotient the problems are exactly complementary. Our original motivation to study this problem lies in its connection to blocking sets. For a recent survey see [1].

K^2 may be mapped to $L = GF(q^2)$ by $(a, b) \mapsto \alpha a + \beta b$, for arbitrary α, $\beta \in L^*$ with $\alpha/\beta \notin K$. If F is a subfield of K, then K and hence also L is a vector space over F. A subset V of K^2 will be called F-linear, if it is mapped in this way to a F-subspace of L. It is easy to check that this property is well-defined, that is, it is independent of the choice of α and β defining the mapping.

Theorem 1.1 *Let $U \subset K^2$ be a point set of size q containing the origin, let D be the set of slopes of secants of U, and put $N := |D|$. Let e (with $0 \leq e \leq n$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then we have one of the following:*

(i) $e = 0$ *and* $(q+3)/2 \leq N \leq q+1$,

(ii) $e = 1$, $p = 2$, *and* $(q+5)/3 \leq N \leq q-1$,

(iii) $p^e > 2$, $e \,|\, n$, *and* $q/p^e + 1 \leq N \leq (q-1)/(p^e-1)$,

(iv) $e = n$ *and* $N = 1$.

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3+1$), then U is $GF(p^e)$-linear, and all possibilities for N can be determined explicitly (in principle).

The proof of this theorem will take the rest of this paper.

All bounds given for N are sharp, in the sense that there are examples with equality, except for the lower bound in case (ii), where one might hope for $N \geq q/2+1$; indeed, this holds for $q \leq 16$. The conclusion that U is p^e-linear is probably also true for p^e equal to 2 or 3, but essentially new ideas are necessary to prove this.

2 Lacunary polynomials

We associate to the set U the Rédei polynomial

$$r(X,Y,Z) = \prod_{(u_1,u_2)\in U} (X + u_1 Y - u_2 Z) = \sum_{j=0}^{q} \rho_j(Y,Z) X^j.$$

For $y \in K$, let $r_y(X) := r(X,y,1)$, and let $r_\infty(X) := r(X,1,0)$. Then r_y is a monic polynomial of degree q in X. This polynomial codes the intersection sizes of the lines in direction y with U - indeed, these intersection sizes are the multiplicities of the zeros of r_y. If y is not a secant direction, then we see all possible zeros with multiplicity one:

$$r_y(X) = X^q - X \Leftrightarrow y \notin D.$$

It follows that $\rho_j = 0$ if $1 < j < q$ and $j \geq N$; indeed, we have found $q+1-N$ distinct zeros of the homogeneous polynomial $\rho_j(Y,Z)$ which has degree at most $q-j$.

We use Rédei's notation f° and $f^{\circ\circ}$ for the degree and the second degree of the polynomial f. (The second degree of f is the degree of the polynomial obtained from f by removing its term of highest degree. It is undefined if f is a monomial.)

The above observation means that r_y is lacunary: its second degree (when defined) is much smaller than its degree. Moreover, it factors completely into linear factors (over K). We repeat the main lemma on such polynomials ([4], Satz 18):

Lemma 2.1 *Let s be a power of p, $1 \leq s < q$, and suppose that $f(X) = X^{q/s} + g(X) \in K[X] \setminus K[X^p]$ is fully reducible (over K). Then either $g^\circ \geq (q+s)/s(s+1)$ or $s = 1$ and $f(X) = X^q - X$.*

Proof: A zero of $f(X)$ with multiplicity μ is a zero of f' with multiplicity at least $\mu - 1$, and a zero of $X^q - X$ with multiplicity 1. Hence $f \,|\, (f^s - (X^q - X))f' = (g^s + X)g'$. By assumption g' is nonzero, so either $g^s + X = 0$ and $f(X) = X^q - X$, or the right hand side is nonzero, and $q/s \leq (s+1)g^\circ - 1$. □

Let $s_y \,|\, q$ be such that $r_y \in K[X^{s_y}] \setminus K[X^{ps_y}]$ and let $s = \min_{y\in D} s_y$. Then every line with slope y meets the set U in a multiple of s_y points, and every secant meets U in a multiple of s points. We see that $s = p^e$ in the terminology of the theorem.

