Quadrics and Difference Sets

W.–A. Jackson
Department of Pure Mathematics
The University of Adelaide
Adelaide SA 5005
Australia

K.A.S. Quinn
Department of Mathematics and Computing
Roehampton Institute
Southlands College
Wimbledon Parkside
London U.K. SW19 5NN

P.R. Wild
Department of Mathematics
Royal Holloway and Bedford New College
Egham Hill, Egham
Surrey U.K. TW20 OEX

ABSTRACT. Let L be a linear form on the Galois field $GF(q^{n+1})$ over $GF(q)$ ($n \geq 2$). We characterize those integers s coprime to $v = (q^{n+1} - 1)/(q - 1)$ such that $L(x^s)$ is (or is related to) a quadratic form on $GF(q^{n+1})$ over $GF(q)$. This relates to a conjecture of Games concerning quadrics of the form rD in $\mathrm{PG}(n, q)$, where D is a difference set in the cyclic group Z_v acting as a Singer group on the points and hyperplanes of $\mathrm{PG}(n, q)$. It has been shown that Games' conjecture does not hold except possibly in the case $q = 2$: here we establish that it holds exactly when $q = 2$. We also suggest a new conjecture. Our result for $q = 2$ enables us to prove another conjecture of Games', concerning m-sequences with three-valued periodic cross-correlation function.

ARS COMBINATORIA 42(1996), pp. 97-106

1 Introduction

Let $\mathrm{PG}(n,q)$ be the projective geometry of dimension $n \geq 2$ over the Galois field $GF(q)$ and let $v = (q^{n+1}-1)/(q-1)$. Let D be a difference set in the cyclic group Z_v acting as a Singer group on the points and hyperplanes of $\mathrm{PG}(n,q)$. We are interested in the following question: for which integers r coprime to v is $rD = \{rd \mid d \in D\}$ a quadric of $\mathrm{PG}(n,q)$?

This question is prompted by [Ga], in which Games gives a construction for perfect ternary sequences. A perfect ternary sequence is a sequence of values from the set $\{-1,0,1\}$ with the property that the periodic autocorrelation function is zero for all non-zero shifts of the sequence. Games constructs a perfect ternary sequence whenever rD is a quadric of $\mathrm{PG}(n,q)$ which has the same size as a hyperplane (that is, r is coprime to v), but is not a hyperplane.

We may consider the points of $\mathrm{PG}(n,q)$ to be the 1–dimensional subspaces of $GF(q^{n+1})$ regarded as a vector space over $GF(q)$. The hyperplanes of $\mathrm{PG}(n,q)$ correspond to linear forms on $GF(q^{n+1})$ over $GF(q)$. Let $L(x)$ be a linear form corresponding to the hyperplane determined by D, let r be coprime to v and let s satisfy $rs \equiv 1 \mod v$. Then rD is a quadric if and only if there is a quadratic form $Q(x)$ on $GF(q^{n+1})$ over $GF(q)$ such that $L(x^s) = 0$ exactly when $Q(x) = 0$.

Note that all the quadrics rD which are hyperplanes are of the following form. Let $q = p^h$, where p is prime. Then p is a multiplier of the difference set D and so p^iD is a translate of D for all integers i. Each associated hyperplane has corresponding linear form $L(\gamma x)$ for some $\gamma \in GF(q^{n+1})$ and may be considered to be a completely degenerate quadric with corresponding quadratic form $Q(x) = (L(\gamma x))^2$.

Let s be an integer. If $L(x^s)$ is a quadratic form and s is coprime to v with $rs \equiv 1 \pmod v$, then by the above it follows that rD is a quadric in $\mathrm{PG}(n,q)$. Games [Ga] has observed that $L(x^s)$ is a quadratic form when $s = q^l + q^m$ for some integers l and m. Here we address the question: for exactly which integers s coprime to v is $Q(x) = L(x^s)$ a quadratic form? We prove that only those congruent modulo $q^{n+1}-1$ to an integer of the form $q^l + q^m$ have this property.

Games [Ga] conjectured that whenever rD is a quadric which is not a hyperplane then r satisfies $r(q^l + q^m) \equiv 1 \pmod v$ for some integers l and m. In [Ja], Jackson and Wild show that Games' conjecture does not hold for any value of q except possibly $q = 2$. As a corollary to the above result we obtain a proof that Games' conjecture holds in the case $q = 2$.

