Symplectic spreads and permutation polynomials

Simeon Ball [*]
Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya
Mòdul C3, Campus Nord
08034 Barcelona, Espanya.
simeon@mat.upc.es

Michael Zieve
Center for Communications Research
805 Bunn Drive
Princeton, NJ 08540–1966
USA.
zieve@idaccr.org

22 September 2003

Abstract

Every symplectic spread of $PG(3,q)$, or equivalently every ovoid of $Q(4,q)$, is shown to give a certain family of permutation polynomials of $GF(q)$ and conversely. This leads to an algebraic proof of the existence of the Tits-Lüneburg spread of $W(2^{2h+1})$ and the Ree-Tits spread of $W(3^{2h+1})$, as well as to a new family of low-degree permutation polynomials over $GF(3^{2h+1})$.

Let $PG(3,q)$ denote the projective space of three dimensions over $GF(q)$. A *spread* of $PG(3,q)$ is a partition of the points of the space into lines. A spread is called *symplectic* if every line of the spread is totally isotropic with respect to a fixed non-degenerate alternating form. Explicitly, the points of $PG(3,q)$ are equivalence classes of nonzero vectors (x_0,x_1,x_2,x_3) over $GF(q)$ modulo multiplication by $GF(q)^*$. Since all non-degenerate alternating forms on $PG(3,q)$ are equivalent (cf. [9, p. 587] or [12, p. 69]), we may use the form

$$((x_0,x_1,x_2,x_3),(y_0,y_1,y_2,y_3)) = x_0y_3 - x_3y_0 - x_1y_2 + y_1x_2. \tag{1}$$

Then a symplectic spread is a partition of the points of $PG(3,q)$ into lines such that $(P,Q)=0$ for any points P,Q lying on the same line of the spread.

Symplectic spreads are equivalent to other objects. A symplectic spread is a spread of the generalised quadrangle $W(q)$ (sometimes denoted as $Sp(4,q)$), whose points are the points of $PG(3,q)$ and whose lines are the totally isotropic lines with respect to a non-degenerate alternating form. By the Klein correspondence (see for example [4], [12, pp. 189] or [15]), a spread of $W(q)$ gives an ovoid of the generalised quadrangle $Q(4,q)$ (sometimes denoted $O(5,q)$) and vice-versa.

Let $\mathcal{S}$ be a spread of $PG(3,q)$. There are q^3+q^2+q+1 points in $PG(3,q)$, and each line contains $q+1$ points. Since $\mathcal{S}$ is a partition of the points of $PG(3,q)$ into lines, it contains exactly q^2+1

[*]This author acknowledges the support of the Ministerio de Ciencia y Tecnologia, España.

lines. The group $PGL(4,q)$ acts transitively on the lines of $PG(3,q)$, so let us assume that $\mathcal{S}$ contains the line l_∞, which we define as

$$\langle (0,0,0,1),(0,0,1,0)\rangle.$$

The plane $X_0 = 0$ contains l_∞, so each of the other q^2 lines of the spread contains precisely one of the q^2 points $\{\langle (0,1,x,y)\rangle \mid x,y \in GF(q)\}$. The plane $X_1 = 0$ also contains l_∞, so the other q^2 lines of the spread are given by two functions f and g such that

$$\mathcal{S} = l_\infty \cup \{\langle (0,1,x,y),(1,0,f(x,y),g(x,y)\rangle \mid x,y \in GF(q)\}.$$

The spread condition is satisfied if and only if for each $a \in GF(q)$ the plane $X_1 = aX_0$ is partitioned by the lines of the spread. These planes contain l_∞ and meet the other lines of $\mathcal{S}$ in the points

$$\{\langle (1,a,ax+f(x,y),ay+g(x,y))\rangle \mid x,y \in GF(q)\}.$$

Hence the spread condition is satisfied if and only if

$$(x,y) \mapsto (ax+f(x,y),ay+g(x,y))$$

is a permutation of $GF(q)^2$ for all $a \in GF(q)$.

