How to use Rédei polynomials in higher dimensional spaces

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

4 October 2004

1 The origin of Rédei polynomials

A polynomial with coefficients from a finite field $GF(q)$ that is the product of linear polynomials is usually referred to as a *Rédei polynomial*. This is due to the appearance of the polynomial

$$R(T,S) = \prod_{(x,y)\in\mathcal{A}} (T - xS + y),$$

where $\mathcal{A}$ is some subset of $GF(q)^2$, in the book of Rédei [15] from the early seventies.

In the affine plane $AG(2,q)$ the point (x,y) is incident with the line $Y = mX + \alpha$ if and only if $\alpha = -mx + y$. Hence $-\alpha$ is a root of $R(T,m)$ of multiplicity k if and only if the line $Y = mX + \alpha$ is incident with k points of the set $\mathcal{A}$. This observation allows one to look at a problem of the following type: Given a subset of points of the affine plane that has restricted intersection properties with the lines of the plane, say something about the size of the subset or, clearly better, determine the possibilities for such a subset.

*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.

The problem for which Rédei introduced the polynomial $R(T,S)$ was that of determining those functions over a finite field that determine few directions. Given a set of q points $\mathcal{A}$ in $AG(2,q)$ each line of a set of q parallel lines is either incident with exactly one point of $\mathcal{A}$ or there is a line incident with at least two points of $\mathcal{A}$. In the latter case we say that the direction corresponding to the parallel class of the line is determined by $\mathcal{A}$. The problem of classifying those functions over a finite field that determine few directions is equivalent to classifying those subsets $\mathcal{A}$ that determine few directions. Let us see why $R(T,S)$ is a useful tool to approach this problem. Suppose $m \in GF(q)$ is a direction not determined by $\mathcal{A}$. That is, for all $\alpha \in GF(q)$, the line $Y = mX + \alpha$ is incident with exactly one point of $\mathcal{A}$. According to the previous paragraph this implies that the polynomial $R(T,m)$ has a simple root α, for all $\alpha \in GF(q)$, hence $R(T,m) = T^q - T$. Let $\mathcal{D}$ be the set of directions determined by the set $\mathcal{A}$ and suppose, without loss of generality, that the infinite direction (the direction corresponding to the parallel class of lines of the form $X = \alpha$) is in $\mathcal{D}$. The monic polynomial

$$g(S) := \prod_{m \notin \mathcal{D}} (S - m),$$

has degree $q + 1 - |\mathcal{D}|$, divides $R(T,S) - T^q + T$, and we can write

$$R(T,S) = T^q - T + g(S)H(T,S),$$

for some polynomial H of degree at most $|\mathcal{D}| - 1$.

We continue a little further along Rédei's arguments as we are about to see a phenomenon which will occur again later on.

Theorem 1.1 *(Rédei) If $\mathcal{A}$ is a set of q points of $AG(2,q)$ determining less than $(q+3)/2$ directions then any line is incident with 0 mod p points of $\mathcal{A}$, or exactly one point of $\mathcal{A}$.*

Proof : Let $m \in \mathcal{D}$ and consider $R(T,m)$. Let $T + \alpha$ be a factor of $R(T,m)$ of multiplicity k, in other words let $Y = mX + \alpha$ be a line incident with k points of $\mathcal{A}$. Since $T + \alpha$ divides both $R(T,m)$ and $T^q - T$ we have that $T + \alpha$ is a factor of $H(T,m)$. It is a factor of multiplicity at least $k - 1$ of $\frac{\partial R}{\partial T}(T,m)$ and so

$$(T + \alpha)^k \mid H(T,m)\frac{\partial R}{\partial T}(T,m).$$

This is true for all linear factors of $R(T,m)$ and since $R(T,m)$ is the product of linear factors

$$R(T,m) \mid H(T,m)\frac{\partial R}{\partial T}(T,m).$$

The left-hand side of this divisibility has degree q and the right-hand side has degree at most $2|\mathcal{D}|-3$. Note that when we differentiate the Rédei polynomial with respect to T we have