Counting the points in U seen from a fixed point $u \in U$ in all possible directions we get:

$$1 + N(s-1) \leq q \quad \text{in other words (for } s > 1\text{):} \quad N \leq \frac{q-1}{s-1},$$

which is precisely the upper bound on N claimed in the theorem.

For a lower bound we use that if y has $s_y = s$, then either $s = q$, $N = 1$, or, by the above lemma (applied to $r_y^{1/s}$), we have $r_y^{\circ\circ} \geq (q+s)/(s+1)$, and $r_j \neq 0$ for $j = r_y^{\circ\circ}$, so that $r_y^{\circ\circ} \leq N-1$ and hence $N \geq 1 + (q+s)/(s+1)$. This proves the lower bounds given in cases (i), (ii) and (iv) of the theorem.

3 A differential equation

Since $r_y^{\circ\circ} \leq N-1$, the upper bound for N implies that $r_y^{\circ\circ} \leq (q-s)/(s-1)$. This allows us to use the following

Lemma 3.1 *Let $f(X) = X^{q/s} + g(X) \in K[X] \setminus K[X^p]$ be fully reducible (over K) with $g^\circ \leq (q-s)/s(s-1)$ if $s \geq 4$, or $g^\circ \leq q/s^2$ if $s = 3$. Then*

$$X^{q/s} + g = (g^s + X)g'.$$

Proof: In the previous section we saw that the left hand side divides the right hand side. So we may write

$$X^{q/s} + g = (g^s + X)g'/m,$$

for some polynomial m of degree

$$m^\circ = sg^\circ + g'^\circ - q/s.$$

Take the derivative and multiply by m^2 to obtain

$$m(m-1)g' = (g^s + X)(mg'' - m'g').$$

If $mg'' - m'g' = 0$ we get $m = 1$, proving the statement. If not, then comparing degrees we get

$$sg^\circ + 3g'^\circ \geq 2q/s.$$

If $s = 3$ then our assumption $g^\circ \leq q/s^2$ shows that this is impossible. For $s > 3$ we use the hypothesis $g^\circ \leq (q-s)/s(s-1)$ (and $g'^\circ < g^\circ$), to get

$$q(s-5) \leq -s(s+3)$$

so that $s < 5$. But if $s = 4$, then $p = 2$. With $k = mg'' - m'g'$ we now have the two equations:

$$mf = (f^s - (X^q - X))f' \quad \text{and} \quad m(m-1)f' = (f^s - (X^q - X))k.$$

This case is ruled out in four steps.

(i) *If $f(a) = 0$, then $m(a) = \mu_a$, the multiplicity of a as a zero of f.*
Indeed, $m = (f^s-(X^q-X))f'/f$, and $(X-a)(f'/f)|_{X=a} = \mu_a$, but $(f^s-(X^q-X))/(X-a)|_{X=a} = 1$, so $m(a) = \mu_a$.

(ii) *The number of zeros of f with odd multiplicity is at most m°.*
Indeed, they are zeros of $m - 1$.

(iii) *The degree of k is at least $q/4 - m^\circ$.*
Indeed, f has a quadratic factor of degree $q/4 - m^\circ$. This factor divides f', and every zero also occurs in $m(m-1)$. On the other side, the zeros of $f^s - (X^q - X)$ all have multiplicity one, so the quadratic factor divides k.

(iv) *$k = 0$ and $m = 1$.*
Indeed, the assumption was $g^\circ \leq (q-s)/s(s-1) < q/12$. We just found $2m^\circ + g^\circ > 4g^\circ + k^\circ$, so $3m^\circ - 3g^\circ > q/4$. Since $m^\circ < 5g^\circ - q/4$ this gives $12g^\circ > q$, contradiction.
□

We now turn to investigate the differential equation $X^{q/s} + g = (g^s + X)g'$. Let $h = g'$. We would like to prove that essentially $g(X) = X + X^s + \ldots + X^{q/s^2}$ (so that h is constant, and $e|n$). But there are other solutions as well (see the proof below). However, in the case of nonconstant h we can bound its degree very precisely, and moreover find information on its shape.