Suppose that $q = 2$ and that D and rD determine two binary m-sequences. When rD is a quadric which is not a hyperplane these sequences have a three-valued cross-correlation function (see Games [Gab]). We prove conjecture 2′ of [Gab], namely that if $n = 2^w - 1$, $w \geq 2$, then $2^l + 2^m$ is coprime to v if and only if $l = m$ and in this case rD is a hyperplane. Thus when $n = 2^w - 1$ such a pair of binary m-sequences of length $2^{n+1} - 1$ cannot arise from a quadric.

It is known [Ja] that whenever r is coprime to v and satisfies $rp^k(q^l + q^m) \equiv 1 \mod v$ for some integers k, l and m, the set rD is a quadric. We conjecture that, except in the case where $n = 2$ and q is odd, these are the only integers r coprime to v for which rD is a quadric. We also make a conjecture for the case where $n = 2$ and q is odd.

2 Notation and Preliminaries

For more details on the following we refer the reader to [De] and [Hi] .

Let $n \geq 2$ and let $g(x) = x^{n+1} + g_n x^n + \cdots + g_1 x + g_0$ be a primitive polynomial over the Galois field $GF(q)$. Let α be a primitive root of g and consider $GF(q^{n+1}) = GF(q)(\alpha)$ as a vector space $V(n+1,q)$ over $GF(q)$. Then any element x of $GF(q^{n+1})$ can be represented as an $(n+1)$-tuple over $GF(q)$. We write $\underline{x} = (x_0, x_1, \ldots, x_n)$ if $x = \sum_{j=0}^{n} x_j \alpha^j$. This gives a one to one correspondence between elements x of $GF(q^{n+1})$ and vectors $\underline{x}$ of $V(n+1,q)$. We denote the set $GF(q^{n+1}) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots, \alpha^{q^{n+1}-2}\}$ by $GF(q^{n+1})^*$, and similarly $GF(q)^* = GF(q) \setminus \{0\}$.

The projective space PG(n,q) has as *points* the 1–dimensional subspaces of $V(n+1,q)$ and as *hyperplanes* the n–dimensional subspaces of $V(n+1,q)$. It can be seen that we can represent each point of PG(n,q) by any non-zero vector in the corresponding 1-dimensional subspace. So $\underline{\alpha}^i$ and $\mu\underline{\alpha}^i$ (where $\mu \in GF(q)^*$) represent the same point. It can be shown that $\underline{\alpha}^i$, $1 \leq i \leq (q^{n+1} - 1)/(q-1)$, represent distinct points in PG(n,q). The hyperplanes too can be represented by non-zero $(n+1)$-tuples $\underline{l} = (l_0, l_1, \ldots, l_n)$, where a point $\underline{x} = (x_0, x_1, \ldots, x_n)$ is incident with $\underline{l} = (l_0, l_1, \ldots, l_n)$ if and only if $\underline{x}\,\underline{l}^T = \sum_{i=0}^{n} l_i x_i = 0$. ($\underline{l}^T$ denotes the transpose of $\underline{l}$.) Thus $\underline{l}$ and $\mu\underline{l}$ (where $\mu \in GF(q)^*$) represent the same hyperplane.

Let $\underline{l}$ be a hyperplane and let $D = \{i \in Z_v \mid \underline{\alpha}^i\,\underline{l}^T = 0\}$. Then D is a Singer difference set in Z_v.

A *linear form* on $GF(q^{n+1})$ over $GF(q)$ is a mapping L: $GF(q^{n+1}) \to GF(q)$ such that $L(\gamma x + \delta y) = \gamma L(x) + \delta L(y)$ for all $\gamma, \delta \in GF(q)$ and all $x, y \in GF(q^{n+1})$. Consider linear forms on $GF(q^{n+1})$ over $GF(q)$. If L is a linear form then there exists an associated element $l \in GF(q^{n+1})$ with $L(x) = \underline{x}\,\underline{l}^T$ for all $x \in GF(q^{n+1})$. Thus there is a correspondence between non-zero linear forms and non-zero vectors of $V(n+1,q)$, and so given a hyperplane represented by tuple $\underline{l}$, then we can associate it with the linear form $L(x) = \underline{x}\,\underline{l}^T$.