$$\frac{\partial R}{\partial T}(T,S) = -1 + g(S)\frac{\partial H}{\partial T}(T,S),$$

which has degree at most $|\mathcal{D}|-2$ in T. If $|D| < (q+3)/2$ then the right-hand side of the divisibility has degree less than q and is therefore zero. If $H(T,m)=0$ then $R(T,m) = T^q - T$ which would imply that $m \notin D$, which is not the case, so we conclude that $\frac{\partial R}{\partial T}(T,m) \equiv 0$. This implies that $R(T,m) \in GF(q)[T^p]$, where $q=p^h$, or equivalently, that there exists a polynomial $r(T) \in GF(q)[T]$ such that

$$R(T,m) = r(T)^p,$$

we say $R(T,m)$ is a p-th power. So any factor $T+\alpha$ of $R(T,m)$ has multiplicity a multiple of p, from which it follows that the line $Y = mX + \alpha$ is incident with a multiple of p points of $\mathcal{A}$.

If $m \notin \mathcal{D}$ then we already saw that each line $Y = mX + \alpha$ is incident with exactly one point of $\mathcal{A}$. □

This theorem is the first example of what is known as a "mod p" result. We shall see more examples of Rédei polynomials providing us with mod p results later on. Let us conclude this section by mentioning that the sets of q points that determine less than $(q+3)/2$ directions are now known to be subspaces over some subfield, see [6] and [3].

If q is prime then the above theorem implies that the only sets of q points determining less than $(q+3)/2$ directions are the lines (and they determine only one direction). Moreover Lovász and Schrijver [13] proved that any set of q points that determines exactly $(q+3)/2$ directions is equivalent to the set

$$\{(x, x^{(q+1)/2}) \mid x \in GF(q)\},$$

and Gács [10] proved that these are the only sets of points determining less than $\lfloor 2(q-1)/3 \rfloor + 1$ directions.

We could now continue in the plane and look at the consequences of Rédei polynomials for blocking sets in $PG(2,q)$ but that is not our focus here. It is worth mentioning that they do provide us with a mod p result, namely that every line of $PG(2,q)$ is incident with 1 mod p points of a minimal blocking set with less than $3(q+1)/2$ points. The excellent survey of Szőnyi, Gács and Weiner [17] provides an up-to-date reference.

2 Early appearances of multivariate Rédei polynomials

The earliest appearance of a multivariate Rédei polynomial seems to be in the article of Brouwer and Schrijver [7], where they consider the polynomial

$$R(Y_1, Y_2, \ldots, Y_n) := \prod_{(x_1,x_2,\ldots,x_n)\in\mathcal{A}} (1 + x_1Y_1 + x_2Y_2 + \ldots + x_nY_n),$$

where $\mathcal{A}$ is a set of points in $AG(n, q)$, containing the origin, with the property that every hyperplane is incident with a point of $\mathcal{A}$, i.e., $\mathcal{A}$ is a *blocking set* with respect to hyperplanes. For all $(y_1, y_2, \ldots, y_n) \in GF(q)^n$, $(y_1, y_2, \ldots, y_n) \neq (0, 0, \ldots, 0)$ the hyperplane

$$y_1X_1 + y_2X_2 + \ldots + y_nX_n = -1$$

is incident with a point of $\mathcal{A}$ and so $R(y_1, y_2, \ldots, y_n) = 0$. Now the geometrical property of the set $\mathcal{A}$ has been translated into an algebraic property of the polynomial R. Moreover, $\deg R = |\mathcal{A}| - 1$. It is a fairly short step to show that $\deg R$ must be at least $n(q - 1)$ and hence that a blocking set of hyperplanes in $AG(n, q)$ has at least $n(q - 1) + 1$ points, a result earlier obtained by Jamison in [12].

The multivariate Rédei polynomial appeared again in the article of Bruen [8] where he generalised the Jamison bound to multiple blocking sets of hyperplanes of $AG(n, q)$ and following on from his work it appears again in [2]. However in all these cases the geometrical property of the set $\mathcal{A}$ is related to points and hyperplanes, as it is in the following.