Lemma 3.2 *Let $X^{q/s} + g = (g^s + X)h$, where $h = g'$. Then either h is constant, or for some $i > 0$, we have $h \in K[X^{s^i}] \setminus K[X^{s^{i+1}}]$,*

$$\frac{q(s-1)}{s^{i+2}} \leq h^\circ < \frac{q(s-1)}{s^{i+2} - s}$$

and $h = \eta\zeta^{s-1}$ for certain polynomials $\eta \in K[X^{s^{i+1}}]$, $\zeta \in K[X^{s^i}]$. In particular, every zero of h has multiplicity at least $(s-1)s^i$.

Proof: If h is not constant, then $q > s^2$, and $h^\circ + 1 \le g^\circ < q/s^2$. In the identity

$$X^{q/s} + (g - Xh) = g^s h,$$

compare the terms of degree not divisible by s on both sides. On the left hand side these have degree at most q/s^2, but on the right hand side there is a factor g^s of degree $sg^\circ \ge (q+s)/(s+1) > q/s^2$, so h does not have any terms of degree not divisible by s, i.e., $h \in K[X^s]$.

Let $h \in K[X^{s^i}] \setminus K[X^{s^{i+1}}]$. Then $i \ge 1$ and $q > s^{i+2}$. Put (for $j \ge 0$)

$$g_j = g - Xh - X^s h^{s+1} - X^{s^2} h^{s^2+s+1} - \ldots - X^{s^{j-1}} h^{s^{j-1}+\ldots+1},$$

(so that $g_0 = g$). By induction on j $(1 \le j \le i)$ we see that $g_j(X) \in K[X^{s^j}]$.

Indeed, for $j = 1$ we have seen this already, and for $2 \le j \le i$ this follows from the identity

$$X^{q/s} + g_j = g_{j-1}^s h.$$

For $0 \le j \le i-1$, all terms of g_{j+1} occur in g_j (since no term of $g_{j+1} - g_j = -X^{s^j} h^{s^j+\ldots+1}$ lies in $K[X^{s^{j+1}}]$), so that $g_i^\circ \le g^\circ$ and

$$s^{i-1} + h^\circ \frac{s^i - 1}{s - 1} \le g^\circ. \tag{1}$$

Write $\tilde{g} = g_i$. Then $\tilde{g}$ satisfies

$$X^{q/s} + \tilde{g} - X^{s^i} h^{s^i+\ldots+1} = \tilde{g}^s h. \tag{2}$$

If the inequality (1) is strict, then $\tilde{g}^\circ = g^\circ$. On the other hand, if we have equality in (1), then we can solve g° and h° from that equality and $sg^\circ + h^\circ = q/s$, and find $h^\circ = (s-1)(q - s^{i+1})/(s^{i+2} - s)$. Since this is a positive integer, $(i+1)e$ divides n, and $q \ge s^{2i+2}$. It follows that h° satisfies the inequalities claimed, and it only remains to show that h has the required shape; in particular, there is nothing to prove anymore for $s = 2$.

If $\tilde{g} = 0$, then (2) implies that h is a monomial. We do have equality in (1), and $h = \alpha X^{h^\circ}$ where $h^\circ = (s-1)(q - s^{i+1})/(s^{i+2} - s)$ and $\alpha^{s^i+\ldots+1} = 1$. Thus, h is an $(s-1)$-th power. (Conversely, this h, together with the g determined by $\tilde{g} = 0$, is a solution of the differential equation considered.)

Now let $\tilde{g} \ne 0$. Write

$$h = \sum_{j=0}^{s-1} \eta_j X^{js^i} \quad \text{and} \quad \tilde{g} = \sum_{j=0}^{s-1} \gamma_j X^{js^i},$$

where $\eta_j, \gamma_j \in K[X^{s^{i+1}}]$ $(0 \le j \le s-1)$. Then

$$\gamma_j - \eta_{j-1} h^{s^i+\ldots+s} = \tilde{g}^s \eta_j \tag{s_j}$$

for $j \ne 0$, and

$$X^{q/s} + \gamma_0 - \eta_{s-1} X^{s^{i+1}} h^{s^i+\ldots+s} = \tilde{g}^s \eta_0. \tag{s_0}$$

Since $\tilde{g}^s$ has larger degree than γ_j, we see from (s_j) that if $\eta_j \ne 0$ then also $\eta_{j-1} \ne 0$. In particular, $\eta_0 \ne 0$. Moreover, $\eta_1 \ne 0$, since $h \notin K[X^{s^{i+1}}]$.