We are interested here in symplectic spreads. The line l_∞ is totally isotropic with respect to the form (1). The other lines of the spread are totally isotropic with respect to the form (1) if and only if for all x and $y \in GF(q)$

$$((0,1,x,y),(1,0,f(x,y),g(x,y)) = -y - f(x,y)$$

is zero. Hence

$$\mathcal{S} := l_\infty \cup \{\langle (0,1,x,y),(1,0,-y,g(x,y)\rangle \mid x,y \in GF(q)\}$$

will be a symplectic spread if and only if

$$(x,y) \mapsto (ax-y, ay+g(x,y)) \tag{2}$$

is a permutation of $GF(q)^2$ for all $a \in GF(q)$. Now make the substitution $b = ax - y$ to see that this is equivalent to $x \mapsto a(ax-b)+g(x,ax-b)$ being a permutation of $GF(q)$ for all $a,b \in GF(q)$, which is equivalent to $x \mapsto g(x,ax-b)+a^2x$ being a permutation of $GF(q)$ for all $a,b \in GF(q)$.

Although merely an observation, this fact seems not to have been noted before, and as we shall see it can be quite useful. So let us formulate this in a theorem.

Theorem 1 *The set of totally isotopic lines*

$$l_\infty \cup \{\langle (0,1,x,y),(1,0,-y,g(x,y))\rangle \mid x,y \in GF(q)\}$$

is a (symplectic) spread if and only if

$$x \mapsto g(x,ax-b)+a^2x$$

is a permutation of $GF(q)$ for all $a,b \in GF(q)$. ■

name	$g(x,y)$	q	restrictions
regular	$-nx$	odd	n non-square
Kantor [8]	$-nx^{\alpha}$	odd	n non-square, $\alpha \vert q$
Thas-Payne [14]	$-nx-(n^{-1}x)^{1/9}-y^{1/3}$	3^h	n non-square, $h>2$
Penttila-Williams [11]	$-x^9-y^{81}$	3^5	
Ree-Tits slice [8]	$-x^{2\alpha+3}-y^{\alpha}$	3^{2h+1}	$\alpha=\sqrt{3q}$
regular	$cx+y$	even	$Tr_{q\to 2}(c)=1$
Tits-Lüneburg [15]	$x^{\alpha+1}+y^{\alpha}$	2^{2h+1}	$\alpha=\sqrt{2q}$

Table 1: The known examples of symplectic spreads of $PG(3,q)$

Symplectic spreads of $PG(3,q)$ are rare. All the known examples are given in Table 1 which comes from [11]. In particular, the *regular* spreads are those for which the polynomial $g(x,y)$ has total degree 1. The main result in [3] implies that when q is prime, symplectic spreads of $PG(3,q)$ are regular.

Note that from any of the examples in the table we could make many other equivalent symplectic spreads and that the function $g(x,y)$ will not in general have such a nice form. For instance, all the examples in the table give spreads $\mathcal{S}$ that contain the line l

$$\langle(0,1,0,0),(1,0,0,0)\rangle.$$

The linear map τ that switches X_0 and X_3 and switches X_1 and X_2 preserves the form (1) but swiches l_∞ and l. The other q^2-1 lines in $\mathcal{S}$ are mapped to the lines

$$\{\langle(y,x,1,0),(g(x,y),-y,0,1)\rangle \mid x,y\in GF(q),\ (x,y)\neq(0,0)\}$$

by τ. Writing these lines as the spans of their points on the planes $X_0=0$ and $X_1=0$, these lines are

$$\{\langle(0,1,u,v),(1,0,-v,\frac{-vx}{y})\rangle \mid x,y\in GF(q),\ (x,y)\neq(0,0)\},$$

where

$$u=\frac{g(x,y)}{xg(x,y)+y^2}$$

and

$$v=\frac{-y}{xg(x,y)+y^2}.$$

(When $y=0$ we interpret $-vx/y$ to be $1/g(x,0)$.) Now one would have to calculate $-vx/y$ in terms of u and v to deduce the function $g(x,y)$ for the spread $\tau(\mathcal{S})$. For an explicit example of this, consider the Kantor spread $\mathcal{S}$ over $GF(27)$ with $g(x,y)=-nx^3$, where $n^3-n=-1$. The function $g(u,v)$ for $\tau(\mathcal{S})$ is

$$nu^{21}v^4+n^8u^{19}v^{18}+n^2u^{17}v^6+n^4u^9v^{10}+n^{18}u^5v^{12}+n^{12}u^3.$$