In [1] Alon and Tarsi use Rédei polynomials to prove Jaeger's conjecture for q non prime. Jaeger's conjecture states that when $q \geq 5$, for all matrices $X \in GL(n, q)$ there exists a vector $y \in GF(q)^n$ with the property that y and Xy have no zero coordinate. In [11] Jaeger only conjectures this for $q = 5$.

Let us see how Rédei polynomials can be used to tackle this problem. If the conjecture is not true then there is a matrix $X \in GL(n, q)$ with the property that Xv has a zero component, for all $y \in GF(q)^n$ with no zero component. The set of n points $\mathcal{A}$ that is made up of the rows of X is a set of n points in $PG(n - 1, q)$ that spans the whole space and has the property that the hyperplane

$$y_1X_1 + y_2X_2 + \ldots + y_nX_n = 0$$

is incident with a point of $\mathcal{A}$ for all $y \in GF(q)^n$ with no zero component.

In other words, if we define a Rédei polynomial

$$R(Y_1, Y_2, \ldots, Y_n) := \prod_{(x_1,x_2,\ldots,x_n)\in\mathcal{A}} (x_1Y_1 + x_2Y_2 + \ldots + x_nY_n)$$

then for all vectors y which have no zero component $R(y_1, y_2, \ldots, y_n) = 0$. This algebraic property of R implies that we can write

$$R(Y_1, Y_2, \ldots, Y_n) = (Y_1^{q-1} - 1)f_1 + (Y_2^{q-1} - 1)f_2 + \ldots + (Y_n^{q-1} - 1)f_n,$$

where $f_1, f_2, \ldots f_n \in GF(q)[Y_1, Y_2, \ldots, Y_n]$ are polynomials of degree at most $n-(q-1)$. The matrix X is non-singular and so has an inverse $X^{-1} = (a_{ij})$. If we make the substitution $Y_i = \sum a_{ij} Z_j$ we have

$$Z_1 Z_2 \ldots Z_n = \sum_{i=1}^{n} \left(\left(\sum a_{ij} Z_j \right)^{q-1} - 1 \right) f_i.$$

Now on the right-hand side when we try to find a term $Z_{i_1} Z_{i_2} \ldots Z_{i_{q-1}}$ from one of the $(\sum a_{ij} Z_j)^{q-1}$ terms, as we must since the left-hand side is $Z_1 Z_2 \ldots Z_n$, the coefficient is a multiple $(q-1)!$. If q is not prime then this is always zero and we have a contradiction.

3 Rédei polynomials in three indeterminates

The Rédei polynomials that we have seen up until now have helped us with problems where we have a set of points with certain intersection properties with hyperplanes. Now we shall look at how to use Rédei polynomials in situations where we have a set of points that have certain intersection properties with smaller dimensional subspaces. The obvious place to start is in three dimensional affine or projective space, so let $\mathcal{A}$ be a subset of the points of $AG(3, q)$ and define

$$R(T, S, U) = \prod_{(x,y,z) \in \mathcal{A}} (T + xS + yU + z).$$

We define polynomials in two indeterminates σ_j, of total degree at most j, by writing

$$R(T, S, U) = \sum_{j=0}^{|\mathcal{A}|} \sigma_j(S, U) T^{|\mathcal{A}|-j}.$$

Let a and b be any elements of $GF(q)$ and consider the factors of the polynomial

$$R(T, aU + b, U) = \prod_{(x,y,z) \in \mathcal{A}} (T + (ax + y)U + bx + z).$$

The point (x, y, z) is incident with the line defined by the hyperplanes $aX + Y = \alpha$ and $bX + Z = \beta$ if and only if $ax + y = \alpha$ and $bx + z = \beta$ if and only if the corresponding factor in $R(T, aU+b, U)$ is $T+\alpha U+\beta$. Note that for a fixed a and b these q^2 lines are parallel. Identifying the affine point (x, y, z) with the projective point $\langle x, y, z, 1\rangle$ then the line defined by the hyperplanes $aX+Y=\alpha$ and $bX+Z=\beta$ is incident with point $\langle 1, -a, -b, 0\rangle$. Indeed, every affine line incident with $\langle 1, -a, -b, 0\rangle$ can be defined by the intersection of two hyperplanes of the form $aX+Y=\alpha$ and $bX+Z=\beta$, for some α and β, and this line is incident with k points of $\mathcal{A}$ if and only if $T+\alpha U+\beta$ occurs as a factor of $R(T, aU+b, U)$ with multiplicity k.