Computing $\eta_j \cdot (s_j) - \eta_{j-1} \cdot (s_{j+1})$ we find for $1 \le j \le s-2$:

$$\eta_j \gamma_j - \eta_{j-1} \gamma_{j+1} = \tilde{g}^s (\eta_j^2 - \eta_{j-1} \eta_{j+1}).$$

The left hand side has degree at most $g^\circ + h^\circ$, while the right hand side is either zero, or has degree at least $s\tilde{g}^\circ$. Claim: $s\tilde{g}^\circ > g^\circ + h^\circ$.

Indeed, either we have $s\tilde{g}^\circ = sg^\circ > g^\circ + h^\circ$, or we have equality in (1) and from equation (s_1) we find (for $s \geq 3$):

$$s\tilde{g}^\circ \geq h^\circ(s^i + \ldots + s - 1) = \frac{s-1}{s}\left(\frac{q-1}{s^{i+1}-1} - 1\right)(s^i + \ldots + s - 1) > \frac{q}{s^2} = sg^\circ + h^\circ > g^\circ + h^\circ.$$

Consequenly, $\eta_j\gamma_j - \eta_{j-1}\gamma_{j+1} = \eta_j^2 - \eta_{j-1}\eta_{j+1} = 0$ for $1 \leq j \leq s-2$, so that all η_j are nonzero, and $\eta_j = \eta_0(\eta_1/\eta_0)^j$ for $0 \leq j \leq s-1$ and

$$s = \eta_0 \sum_j (\frac{\eta_1}{\eta_0}X^{s^i})^j = \eta_0(\frac{\eta_1}{\eta_0}X^{s^i} - 1)^{s-1}.$$

Let $\eta_0 = u_0 u$ and $\eta_1 = u_1 u$ where $u = \gcd(\eta_0, \eta_1)$ so that $\gcd(u_0, u_1) = 1$. Then u, u_0, $u_1 \in K[X^{s^{i+1}}]$, and

$$h = \frac{u}{u_0^{s-2}}(u_1 X^{s^i} - u_0)^{s-1}.$$

Now it follows that $u_0^{s-2} \mid u$ (note that if $X \mid u_0$ then the multiplicity of the factor X in u_0 and u is a multiple of s^{i+1}, while it is less than s^{i+1} in $(u_1X^{s^i} - u_0)^{s-1}$). Say $u/u_0^{s-2} = \eta$, for $\eta \in K[X^{s^{i+1}}]$ and h has the required form with $\zeta = u_1 X^{s^i} - u_0$.

It remains to prove the degree estimate for h in case $\tilde{g}^\circ = g^\circ$. But in this case $h^\circ = q/s - sg^\circ$ is a multiple of s^{i+1}, so that $\eta_0^\circ = h^\circ$.

From $\eta_0 = \eta u_0^{s-1}$ and $\eta_1 = \eta u_0^{s-2} u_1$ it also follows that $\eta_1^\circ \geq h^\circ(s-2)/(s-1)$. Now consider $\eta_1.(s_0) - \eta_0.(s_1)$:

$$\eta_1 X^{q/s} + \eta_1\gamma_0 - \eta_0\gamma_1 - (-\eta_0^2 + \eta_1 X^{s^{i+1}}\eta_{s-1})s^{s^i+\ldots+s} = 0.$$

This gives the degree estimate for h. □

4 Considering all directions simultaneously

Let D_w be the set of $y \in D$ with $s_y = w$, and put $N_w := |D_w|$. Then $N = \sum_w N_w$, and counting the points of U seen from a fixed point $u \in U$ in all directions we get $\sum N_w(w-1) \leq q - 1$. If $N_w = 0$ for $s < w < t$, then it follows from $N > q/(s+1)$ that

$$\sum_{w>s} N_w < \frac{2q}{(t-s)(s+1)} \quad \text{and} \quad N_s > \frac{q}{s+1} - \frac{2q}{(t-s)(s+1)}.$$

In particular, these estimates hold for $t = ps$.