A polynomial h in one variable over $GF(q)$ is called *additive* if $h(x+u)=h(x)+h(u)$ for all $x,u\in GF(q)$. In case $g(x,y)=h_1(x)+h_2(y)$ with h_1 and h_2 being additive polynomials, the symplectic spread corresponds to a translation ovoid of $Q(4,q)$, which in turn comes from a semifield flock of the quadratic cone in $PG(3,q)$. This has been the subject matter of a number of articles, see for example [1], [2] or [10]. The classification of such examples is an open problem whose solution would be of much interest. The partial classification in [2] implies that if there are any further examples over $GF(p^h)$ then $p < 4h^2 - 8h + 2$. Theorem 1 in this case reads: The polynomial $g(x,y) = h_1(x) + h_2(y)$ will give a symplectic spread if and only if $h_1(x) + h_2(ax) + a^2x$ is a permutation polynomial for all $a \in GF(q)$, or equivalently $h_1(x) + h_2(ax) + a^2x$ has no zeros in $GF(q)^*$ for all $a \in GF(q)$.

The two examples where $g(x,y)$ is not of this form are the Tits-Lüneburg spread and the Ree-Tits spread.

Let us first check the Tits-Lüneburg example, where $\alpha = \sqrt{2q}$. In this case

$$g(x, ax - b) + a^2x = x^{\alpha+1} + (ax)^\alpha - b^\alpha + a^2x.$$

So we should have that $x^{\alpha+1} + (ax)^\alpha + a^2x$ is a permutation polynomial for all $a \in GF(q)$, which is easy to see since this polynomial is $(x + a^\alpha)^{\alpha+1} + a^{\alpha+2}$. Note that composing permutation polynomials with permutation polynomials gives permutation polynomials so it is enough to check that $x^{\alpha+1}$ is a permutation polynomial, which it is since $(2^{h+1}+1, 2^{2h+1}-1) = 1$.

Now we come to the interesting Ree-Tits slice example, $g(x,y) = -x^{2\alpha+3} - y^\alpha$ where $q = 3^{2h+1}$ and $\alpha = \sqrt{3q}$. This spread was discovered by Kantor [8] as an ovoid of $Q(4,q)$. It is the slice of the Ree-Tits ovoid of $Q(6,q)$. It provides us with an interesting class of permutation polynomials, namely, the polynomials $f_a(x) := b^\alpha - (g(x, ax-b) + a^2x)$,

$$f_a(x) = x^{2\alpha+3} + (ax)^\alpha - a^2x.$$

The polynomial f_a is remarkable in that it is a permutation polynomial over $GF(q)$ whose degree is approximately $\sqrt{q}$. There are only a handful of known permutation polynomials with such a low degree. The bulk of these examples are *exceptional polynomials*, namely polynomials over $GF(q)$ which permute $GF(q^n)$ for infinitely many values n. However, we will show below that f_a is not exceptional, so long as $\alpha > 3$ and $a \neq 0$. There are also some non-exceptional permutation polynomials of degree approximately $\sqrt{q}$ in case q is a square or a power of 2. However, our example is the first for which q is an odd nonsquare.

It follows from [8] and Theorem 1 that f_a is a permutation polynomial. Conversely we now give a direct proof that f_a is a permutation polynomial, which (along with Theorem 1) gives a new proof that the Ree-Tits examples are in fact symplectic spreads. Our proof that f_a is a permutation polynomial uses the method of Hans Dobbertin [5].

Theorem 2 *Let $q = 3^{2h+1}$ and let $\alpha = \sqrt{3q}$. For all $a \in GF(q)$ the polynomial $f_a(x) := x^{2\alpha+3} + (ax)^\alpha - a^2x$ is a permutation polynomial over $GF(q)$.*

Proof. If $f_a(x)$ is a permutation polynomial then so is $\zeta^{2\alpha+3} f_a(x/\zeta)$ for any $\zeta \in GF(q)^*$, and the latter polynomial equals $f_{a\zeta^{\alpha+1}}(x)$. Since $(\alpha+1, q-1) = 2$, it follows that if f_a is a permutation polynomial then so is $f_{a\zeta^2}$ for any $\zeta \in GF(q)^*$. Thus it suffices to verify the theorem for a single nonzero square a, a single nonsquare a, and the value $a = 0$ (in which case the theorem is trivial). Since -1 is a non-square in $GF(3^{2h+1})$ we can assume from now on that $a^2 = 1$.