Let us fix a situation to see how we can make use of this. Let $\mathcal{A}$ be a set of q^2 points that does not determine every direction, so we can assume there is a point $\langle 1, -a, -b, 0\rangle$ whose corresponding parallel class of q^2 lines are each incident with exactly one point of $\mathcal{A}$. Each factor in $R(T, aU+b, U)$ is distinct and we have

$$R(T, aU+b, U) = \prod_{\alpha,\beta\in GF(q)} (T+\alpha U+\beta)$$

$$= T^{q^2} - ((U^q - U)^{q-1} + 1)T^q + (U^q - U)^{q-1}T.$$

However, we also have that,

$$R(T, aU+b, U) = \sum_{j=0}^{q^2} \sigma_j(aU+b, U)T^{|\mathcal{A}|-j}$$

and hence for $1 \leq j \leq q^2 - q - 1$,

$$\sigma_j(aU+b, U) \equiv 0.$$

Hence we have that $\sigma_j(S, U) \equiv 0 \bmod S - aU - b$ from which it follows that

$$S - aU - b \mid \sigma_j(S, U).$$

If there are more pairs (a, b) than the degree of σ_j for which this holds then $\sigma_j(S, U) \equiv 0$.

So in our situation let N be the number of directions $\langle 1, -a, -b, 0\rangle$ not determined by two points of $\mathcal{A}$. Then

$$R(T, S, U) = T^{q^2} + \sum_{j=0}^{q^2-N} \sigma_{q^2-j}(S, U)T^j.$$

When we evaluate both $S = s$ and $U = u$ we are looking at the intersection properties of $\mathcal{A}$ with planes. Indeed, a factor $T+\alpha$ has multiplicity k in $R(T, s, u)$ if and only if the plane $sX+uY+Z=\alpha$ is incident with k points of $\mathcal{A}$. However, $R(T, s, u) = T^{q^2}+g(T)$, where $\deg g \leq q^2 - N$, and moreover factorises into linear factors in $GF(q)[T]$. Some short arguments lead to the following theorem.

Theorem 3.1 ([4]) *If $\mathcal{A}$ is a set of q^2 points of $AG(3,q)$ that does not determine at least $p^e q$ directions for some $e \in \mathbb{N} \cup \{0\}$ then every plane meets $\mathcal{A}$ in 0 mod p^{e+1} points.*

By [16, Theorem 11] we know that if the number of directions determined is less than $q(q+3)/2$ then the set $\mathcal{A}$ is $GF(s)$-linear for some subfield $GF(s)$ of $GF(q)$. In the case when q is prime this means that $\mathcal{A}$ is a plane. Theorem 3.1 says that in the case when q is prime and we have a set of points that determine less than q^2+2 directions then every plane contains 0 mod q points. It would be interesting to know if this implies that $\mathcal{A}$ is a cone.

Some immediate corollaries of Theorem 3.1 relate to ovoids of the generalised quadrangles $T_2(O)$ or $T_2^*(O)$, see [14, pp.37–38] for a description of these quadrangles.

Corollary 3.2 ([4]) *Let $\mathcal{O}$ be an ovoid of the generalised quadrangle $T_2^*(O)$. The planes of $AG(3,q)$ are incident with zero mod p points of $\mathcal{O}$.*

Corollary 3.3 ([4]) *Let $\mathcal{O}$ be an ovoid of the generalised quadrangle $T_2(O)$ containing the point (∞). The planes of $AG(3,q)$ are incident with zero mod p points of $\mathcal{O}$.*

In the case that O is a conic the generalised quadrangle $T_2(O)$ is isomorphic to $Q(4,q)$. Since we can choose any point of $Q(4,q)$ to be the point (∞), the corollary says that every elliptic quadric meets an ovoid of $Q(4,q)$ in 1 mod p points or not at all. In fact one can eliminate the possibility that an elliptic quadric and an ovoid are disjoint but that does involve slightly more work, see [5]. A short counting argument leads to the following theorem.