If $L(x)$ is a linear form, then for any $a \in GF(q^{n+1})$, $L(ax)$ is also a linear form. As the linear forms $L(ax)$ and $L(bx)$ are distinct for $a, b \in GF(q^{n+1})$,

$a \neq b$, it follows that given any linear form $L'(x)$ there exists $a \in GF(q^{n+1})$ with $L'(x) = L(ax)$ for all $x \in GF(q^{n+1})$.

Let $M_{n+1}(q)$ denote the set of $(n+1) \times (n+1)$ matrices over $GF(q)$. A *bilinear form* is a mapping $B\colon GF(q^{n+1}) \times GF(q^{n+1}) \to GF(q)$ such that B is linear in each variable. In this case there exists $A \in M_{n+1}(q)$ with $B(x,y) = \underline{x}A\underline{y}^T$, for all $x, y \in GF(q^{n+1})$. A *quadratic form* is a mapping $Q\colon GF(q^{n+1}) \to GF(q)$ such that the form $B(x,y)$ defined by $B(x,y) = Q(x+y) - Q(x) - Q(y)$ is bilinear, with $B(x,y) = B(y,x)$ and

$Q(\delta x) = \delta^2 Q(x)$ for all $\delta \in GF(q)$ and all $x, y \in GF(q^{n+1})$. If $Q(x)$ is a quadratic form, it can be shown that there exists $A \in M_{n+1}(q)$ with $Q(x) = \underline{x}A\underline{x}^T$ for all $x \in GF(q^{n+1})$. Thus if B is a bilinear form then $Q(x) = B(x,x)$ is a quadratic form. A *quadric* in $\mathrm{PG}(n,q)$ is the set of points x for which $Q(x) = 0$ for some quadratic form Q on $GF(q^{n+1})$ over $GF(q)$.

We shall need the following result.

Lemma 1. *Let s be an integer coprime to v and let $L(x)$ be a non-zero linear form. Suppose $Q(x) = L(x^s)$ is a quadratic form. Then for any non-zero linear form $L'(x)$ we have that $Q'(x) = L'(x^s)$ is a quadratic form. (All the forms are on $GF(q^{n+1})$ over $GF(q)$.)*

Proof: Let $L'(x)$ be a non-zero linear form. So there exists $a \in GF(q^{n+1})$ with $L'(x) = L(ax)$ for all $x \in GF(q^{n+1})$. Since s is coprime to v there exists integers c, d with $cs + dv = 1$. So $(a^c)^s (a^v)^d = a$. Let $b = a^c \in GF(q^{n+1})$ and $\gamma = (a^v)^d \in GF(q)$. Then $a = \gamma b^s$. Hence $Q'(x) = L'(x^s) = L(ax^s) = \gamma L(b^s x^s) = \gamma Q(bx)$ and it follows that $Q'(x)$ is a quadratic form. □

3 Main Theorem

We now prove our main result. Let $q = p^h$, where p is a prime and $h \geq 1$. Let $n \geq 2$ and recall that $v = (q^{n+1} - 1)/(q-1)$.

Theorem 1. *Let $L(x)$ be a non-zero linear form on $GF(q^{n+1})$ over $GF(q)$ and let s be an integer coprime to v. Then $Q(x) = L(x^s)$ is a quadratic form if and only if $s \equiv q^l + q^m \mod q^{n+1} - 1$ for some integers l and m.*

Proof: That $L(x^s)$ is a quadratic form when $s = q^l + q^m$ for some integers l and m has been observed by Games [Ga]. It remains to prove that if $L(x^s)$ is a quadratic form then s is of the stated form.

Suppose that $Q(x) = L(x^s)$ is a quadratic form on $GF(q^{n+1})$ over $GF(q)$. Since $x^{q^{n+1}-1} = 1$ for all $x \in GF(q^{n+1})^*$ we have $L(x^s) = L(x^{s'})$ when $s \equiv s' \mod q^{n+1} - 1$. Hence we may assume that $0 < s \leq q^{n+1} - 1$. We write $s = (a_n \ldots a_1 a_0)_q$ if

$$s = a_n q^n + a_{n-1} q^{n-1} + \cdots + a_1 q + a_0$$

where for each a_i, $0 \le a_i < q$, so that the a_i are the digits of s in base q notation.