Suppose that f_a is not a permutation polynomial. Let x, y be distinct elements of $GF(q)$ such that $f_a(x) = f_a(y) = d$. The equations $f_a(x) = d$ and $f_a(x)^\alpha = d^\alpha$ give

$$x^{2\alpha+3} + ax^\alpha - x = d \tag{3}$$
$$x^{6+3\alpha} + ax^3 - x^\alpha = d^\alpha. \tag{4}$$

By viewing these equations as low-degree polynomials in x^α whose coefficients are low-degree polynomials in x, we can solve for x^α as a low-degree rational function in x. Namely, multiplying (3) by $x^{\alpha+3}$ and then subtracting (4) gives

$$ax^{2\alpha+3} - x^{\alpha+4} - ax^3 + x^\alpha = dx^{\alpha+3} - d^\alpha; \tag{5}$$

multiplying (3) by a and subtracting (5) gives

$$x^\alpha(x^4 + dx^3) = ax + da - ax^3 + d^\alpha. \tag{6}$$

This expresses x^α as a low-degree rational function in x, so long as $x \notin \{0, -d\}$. For later use we record this equation in the form $F(x^\alpha, x) = 0$ where

$$F(T, U) := U^4T + dU^3T - aU - da + aU^3 - d^\alpha.$$

Note that x and y are not both in $\{0, -d\}$, for if so then $d = f_a(0) = 0$ so $x = y = 0$, contradiction. Thus, by swapping x and y if necessary, we may assume $x \notin \{0, -d\}$.

Solving for x^α in (6) and substituting into (3) gives a low-degree polynomial satisfied by x:

$$(ax + da - ax^3 + d^\alpha)^2 + a(x + d)(ax + da - ax^3 + d^\alpha) = (x^2 + dx)^3.$$

By expanding this equation we get

$$(d^\alpha a - d^3)x^3 - x^2 + dx - d^2 + d^{2\alpha} = 0. \tag{7}$$

Next we handle the cases $y = 0$ and $y = -d$. If $y = 0$ then $d = f_a(y) = 0$ and (7) implies $x = 0$, contradiction. If $y = -d$ then the analogue of (6) with y in place of x says that $d^\alpha = -ad^3$, so $d^{2\alpha-6} = 1$ and since $(q-1, 2\alpha-6) = 2$ that $d^2 = 1$ and hence $a = -1$. Then equation (7) simplifies to $dx(x + d)^2 = 0$. Since $d = 0$ implies $x = 0$ we have $x \in \{0, -d\}$, again a contradiction.

Hence we may assume $y \notin \{0, -d\}$, and moreover we may assume $d \neq 0$ and $d^3 \neq -d^\alpha a$. We can also assume that $d^3 \neq d^\alpha a$. For, if $d^3 = d^\alpha a$ then $d^{2\alpha-6} = 1$ and again since $(q-1, 2\alpha-6) = 2$ that $d^2 = 1$ and hence $a = 1$. Then equation (7) simplifies to $x(x + d) = 0$, a contradiction.

In particular, equation (7) remains valid if we substitute y for x. Thus x and y are roots of the polynomial

$$\psi(t) := (d^\alpha a - d^3)t^3 - t^2 + dt - d^2 + d^{2\alpha}. \tag{8}$$

We express the roots of $\psi(t)$ in terms of x. Since $\psi(x) = 0$, we know that $t - x$ is a factor of $\psi(t)$: in fact, writing $A := d^\alpha a - d^3$, we have

$$\psi(t)/(t - x) = At^2 + (Ax - 1)t + (Ax^2 + d - x). \tag{9}$$

The discriminant of this quadratic polynomial is

$$\delta := (Ax-1)^2 - A(Ax^2+d-x) = 1 - A(x+d).$$

If $\delta = 0$ then $x = -d + 1/A$ and $y = (Ax-1)/A = -d$ which we have already excluded, so assume from now on that $\delta \neq 0$.