Theorem 3.4 ([5]) *When q is prime an ovoid of $Q(4,q)$ is an elliptic quadric.*

Although the Rédei polynomial considered in [5] is the same as we have used here, they used a more roundabout argument involving the Klein correspondence to deduce the fact that for nearly all j the identity $\sigma_j(aU, U-a) \equiv 0$ holds for all $a \in GF(q)$. Now we see that from $\sigma_j(aU+b, U) \equiv 0$, one only need substitute U with $U-a$ and put $b = a^2$ to obtain the same equivalence.

The previous theorem can be pushed a little further. De Beule and Metsch recently proved the following.

Theorem 3.5 ([9]) *When q is prime a set of q^2+2 points that blocks every line of $Q(4,q)$ is an elliptic quadric together with a point.*

4 Rédei polynomials in four indeterminates

We shall look briefly at Rédei polynomials in four indeterminates. Let $\mathcal{A}$ be a subset of points of $AG(4,q)$ and define

$$R(T,S,U,V) = \prod_{(x,y,z,w)\in\mathcal{A}} (T + xS + yU + zV + w).$$

We define polynomials in three indeterminates σ_j, of total degree at most j, by writing

$$R(T,S,U,V) = \sum_{j=0}^{|\mathcal{A}|} \sigma_j(S,U,V) T^{|\mathcal{A}|-j}.$$

Let a, b, c and d be any elements of $GF(q)$ and consider the factors of the polynomial

$$R(T, aU + bV + c, U, V) = \prod_{(x,y,z,w)\in\mathcal{A}} (T + (ax + y)U + (bx + z)V + cx + w).$$

The point (x, y, z, w) is incident with the line defined by the hyperplanes $aX + Y = \alpha$, $bX + Z = \beta$ and $cX + W = \gamma$ if and only if $ax + y = \alpha$, $bx + z = \beta$ and $cx + w = \gamma$ if and only if the corresponding factor in $R(T, aU + bV + c, U, V)$ is $T + \alpha U + \beta V + \gamma$. Hence this substitution allows us to use the intersection properties that $\mathcal{A}$ may have with lines.

On the other hand considering the factors of the polynomial

$$R(T, aV + c, bV + d, V) = \prod_{(x,y,z,w)\in\mathcal{A}} (T + (ax + by + z)V + cx + dy + w).$$

The point (x, y, z, w) is incident with the plane defined by the hyperplanes $aX + bY + Z = \alpha$ and $cX + dY + W = \beta$ if and only if $ax + by + z = \alpha$ and $cx + dy + w = \beta$ if and only if the corresponding factor in $R(T, aV + c, bV + d, V)$ is $T + \alpha V + \beta$. Hence this substitution allows us to use the intersection properties that $\mathcal{A}$ may have with planes.

5 Rédei polynomials in many indeterminates

Let us prove the natural generalisation of Theorem 3.1 to $AG(n, q)$ by using Rédei polynomials in n variables.

Theorem 5.1 *If $\mathcal{A}$ is a set of q^{n-1} points of $AG(n,q)$ that does not determine at least $p^e q$ directions for some $e \in \mathbb{N} \cup \{0\}$ then every hyperplane meets $\mathcal{A}$ in* 0 *mod p^{e+1} points.*

Proof : Let $\mathcal{A} \subset AG(n,q) = PG(n,q) \setminus \pi_\infty$ where π_∞ is defined by the equation $X_0 = 0$. Let $\mathcal{D}$ be the set of directions determined by $\mathcal{A}$, i.e.

$$\mathcal{D} = \{P \in \pi_\infty \mid P \in \langle Q, R \rangle,\ Q, R \in \mathcal{A}\}.$$

Define the Rédei polynomial as

$$R(T,X) = \prod_{\langle 1,a_1,\ldots,a_n\rangle \in \mathcal{A}} \left(T + \sum_{i=1}^{n} a_i X_i \right),$$

where $X = (X_1, \ldots, X_n)$, and define the polynomials $\sigma_j(X)$ by writing

$$R(T,X) = \sum_{j=0}^{q^{n-1}} T^{q^{n-1}-j} \sigma_j(X).$$

Note that the total degree of σ_j is at most j.