Consider $Q(\delta)$ where $\delta \in GF(q)$. Since $Q(x)$ is a quadratic form, we have $Q(\delta) = \delta^2 Q(1)$. Therefore $L(\delta^s) = \delta^2 L(1^s)$, and by the linearity of L, we have $L(\delta^s - \delta^2) = 0$. Thus, by Lemma 1, $L'(\delta^s - \delta^2) = 0$ for all non-zero linear forms L'. It follows that $\delta^s - \delta^2 = 0$ (for all $\delta \in GF(q)$), and therefore $s \equiv 2 \mod q-1$. That is,

$$a_n q^n + a_{n-1}q^{n-1} + \cdots + a_1 q + a_0 \equiv 2 \pmod{q-1},$$

and as $q \equiv 1 \mod q-1$, it follows that

$$a_n + a_{n-1} \cdots + a_0 \equiv 2 \pmod{q-1}. \qquad 1$$

Since $Q(x)$ is a quadratic form, the form $Q(x+y) - Q(x) - Q(y)$ is bilinear in x and y. Thus $B(x,y) = L((x+y)^s) - L(x^s) - L(y^s)$ is bilinear in x and y. Hence $B(x+y,z) - B(x,z) - B(y,z) = 0$, that is

$$\begin{aligned}&\left[L((x+y+z)^s) - L((x+y)^s) - L(z^s)\right] - \left[L((x+z)^s) - L(x^s) - L(z^s)\right]\\&- \left[L((y+z)^s) - L(y^s) - L(z^s)\right] = 0 \quad \text{for all } x,y,z \in GF(q^{n+1}). \qquad (2)\end{aligned}$$

Using the linearity of L and Lemma 1, equation 2 remains true if every occurrence of L is deleted. Simplifying what remains, we deduce that

$$\begin{aligned}(x+y+z)^s - (x+y)^s - (x+z)^s - (y+z)^s + x^s + y^s + z^s = 0\\ \text{for all } x,y,z \in GF(q^{n+1}).\end{aligned}$$

This equation is a polynomial identity as the degree of each variable is less than q^{n+1}. It holds only if there are no non-trivial $x^u y^v z^w$ terms in the expansion of $(x+y+z)^s$ $(u,v,w > 0)$.

Recall that $q = p^h$, where p is prime. Expanding $(x+y+z)^s$ using multinomial coefficients modulo p, there is a non-trivial $x^u y^v z^w$ term with $u,v,w > 0$ if and only if we can decompose the $s = (s_{nh-1} \dots s_1 s_0)_p$ into a partition of three [Di, p273]. By a partition of three of s we mean $s = u+v+w$, where $u,v,w > 0$, $u = (u_{nh-1} \dots u_1 u_0)_p$, $v = (v_{nh-1} \dots v_1 v_0)_p$, $w = (w_{nh-1} \dots w_1 w_0)_p$, and $s_i = u_i + v_i + w_i$ $(0 \le i \le nh-1)$.

So, for there to be no partition of s into three, we have either $s = p^i$ or $s = p^i + p^j$ for some $i,j \ge 0$. If $s = p^i$ then by equation 1 $p = 2$ and $s = q^l + q^l$ for some $0 \le l \le n$. If $s = p^i + p^j$ then from equation 1 we can conclude that $h \mid i$ and $h \mid j$, so $s = q^l + q^m$ for some $0 \le l,m \le n$. □

Applied to quadrics in PG(n,q) related to Singer difference sets, Theorem 1 yields the following. Let D be a difference set in the cyclic group Z_v acting as a Singer group on the points and hyperplanes of PG(n,q) where $v = (q^{n+1}-1)/(q-1)$. Let $L(x)$ be a linear form associated with the hyperplane corresponding to D. Let r be an integer coprime to v such that rD is a quadric in PG(n, q). Then there is a quadratic form $Q(x)$ for rD, and an integer s with $rs \equiv 1 \pmod v$, such that

$$Q(x) = L(x^s) \quad \text{for all } x \in GF(q^{n+1})$$

if and only if

$$s \equiv q^l + q^m \pmod{q^{n+1} - 1} \quad \text{for some integers } l \text{ and } m.$$

Theorem 1 immediately gives a proof for Games' conjecture for $q = 2$.