Substituting $d = x^{2\alpha+3} + ax^{\alpha} - x$ we find that

$$A = -x^{6\alpha+9} + ax^{3\alpha+6} - ax^{3\alpha} - ax^{\alpha} - x^3$$

and

$$\delta = (x^{4\alpha+6} - ax^{3\alpha+3} + x^{2\alpha} + ax^{\alpha+3} - 1)^2.$$

Thus putting $\sqrt{\delta} = x^{4\alpha+6} - ax^{3\alpha+3} + x^{2\alpha} + ax^{\alpha+3} - 1$, we can write the roots of $\psi(t)/(t-x)$ as

$$y_1 := x - (\sqrt{\delta}+1)/A = \frac{x^{3\alpha+4} + ax^{2\alpha+1} + x^{\alpha} + ax}{x^{3\alpha+3} + ax^{2\alpha} + a}$$

and

$$y_2 := x + (\sqrt{\delta}-1)/A = \frac{x^{3\alpha+7} - ax^{2\alpha+4} - x^{\alpha+3} + x^{\alpha+1} + ax^4 - a}{x^{3\alpha+6} - ax^{2\alpha+3} + x^{\alpha} + ax^3}.$$

Now one can verify that $F(y_2^{\alpha}, y_1) = 0$ and $F(y_1^{\alpha}, y_2) = 0$. But we know that $F(y^{\alpha}, y) = 0$ and $y \in \{y_1, y_2\}$. Since $y_1 \neq y_2$, this implies $F(T, y) = 0$ has more than one root. But this is a linear polynomial in T, a contradiction. ∎

Recall that a polynomial f over $GF(q)$ is called *exceptional* if it permutes $GF(q^n)$ for infinitely many n. We now show that, except in some special cases, f_a is not exceptional. Our proof relies on the classification of monodromy groups of indecomposable exceptional polynomials, due to Fried, Guralnick, and Saxl [6]. A polynomial is *indecomposable* if it is not the composition of two polynomials of lower degree.

Lemma 1 *When $\alpha > 3$ and $a \neq 0$, $f_a(x)$ is indecomposable.*

Proof. The derivative of f_a is $f_a' = -a^2$, which is a nonzero constant. If $f_a(x) = g(h(x))$ then $-a^2 = f_a'(x) = g'(h(x))h'(x)$, so both g' and h' are nonzero constants. Thus $g(x) = u(x^3) + cx$ and $h(x) = v(x^3) + dx$ for some polynomials u and v and nonzero constants c and d. Since the degree of f_a is not divisible by 9, either g or h has degree not divisible by 3, and hence must have degree 1. Thus f_a is indecomposable. ∎

Theorem 3 *When $\alpha > 3$ and $a \neq 0$, $f_a(x)$ is not exceptional.*

Proof. This follows directly from the preceeding lemma and [6, Theorems 13.6 and 14.1], according to which there is no indecomposable exceptional polynomial of degree $2\alpha + 3$ over a finite field of characteristic 3. ∎

In all the examples in Table 1 the polynomial g is of the form $g(x,y) = h_1(x) + h_2(y)$. In Glynn [7] such a polynomial $g(x,y)$ with this property is called *separable*. Every known example of a symplectic spread of $PG(3,q)$ is equivalent to a symplectic spread with $g(x,y)$ separable. In the examples not only is the polynomial $g(x,y) = h_1(x) + h_2(y)$ separable but $h_2(y) = Cy^\sigma$, where $y \mapsto y^\sigma$ is an automorphism of $GF(q)$. We can classify these examples in the case when q is even using Glynn's Hering classification of inversive planes [7].

Theorem 4 *Let q be even. If $g(x,y) = h_1(x)+Cy^\sigma$ is a separable polynomial that gives a symplectic spread of $PG(3,q)$ then the spread is either a regular spread or a Tits-Lüneburg spread.*

Proof. If $C = 0$ then Theorem 1 implies $h_1(x)+a^2x$ is a permutation polynomial for all $a \in GF(q)$. Let x and y be distinct elements of $GF(q)$, and put $d = (h_1(x)+h_1(y))/(x+y)$. Then $h_1(x)+dx = h_1(y) + dy$, so the polynomial $h_1(x) + dx$ is not a permutation polynomial, a contradiction.