Let $P = \langle 0, y_1, y_2, \ldots, y_n \rangle \in \pi_\infty \setminus \mathcal{D}$ be a direction not determined by $\mathcal{A}$ and since P must have a non-zero coordinate, we may assume that $y_m = 1$, for some m. Now consider the Rédei polynomial $R(T,X)$ modulo $\sum_{i=1}^{n} y_i X_i$. We get

$$R(T,X) \equiv \prod_{\langle 1,a_1,\ldots,a_n\rangle \in \mathcal{A}} \left(T + \sum_{i=1}^{n} (a_i - a_m y_i) X_i \right) \mod \sum_{i=1}^{n} y_i X_i.$$

For all $\gamma \in GF(q)^{n-1}$, the line defined by the $n-1$ equations $X_i - y_i X_m = \gamma_i X_0$, where $i \neq m$, contains the point P, which is a direction not determined by $\mathcal{A}$, and so contains exactly one point of $\mathcal{A}$. Hence there is exactly one $\langle 1, a_1, \ldots, a_n \rangle \in \mathcal{A}$ such that $a_i - a_m y_i = \gamma_i$ for all $i \neq m$ and we have

$$R(T,X) \equiv \prod_{\gamma \in GF(q)^{n-1}} \left(T + \sum_{i=1, i\neq m}^{n} \gamma_i X_i \right) \mod \sum_{i=1}^{n} y_i X_i.$$

The above polynomial is linear over $GF(q)$ in T and so

$$R(T,X) \equiv T^{q^{n-1}} + \sum_{k=0}^{n-2} \sigma_{q^{n-1}-q^k}(X) T^{q^k} + \sigma_{q^{n-1}}(X) \mod \sum_{i=1}^{n} y_i X_i$$

and we conclude that

$$\sigma_j(X) \equiv 0 \mod \sum_{i=1}^{n} y_i X_i,$$

whenever $j \neq q^{n-1}$ and $j \neq q^{n-1} - q^k$ for some k. Hence for each $P = \langle 0, y_1, y_2, \ldots, y_n \rangle \in \pi_\infty \setminus \mathcal{D}$

$$\sum_{i=1}^{n} y_i X_i \mid \sigma_j(X)$$

in these cases and so $\sigma_j(X) \equiv 0$ whenever $deg(\sigma_j) \leq j < |\pi_\infty \setminus \mathcal{D}|$. By hypothesis $|\pi_\infty \setminus \mathcal{D}| \geq p^e q$ and so we can write

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

Now let $x \in GF(q)^n$ be any vector in n coordinates and let d be maximal such that $R(T, x) \in GF(q)[T^{p^d}] \setminus GF(q)[T^{p^{d+1}}]$. We wish to prove that $d \geq e+1$. Write $R(T, x) = S(T)^{p^d}$, so $S \in GF(q)[T] \notin GF(q)[T^p]$ and importantly $\frac{\partial S}{\partial T} \neq 0$. Moreover

$$S(T) = T^{q^{n-1}/p^d} + S_1(T),$$

where $deg(S_1) \leq q^{n-1}/p^d - qp^{e-d}$. Since $S(T)$ is the product of linear factors

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

The degree of the right-hand side of this divisibility is less than $q + deg(S_1) \leq q + q^{n-1}/p^d - qp^{e-d}$.

If $d \leq e$ the degree of the left-hand side, which is the degree of S and equal to q^{n-1}/p^d, will be greater than the degree of right-hand side and we conclude that the right-hand side of the divisibility must be zero. However this implies that $\frac{\partial S}{\partial T}$ is zero, a contradiction, hence $d \geq e+1$.