Corollary 1. *Let D be a difference set in the cyclic group $Z_{2^{n+1}-1}$ acting as a Singer group on the points and hyperplanes of $PG(n, 2)$. Suppose that r is an integer coprime to $v = 2^{n+1} - 1$. Then rD is a quadric of $PG(n, 2)$ if and only if $r(2^l + 2^m) \equiv 1 \mod v$ for some integers l and m.*

Proof: Suppose that rD is a quadric of PG$(n, 2)$, with corresponding quadratic form $Q(x)$, and let s satisfy $rs \equiv 1 \mod 2^{n+1} - 1$. Let $L(x)$ be a linear form corresponding to the hyperplane associated with D. Then $L(x^s) = 0$ if and only if $Q(x) = 0$. As $L(x^s)$ and $Q(x)$ take values in GF(2), it follows that $L(x^s) = Q(x)$ for all $x \in GF(2^{n+1})$. Hence, by Theorem 1, $s \equiv 2^l + 2^m \mod 2^{n+1} - 1$ for some integers l and m.

As we noted in the introduction, the converse is well known [Ga]. □

4 Occurrence of Non-Hyperplane Quadrics

Let q be a prime power. In this section we examine when there exists $q^l + q^m$ coprime to $(q^{n+1} - 1)/(q - 1)$. For a special class of values of n we apply the result to prove conjecture 2′ of [Gab].

Lemma 2. *Let $n \geq 2$ be an integer and let q be a prime power. Put $v = (q^{n+1} - 1)/(q - 1)$.*

- *(a) If n is even then $q^{\frac{n}{2}} + 1$ is coprime to v.*
- *(b) If n is odd and q is odd then $q^l + q^m$ is not coprime to v for any l, m $(0 \leq l \leq m \leq n)$.*
- *(c) If n is odd and $n = 2^w a - 1$ with $a > 1$ odd, and q is even, then $q^{2^w} + 1$ is coprime to v.*
- *(d) If n is odd and $n = 2^w - 1$ and q is even, then $q^l + q^m$ is not coprime to v for any l, m $(0 \leq l \leq m \leq n)$ unless $l = m$.*

Proof: (a) As $v = q^n + q^{n-1} + \cdots q + 1 = (q^{\frac{n}{2}} + q^{\frac{n}{2}-1} + \cdots + q)(q^{\frac{n}{2}} + 1) + 1$, $q^{\frac{n}{2}} + 1$ is coprime to v. In case (b), both v and $q^l + q^m$ are even, so they are not coprime. For (c) $q^{n+1} - 1 = q^{2^w a} - 1 \equiv (-1)^a - 1 \equiv -2 \mod q^{2^w} + 1$. Hence $q^{2^w} + 1$ is coprime to v.

Consider now case (d). If $n = 2^w - 1$ then

$$v = \prod_{i=0}^{w-1} (q^{2^i} + 1). \qquad 3$$

Now $q^l + q^m = q^l(1 + q^{m-l})$ so it is sufficient to show that $1 + q^m$ is not coprime to v for all m, $0 \le m < 2^w - 1$. If $m = 0$ then $1 + q^m = 2$, and 2 divides v unless q is even; this is the exception above. Otherwise $m \ge 1$ and we can write $m = 2^u t$ where $0 \le u < w$ and t is odd. So $1 + q^m = 1 + (q^{2^u})^t$ and so $1 + q^{2^u}$ divides $1 + q^m$. By equation 3, $1 + q^{2^u}$ also divides v. Thus $1 + q^m$ is never coprime to v if $m \ge 1$. □

The following corollary restates and proves conjecture 2′ of [Gab].

Corollary 2. *Let D be a difference set in the cyclic group $Z_{2^{n+1}-1}$ acting as a Singer group on the points and hyperplanes of $PG(n, 2)$. Suppose that $n = 2^w - 1$ ($w \ge 2$) and r is an integer coprime to $v = 2^{n+1} - 1$. If rD is a quadric then it is completely degenerate, that is, rD is a hyperplane.*

Proof: Suppose rD is a quadric. By Corollary 1, we have $r(2^l + 2^m) \equiv 1 \mod 2^{n+1} - 1$ for some integers l, m. By Lemma 2, $r2^k \equiv 1 \pmod v$ for some k, $1 \le k \le n$. However, 2 is a multiplier of D, so rD is a hyperplane. □

As remarked in the introduction, it follows from Corollary 2 that a pair of binary m-sequences with three-valued cross-correlation function cannot arise from a quadric of PG$(n, 2)$.