Now assume that $C \neq 0$. Put $z = h_1(x) + Cy^\sigma$ and rewrite this as $y = C^{-1}z^{1/\sigma} - C^{-1}h_1(x)^{1/\sigma}$. Define the function $s(x,z) := C^{-1}z^{1/\sigma} - C^{-1}h_1(x)^{1/\sigma}$. Then $g(x,y) = z$ if and only if $s(x,z) = y$. We have already seen in equation (2) that $g(x,y)$ will give a symplectic spread if and only if

$$(x,y) \mapsto (ax - y, ay + g(x,y))$$

is a permuatation of $GF(q)^2$. This is equivalent to the condition that for all $(x,y) \neq (u,v)$

$$(ax - y, ay + g(x,y)) \neq (au - v, av + g(u,v))$$

for all $a \in GF(q)$. If these pairs were equal then eliminating a this gives the condition that for all $(x,y) \neq (u,v)$

$$(y-v)^2 + (x-u)(g(x,y) - g(u,v)) \neq 0.$$

Now put $z = g(x,y)$ so that $s(x,z) = y$, and put $w = g(u,v)$ so that $s(u,w) = v$. Then we have that $(x,z) \neq (u,w)$

$$(s(x,z) - s(u,w))^2 + (x-u)(z-w) \neq 0.$$

When q is even this is exactly the polynomial condition on such a polynomial $s(x,z)$ that Glynn studies in [7] and that he classifies as coming from either a regular spread or a Tits-Lüneburg spread. ■

When q is odd we can use Thas' classification of flocks of the quadratic cone in $PG(3,q)$ whose planes are incident with a common point from [13] to prove the following theorem. We realise that for many readers familiar with flocks and semifield flocks the next theorem is immediate, but we include a proof for those readers who may not be.

Theorem 5 *Let q be odd. If $g(x,y) = h_1(x)$ is a separable polynomial that gives a symplectic spread of $PG(3,q)$ then the spread is either a regular spread or a Kantor spread.*

Proof.

name	q	Δ	$(q-1,\Delta d)+1$
regular	odd	1	1
Kantor	odd	1	$(q-1,(\alpha-1)/2)+1$
Thas-Payne	3^h	.	q
Penttila-Williams	3^5	11	23
Ree-Tits slice	3^{2h+1}	1	3
regular	even	1	1
Tits-Lüneburg	2^{2h+1}	1	2

Table 2: The class Δ of the known examples of symplectic spreads of $PG(3,q)$

Consider the set of q planes of $PG(3,q)$

$$\{X_0 + h_1(x)X_1 + xX_3 = 0 \mid x \in GF(q)\}.$$

We claim that any two of these planes intersect in a line which is disjoint from the degenerate quadric $X_1X_3 = X_2^2$. Indeed take two planes coordinatised by x and y, $x \neq y$. Then the points in their intersection (z_0, z_1, z_2, z_3) satisfy $(h_1(x) - h_1(y))z_1 + (x-y)z_3 = 0$, and the points which also lie on the degenerate quadric satisfy

$$(h_1(x) - h_1(y))z_1^2 + (x-y)z_2^2 = 0.$$

If $z_1 \neq 0$ then $h_1(x) + (z_2/z_1)^2 x$ is not a permutation polynomial, a contradiction. If $z_1 = 0$ then $z_2 = 0$ and $z_0 = -xz_3 = -yz_3$. But $x \neq y$ implies that $z_3 = 0$ and $z_0 = 0$ which is nonsense. We have shown that the set of planes form a flock of the quadratic cone in $PG(3,q)$. Moreover all these planes are incident with $(0,0,1,0)$. By a theorem of Thas [13] this flock is either linear or of Kantor type. In other words, the spread is either regular or Kantor. ■

In general the permutation polynomial condition from Theorem 1 requires the existence of q^2 permutation polynomials, one for each pair $(a,b) \in GF(q)^2$. If $g(x,y) = h_1(x) + h_2(y)$ and $h_2(y)$ is additive then Theorem 1 simplifies to: The polynomial $g(x,y) = h_1(x)+h_2(y)$ will give a symplectic spread if and only if $f_a(x) := h_1(x) + h_2(ax) + a^2x$ is a permutation polynomial for all $a \in GF(q)$. This condition only requires the existence of q permutation polynomials. Moreover as we saw in the proof of Theorem 2, if the non-zero terms in h_1 and h_2 have suitable degrees, many of these permutation polynomials may be equivalent.