We have shown that for all $x \in GF(q)^n$

$$R(T, x) = \prod_{\langle 1, a_1, \ldots, a_n \rangle \in \mathcal{A}} \left(T + \sum_{i=1}^{n} a_i x_i \right) \in GF(q)[T^{p^{e+1}}]$$

and so all its factors $T + \alpha$ occur with multiplicity a multiple of p^{e+1}. Hence there are a multiple of p^{e+1} points of $\mathcal{A}$ satisfying

$$\sum_{i=1}^{n} a_i x_i = \alpha,$$

or in other words there are 0 modulo p^{e+1} points of $\mathcal{A}$ on the hyperplane defined by the equation

$$\sum_{i=1}^{n} x_i X_i = \alpha.$$

This concludes the proof. $\square$

6 Rédei polynomials for polar spaces

Let us look at a possible application to polar spaces of higher rank. We hope that, following the success of using Rédei polynomials for $Q(4,q)$ they may be equally useful. By means of demonstrating how this may be done, consider an ovoid $\mathcal{O}$ of the polar space $Q(6,q)$ defined by the quadratic form

$$X_0X_6 + X_1X_5 + X_2X_4 + X_3^2.$$

Now we can assume that $\langle 1,0,0,0,0,0,0\rangle$ is a point of $\mathcal{O}$ and so the hyperplane $X_6 = 0$, the tangent space at $\langle 1,0,0,0,0,0,0\rangle$, is incident with no other points of $\mathcal{O}$. Let

$$\mathcal{A} := \{(x_1,x_2,x_3,x_4,x_5) \mid (-x_1x_5 - x_2x_4 - x_3^2, x_1,x_2,x_3,x_4,x_5,1) \in \mathcal{O}\},$$

a set of q^3 elements of $GF(q)^5$ and define the Rédei polynomial

$$R(T,Y_1,Y_2,Y_3,Y_4) := \prod_{(x_1,x_2,x_3,x_4,x_5)\in\mathcal{A}} (T + x_1Y_1 + x_2Y_2 + x_3Y_3 + x_4Y_4 + x_5).$$

As before we define polynomials σ_j, now in four indeterminates and of total degree at most j, by writing

$$R(T,Y_1,Y_2,Y_3,Y_4) = \sum_{j=0}^{q^3} \sigma_j(Y_1,Y_2,Y_3,Y_4) T^{q^3-j}.$$

Let a, b and c be any elements of $GF(q)$ and consider the factors of the polynomial

$$R(T, -aY_3 - bY_4 + a^2, -cY_3 + c^2Y_4 + b + 2ac, Y_3, Y_4)$$

$$= \prod_{(x_1,x_2,x_3,x_4,x_5)\in\mathcal{A}} (T + (x_3 - cx_2 - ax_1)Y_3 + (x_4 + c^2x_2 - bx_1)Y_4 + x_5 + (b+2ac)x_2 + a^2x_1).$$

Now $T+\alpha Y_3+\beta Y_4+\gamma$ occurs as a factor if and only if there is an element of $\mathcal{A}$ such that

$$x_3 - cx_2 - ax_1 = \alpha,$$
$$x_4 + c^2x_2 - bx_1 = \beta,$$
$$x_5 + (b+2ac)x_2 + a^2x_1 = \gamma.$$

These equations define a three-dimensional affine subspace Σ of the $AG(6,q)$ defined by the equation $X_6 = 1$. The projective plane π defined by the equations

$$X_6 = 0,$$
$$X_3 - cX_2 - aX_1 = 0,$$
$$X_4 + c^2X_2 - bX_1 = 0,$$
$$X_5 + (b+2ac)X_2 + a^2X_1 = 0.$$

is the plane $\langle(1,0,0,0,0,0,0),(0,1,0,a,b,-a^2,0,),(0,0,1,c,-c^2,-b-2ac,0)\rangle$ and is totally isotropic. So the quadratic form restricted to be the three-dimensional projective space $\Sigma \cup \pi$ is degenerate (it is totally singular on the plane π). Hence the form factorises into two linear factors when restricted to this space and so there is another totally isotropic plane π' contained in Σ. This plane is incident with a unique point of $\mathcal{O}$ and so Σ is incident with a unique point of $\mathcal{O}$. So, for every a, b and c in $GF(q)$ and α, β and γ there is exactly one element of $\mathcal{A}$ satisfying the equations above. In other words