5 A Generalisation

Let $q = p^h$ where p is prime and let D be a difference set in Z_v acting as a Singer group on PG(n, q), where $n \ge 2$ and $v = (q^{n+1} - 1)/(q - 1)$. Let $L(x)$ be a linear form on $GF(q^{n+1})$ over $GF(q)$ corresponding to the hyperplane associated with D. Suppose r is coprime to v and rD is a quadric with quadratic form $Q(x) = L(x^{s_0})$ where $s_0 \equiv q^l + q^m \mod (q^{n+1} - 1)$ satisfies $rs_0 \equiv 1 \mod v$. There are $q-1$ residues s modulo $q^{n+1}-1$ such that $rs \equiv 1 \mod v$, namely $s_0 + tv$ $(0 \le t \le q - 2)$. Although $L(x^{s_0+tv})$ may not be a quadratic form, each set $\{x \mid L(x^{s_0+tv}) = 0\}$ represents the same quadric rD with quadratic form $Q(x)$. This follows since $L(x^{s_0+tv}) = (x^v)^t L(x^{s_0})$ as $x^v \in GF(q)$ for all $x \in GF(q^{n+1})$.

For example, in PG$(2, q)$ with difference set D, the set $-D$ is a quadric. We can choose $s = q + q^2$, so $L(x^s)$ is a quadratic form. However, $L(x^{-1})$ is not usually a quadratic form.

The following theorem explains the the relation between $L(x^{s_0+tv})$ and $Q(x)$.

Theorem 2. *Let $L(x)$ be a non-zero linear form on $GF(q^{n+1})$ over $GF(q)$. Let α be a generator of $GF(q^{n+1})$. Let s be an integer coprime to v. Then there exists an element $\delta \in GF(q)^*$ such that*

$$Q(\alpha^i) = \delta^i L(\alpha^{is}) \qquad 4$$

is a quadratic form, if and only if $s \equiv q^l + q^m \mod v$ for some integers l and m.

Proof: Let $\mu = \alpha^v$. Then μ is a generator of $GF(q)$. Now for any integer t,

$$L(\alpha^{i(s+tv)}) = L((\alpha^v)^{ti}\alpha^{is}) = L(\delta^i \alpha^{is}) = \delta^i L(\alpha^{is}) \qquad 5$$

where $\delta = \mu^t \in GF(q)^*$.

Suppose $s + tv = q^l + q^m$ for some integer t. Then $Q(\alpha^i) = L(\alpha^{i(s+tv)})$ is a quadratic form by Theorem 1, and it follows from Equation 5 that $Q(x)$ given by Equation 4 is a quadratic form.

Conversely, suppose that there exists $\delta \in GF(q)^*$ such that $Q(x)$ given by Equation 4 is a quadratic form. Since μ is a generator of $GF(q)$, there exists an integer $t < q - 1$ with $\delta = \mu^t$. So, from Equation 4, $Q(\alpha^i) = \delta^i L(\alpha^{is}) = L(\delta^i \alpha^{is}) = L(\alpha^{i(s+tv)})$. By Theorem 1, $s + tv$ is of the form $q^l + q^m$, as required. □

As we noted in the introduction, if r is an integer coprime to v such that $rp^k(q^l + q^m) \equiv 1 \mod v$, then rD is a quadric of $PG(n, q)$. The following is effectively a generalisation of Theorem 1 and Theorem 2 to cover all these values of r.