Let us call $y \in D$ regular if $s_y = s$. The number of regular points is N_s. For a regular point the previous lemmas apply, that is $r_y^{1/s} = X^{q/s} + g_y = (g_y^s + X)h_y$ with $h_y = g_y'$ (provided of course that $s \geq 4$, or $s = 3$ and $N \leq q/3 + 1$). Let us call the regular point y of type i if $h_y \in K[X^{s^i}] \setminus K[X^{s^{i+1}}]$ and of type ∞ if h_y is constant.

Lemma 4.1 *There is a regular point y with h_y constant when $s \geq 4$, or $s = 3$ and $N \leq q/3 + 1$.*

Proof: Count triples $(a, b, y) \in U \times U \times D$ where the line joining a and b has slope y. Since every pair determines one direction this number is exactly $q(q-1)$. Let N_y be the number of such triples for a fixed y. If y is regular of type $i < \infty$, each line of length L in direction y contributes $L(L-1)$ to N_y, so that $N_y = q(s-1) + \sum_L L(L-s)$. But lines of length larger than s have length $s(1 + a_\alpha s^i)$, and contribute a factor of multiplicity $1 + a_\alpha s^i$ to g_y and of multiplicity $a_\alpha s^i$ to h_y. Since $\sum_\alpha a_\alpha s^i = h_y^\circ$ and $a_\alpha \geq s - 1$ (by the previous lemma), we find

$\sum L(L-s) \geq s^{i+2} \sum_\alpha a_\alpha(1+a_\alpha s^i) > s^{i+2}(s-1)h_y^\circ \geq (s-1)^2 q$. It follows that $N_y \geq q(s^2-s)$. Hence the number of regular points not of type ∞ is at most

$$\frac{q(q-1)}{q(s^2-s)} = \frac{q-1}{s^2-s}.$$

Since the number of regular points is

$$N_s > \frac{q}{s+1} - \frac{2q}{s(s+1)(p-1)},$$

there is a regular point y with constant h_y when $s \geq 3$. □

At this point we can conclude that $e \,|\, n$, and also $N \geq q/s+1$. This completes the proof of parts (i)-(iv) of the theorem.

5 U is a subspace

We now proceed to show that the set U is $GF(s)$-linear. This is done by showing that the Rédei polynomial $r(X,Y,Z)$ is of the form

$$r(X,Y,Z) = \sum_i \rho_{q/s^i}(Y,Z)X^{q/s^i}.$$

i.e., that $\rho_j = 0$ unless j is a power of s. Note that $\rho_0 = 0$ since U contains the origin.

Let D_s^∞ be the set of points $y \in D_s$ (the set of regular points) of type ∞, and put $N_s^\infty := |D_s^\infty|$. If $y \in D_s^\infty$ then $r_y = X^{q/s} + g_y$ can be solved from $X^{q/s} + g_y = (g_y^s + X)c$ for some $c \in K$, and we see that $\rho_{q/s}(y) \neq 0$. Here we abuse notation by writing $\rho_j(y) = \rho_j(y,1)$ for $y \in K$, and $\rho_j(\infty) = \rho_j(1,0)$. Since there is such a point y, we have $\rho_{q/s} \neq 0$. Since $\rho_{q/s}^\circ \leq q - q/s$ it follows that for at least q/s points $y \in D$, $\rho_{q/s}(y) \neq 0$. Therefore, the number of y with $r_y^{\circ\circ} \geq q/s$ is at least q/s. If $y \in D_s \setminus D_s^\infty$ then $q/(s+1) < r_y^{\circ\circ} < q/s$. So, the at least q/s points y where $\rho_{q/s}$ does not vanish all lie in $D_s^\infty \cup \bigcup_{w>s} D_w$, and it follows that

$$N_s^\infty \geq \frac{q}{s} - \frac{2q}{(p-1)s(s+1)}.$$

We want to prove that in $r(X,Y,Z)$ only the terms with X-degree of the form q/s^i for some i survive. Call j exceptional if j is not of this form. So we want to show that $\rho_j = 0$ for exceptional j. Now if j is exceptional, then $\rho_j(y) = 0$ for $y \notin D$ and also for $y \in D_s^\infty$, and these two sets together have more than

$$q - \frac{q-1}{s-1} + \frac{q}{s} - \frac{2q}{(p-1)s(s+1)}$$

points. Since ρ_j has degree at most $q-j$, this shows that there are no exceptional numbers j with $q/s > j > q/(s+1)$, in other words $D_s = D_s^\infty$: all regular points are of type ∞.