$$\begin{aligned} &R(T, -aY_3 - bY_4 + a^2, -cY_3 + c^2Y_4 + b + 2ac, Y_3, Y_4) \\ &= \prod_{(\alpha,\beta,\gamma)\in GF(q)^3} (T + \alpha Y_3 + \beta Y_4 + \gamma) \\ &= T^{q^3} + \text{terms of degree at most } q^2 \text{ in } T, \end{aligned}$$

where the last equality follows from the fact that the expression is linear over $GF(q)$ in T. Hence for $1 \le j \le q^3 - q^2 - 1$,

$$\sigma_j(-aY_3 - bY_4 + a^2, -cY_3 + c^2Y_4 + b + 2ac, Y_3, Y_4) \equiv 0.$$

This certainly implies that $\sigma_j(Y_1, Y_2, Y_3, Y_4) \equiv 0$ for $1 \le j \le q-1$ but it is not clear to us if this implies that more of the σ_j are identically zero. Arguing as in the case for $Q(4,q)$ we can obtain the following theorem which can also be deduced from the corresponding theorem for $Q(4,q)$, see [5].

Theorem 6.1 *A hyperplane of $PG(6,q)$ meets an ovoid of $Q(6,q)$ in 1 mod p points.*

If one was able to prove that $\sigma_j(Y_1, Y_2, Y_3, Y_4) \equiv 0$ for $1 \le j \le p^e q - 1$ this would lead to a theorem saying that every hyperplane meets an ovoid in 1 mod p^{e+1} points. Some random computer searching with the known examples suggests that 1 mod q may be true for ovoids of $Q(6,q)$ and 1 mod p^h for ovoids of $Q(4,p^{2h})$ or $Q(4,p^{2h+1})$. For a list of the known examples of ovoids of orthogonal polar spaces we refer to [18].

References

[1] N. Alon and M. Tarsi, A nowhere-zero point in linear mappings. *Combinatorica*, **9** (1989) 393–395.

[2] S. Ball, On intersection sets in Desarguesian affine spaces, *European J. Combin.*, **21** (2000) 441–446.

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

[4] S. Ball and M. Lavrauw, On the graph of a function in two variables over a finite field, preprint.

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

[6] 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.

[7] A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory Ser. A*, **24** (1978) 251–253.

[8] A. A. Bruen, Polynomial multiplicities over finite fields and intersection sets, *J. Combin. Theory Ser. A*, **60** (1992) 19–33.

[9] J. De Beule and K. Metsch, Minimal blocking sets of size q^2+2 of $Q(4,q)$, q an odd prime, do not exist, preprint.

[10] A. Gács, On a generalization of Rédei's theorem, *Combinatorica*, **23** (2003) 585–598.

[11] F. Jaeger, Problem presented in the *6th Hungar. Comb. Coll., Eger,* Hungary 1981, and: *Finite and Infinite Sets* (eds: A. Hajnal, L. Lovász and V. Sós). North Holland, Amsterdam, 1982 II, 879.

[12] R. Jamison, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A*, **22** (1977) 253–266.

[13] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.*, **16** (1981) 449–454.

[14] S. E. Payne and J. A. Thas, *Finite generalized quadrangles*, Research Notes in Mathematics 110, Pitman, 1984.

[15] L. Rédei, *Lückenhafte Polynome über endlichen Körpen*, Birkhäuser-Verlag, Basel, 1970. (English translation: *Lacunary Polynomials over finite fields*, North-Holland, Amsterdam, 1973.)

[16] 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.

[17] T. Szőnyi, A. Gács and Z. Weiner, On the spectrum of minimal blocking sets in $\mathrm{PG}(2,q)$, *J. Geom*, **76** (2003) 256–281.

[18] B. Williams, Ovoids of parabolic and hyperbolic spaces, Ph.D thesis, 1999; available from `http://cage.ugent.be/~nick/Theses/theses.html`.