Theorem 3. *Let $L(x)$ be a non-zero linear form on $GF(q^{n+1})$ over $GF(q)$. Let s be an integer coprime to $v = (q^{n+1} - 1)/(q - 1)$ and let k be an integer. Then $Q(x) = L(x^s)^{p^k}$ is a quadratic form if and only if $sp^k \equiv (q^l + q^m) \mod q^{n+1} - 1$ for some integers l and m. Further, there exists an element $\delta \in GF(q)^*$ such that $Q(\alpha^i) = \delta^i L(\alpha^{is})$ is a quadratic form, if and only if $s \equiv q^l + q^m \pmod v$ for some integers l and m.*

Proof: It is easy to check that $L'(x) = L(x^{p^{h-1}})^p$ is a linear form if and only if $L(x) = L'(x^p)^{p^{h-1}}$ is a linear form. Thus for any integer k we have $Q(x) = L(x^s)^{p^k} = L'(x^{sp^k})$ for some linear form $L'(x)$. The result follows on applying Theorem 1 and Theorem 2 to $L'(x)$. □

6 A Conjecture

Our conjecture is as follows. Let $q = p^h$ and $v = (q^{n+1} - 1)/(q - 1)$. Note that $p^{h(n+1)} \equiv 1 \pmod v$. Hence $sp^k \equiv q^l + q^m \pmod v$ if and only if $s \equiv p^{k'}(q^l + q^m) \pmod v$ where $k + k' = h(n + 1)$.

Note that rp^kD is a translate of rD as p is a multiplier of the difference set D.

Conjecture 1: *Let D be a difference set in Z_v acting as a Singer group on the points and hyperplanes of* PG(n, q) *where $v = (q^{n+1} - 1)/(q - 1)$ and $q = p^h$ with p prime. Let r be an integer coprime to v.*

- (a) *Except in the case where $n = 2$ and q is odd, rD is a quadric of* PG(n, q) *if and only if*

  $rp^k(q^l + q^m) \equiv 1 \mod v$ *for some integers k, l, m.*

- (b) *In the case where $n = 2$ and q is odd, rD is a quadric of* PG(n, q) *if and only if*

  either $rp^k(q^l + q^m) \equiv 1 \mod v$ *for some integers k, l, m,*

  or $rp^k \equiv 2 \mod v$ *for some integer k.*

We have verified this conjecture for PG(n, q) in the following cases: $n = 3$ with $q = 3, 5, 9$, and $n = 4$ with $q = 3, 5$; and we have proved (by Theorem 1) that it is true when $q = 2$.

Finally, we briefly consider a more general question. We shall say that a set rD is a *quasi-quadric* if it has the same intersection properties with hyperplanes as a quadric of the form $r'D$ (that is, the same sizes of intersection, with the same multiplicities: these are detailed by Games in [Ga]). We might ask: for which integers r coprime to v is rD a quasi-quadric? This is relevant since Games' construction for perfect ternary sequences can be applied to some quasi-quadrics which are not quadrics.

Firstly, if rD is a quadric and $rs \equiv 1 \pmod v$, then it is not difficult to see that sD is a quasi-quadric. If $n = 2$ and q is odd then every quasi-quadric is a quadric by Segre's Theorem (Theorem 8.2.4 in [Hi]). This accounts for the case $rp^k \equiv 2 \mod v$ in our conjecture. However in general sD is not a quadric: we found examples of such sets which are not quadrics in $PG(4, 5)$ and $PG(4, 3)$. Note that it is easy to verify that in PG$(2, q)$ s is of the form given in our conjecture if and only if r is of this form.

It is possible for quasi-quadrics rD, where r is neither a value given by our conjecture, nor an inverse modulo v of one of these values, to exist in PG(n, q). We found examples of such sets in $PG(4, 3)$: for example $5D$.

7 Acknowledgements

We are grateful to the referee for the useful corrections and comments.

References

[1] L.D. Baumert, *Cyclic difference sets*. Springer-Verlag, Berlin (1971).

[2] P. Dembowski, *Finite geometries*. Springer-Verlag, New York (1986).

[3] L.E. Dickson, *History of the theory of numbers*, Vol 1. Carnegie Institution of Washington, Washington D.C. (1919).

[4] R.A. Games, The geometry of quadrics and correlations of sequences. *Trans. Inform. Theory* **32** (1986), 423–426.

[5] R.A. Games, The geometry of m-sequences: three-valued crosscorrelations and quadrics in finite projective geometry. *SIAM J. Alg. Discrete Math.* **7** (1986), 43–52.

[6] J.W.P. Hirschfeld, *Projective geometries over finite fields*. Clarendon Press, Oxford (1979).

[7] W.-A. Jackson and P.R. Wild, Relations between two perfect ternary sequence constructions. *Des. Codes Cryptogr.* **2** (1992), 325–332.