Let us now extend the definition of regular. We call the polynomial f regular if it is $GF(s)$-linear, so if it is in the span of $\{X, X^s, X^{s^2}, \ldots\}$. Also $y \in K \cup \{\infty\}$ is regular if the polynomial $r_y(X)$ is regular. So points in D that were regular before still are, and points outside D are regular as well. The aim is of course to show that all points are regular. Let $t = \min\{s_y \,|\, y \text{ irregular}\}$. So $t > s$. Take $y \in D_t$, irregular. Then $r_y \in K[X^t]$. The number of irregular points is bounded from above by $\sum_{w \geq t} N_w < 2q/(t-s)(s+1)$. Hence, if j is exceptional, then also $j \leq 2q/(t-s)(s+1)$ (again because all regular points are zeros of ρ_j which has degree at most $q-j$). Write

$$r_y = X^q + g + h^t$$

where g is regular of degree at most q/s, and h^t corresponds to the exceptional part. In particular $th^\circ \leq 2q/(t-s)(s+1)$.

First assume t is not a power of s. So $s^i < t < s^{i+1}$ for some $i \geq 1$. And $h' \neq 0$. The usual divisibility relation for $r_y^{1/t}$ is

$$r_y^{1/t} = (X^{q/t} + g^{1/t} + h) \,|\, (X + g + h^t)h'. \tag{3}$$

Also for $1 \leq j \leq i$ one has $r_y^{1/t} \,|\, r_y^{1/s^j}$ or

$$X^{q/s^j} \equiv -g^{1/s^j} - h^{t/s^j} \bmod r_y^{1/t}.$$

Note that g^{1/s^j} is regular, of degree at most q/s^{j+1}. This means that we may reduce g to a linear combination of polynomials X, X^s, $X^{s^2}, \ldots, X^{q/s^{i+1}}$ and $h^{t/s}$, $h^{t/s^2}, \ldots, h^{t/s^i}$ modulo $r_y^{1/t}$.

This reduces the right hand side of (3) to a polynomial of degree at most $q/s^{i+1} + h'^{\circ} < q/t$. So the right hand side is zero after this reduction, an impossibility since $h' \neq 0$ and the factor in front of it is of the form X plus a p-th power.

So in fact t is a power of s, say $t = s^i$, $i > 1$, and we proceed exactly as before, except that now $g^{1/t}$ may have a linear term, so that in the right hand side h' must be replaced by $(h + g^{1/t})'$. The right hand side zero again so some linear combination of X, X^s, $X^{s^2}, \ldots$, h, h^s, $h^{s^2}, \ldots$ is zero and it is an exercise to show that h and also h^t are in fact regular. (Here one has to observe that the constant term of h is zero because we took the origin in U.)

Finally, let $w \in GF(q^2) \setminus GF(q)$, and map $AG(2,q)$ to $GF(q^2)$ by $(a,b) \mapsto -aw + b$. The images of the points of U under this map are the zeros of

$$r_w(X) = \prod (X + a_i w - b_i) \in \langle X, X^s, X^{s^2}, \ldots, X^q \rangle_{GF(q^2)}.$$

From the form of r_w it now follows that $r_w(X_1 + X_2) = r_w(X_1) + r_w(X_2)$ and $r_w(\alpha X) = \alpha r_w(X)$, for all X, X_1, $X_2 \in GF(q^2)$ and $\alpha \in GF(s)$ □

References

[1] A. Blokhuis, *Blocking sets in Desarguesian Planes*, in: Paul Erdős is Eighty, vol. **2**, (1996) 1–23. ed.: D. Miklós, V.T. Sós, T. Szőnyi, Bolyai Soc. Math. Studies.

[2] A. Blokhuis, A.E. Brouwer & T. Szönyi, *The number of directions determined by a function f on a finite field*, J. Comb. Th. (A) **70** (1995) 349-353.

[3] R.J. Evans, J. Greene & H. Niederreiter, *Linearized polynomials and permutation polynomials of finite fields*, Michigan Math. J. **39**, (1992) 405–413.

[4] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970. MR 45#3366 (English translation: Lacunary polynomials over finite fields, North Holland, Amsterdam, 1973, MR 50#4548)