Let us investigate this further. We define a set of polynomials $\{f_a(x) \mid a \in GF(q)\}$ to be of *class* Δ if there exists a t and d such that

$$f_a(bx) = b^t f_{ab^d}(x)$$

for all $b^{q-1/\Delta} = 1$ and a and $x \in GF(q)$. Now we can lessen the condition in Theorem 1 for $\Delta < q-1$.

Theorem 6 *Let the set of q polynomials $\{f_a(x) \mid a \in GF(q)\}$, where $f_a(x) = h_1(x) + h_2(ax) + a^2x$ and h_2 is additive, be of class Δ. The f_a is a permutation polynomial for all $a \in GF(q)$ if and only if f_a is a permutation polynomial for $a = 0$ and $a = \varepsilon^r$, for all $1 \leq r < (q-1,\Delta d)$, where ε is a fixed primitive element.*

Proof. Write $a = \varepsilon^{n_1(q-1,\Delta d)+n_0}$ where $n_0 < (q-1, \Delta d)$. Now choose b such that $b^d = \varepsilon^{-n_1(q-1,\Delta d)}$. ■

In Table 2 we have listed the class for the known examples and the quantity $(q-1, \Delta d) + 1$, the number of permutation polynomials that need to be checked in each case. Inspired by this table we used the mathematical package GAP to look at polynomials over $GF(q)$, $q = p^h$, of the form $g(x, y) = Dx^t + Cy^\sigma$ for all σ a power of p and D and C elements of $GF(q)$ where the corresponding set of polynomials $\{f_a(x) \mid a \in GF(q)\}$ is of class Δ with Δ small. An exhaustive search was carried out for $\Delta \leq 23$ and $q \leq 67^2 = 4489$, $\Delta = 2$ and $q < 3^8 = 6561$, $\Delta = 1$ and $q < 3^9 = 19683$. No new examples of symplectic spreads were found.

References

[1] L. Bader, G. Lunardon, On non-hyperelliptic flocks, *European J. Combin.* **15** (1994), 411–415.

[2] S. Ball, A. Blokhuis and M. Lavrauw, On the classification of semifield flocks, *Adv. Math.*, to appear.

[3] S. Ball, P. Govaerts and L. Storme, On ovoids of $Q(4, q)$ and $Q(6, q)$, preprint.

[4] P. J. Cameron, *Projective and Polar Spaces*, QMW Maths Notes 13, (1991). Updated version,

`http:\\www.maths.qmw.ac.uk\~pjc\pps`

[5] H. Dobbertin, Uniformly representable permutation polynomials, in: *Sequences and their applications*, Springer, 2002, pp.1–22.

[6] M. Fried, R. Guralnick and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* **82** (1993), 157–225.

[7] D. G. Glynn, The Hering classification for inversive planes of even order, *Simon Stevin* **58** (1984), 319–353.

[8] W. Kantor, Ovoids and translation planes, *Canad. J. Math.* **34** (1982), 1195–1207.

[9] S. Lang, *Algebra*, Third Edition, Addison Wesley, 1993.

[10] M. Lavrauw, *Scattered subspaces with respect to spreads and eggs in finite projective spaces*, Ph. D. thesis, Technical University of Eindhoven, The Netherlands, 2001.

[11] T. Penttila and B. Williams, Ovoids of parabolic spaces, *Geom. Dedicata* **82** (2000), 1–19.

[12] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, 1992.

[13] J. A. Thas, Generalized quadrangles and flocks of cones, *European J. Combin.* **8** (1987), 441–452.

[14] J. A. Thas and S. E. Payne, Spreads and ovoids in finite generalised quadrangles, *Geom. Dedicata* **52** (1994), 227–253.

[15] J. Tits, Ovoides et Groupes de Suzuki, *Arch. Math.* XIII (1962), 187–198.