Journal of Algebraic Combinatorics **13** (2001), 67–76

Sets of Type (a, b) From Subgroups of $\Gamma L(1, p^R)$

NICHOLAS HAMILTON nick@maths.uq.edu.au
Department of Mathematics, The University of Queensland, St. Lucia, Queensland, Australia

TIM PENTTILA penttila@maths.uwa.edu.au
Department of Mathematics, The University of Western Australia, Nedlands, Western Australia, Australia

Received February 23, 1999; Revised March 20, 2000

Abstract. In this paper k-sets of type (a, b) with respect to hyperplanes are constructed in finite projective spaces using powers of Singer cycles. These are then used to construct further examples of sets of type (a, b) using various disjoint sets. The parameters of the associated strongly regular graphs are also calculated. The construction technique is then related to work of Foulser and Kallaher classifying rank three subgroups of $A\Gamma L(1, p^R)$. It is shown that the sets of type (a, b) arising from the Foulser and Kallaher construction in the case of projective spaces are isomorphic to some of those constructed in the present paper.

Keywords: k-set of type (a, b), Singer cycle, strongly regular graph

1. Introduction

In a finite projective space of dimension n and order q, a k-set of type (a, b) is a set $\mathcal{K}$ of k points such that every hyperplane of the space meets $\mathcal{K}$ in either a or b points, for some integers $a < b$.

In projective planes, k-sets of type (a, b) have been extensively studied. They include hyperovals ($k = q + 2$, $a = 0$, $b = 2$, q even), maximal arcs ($k = q(b - 1) + b$, $a = 0$), unitals ($k = q^{3/2}+1$, $a = 1$, $b = q^{1/2}+1$, q a square) and Baer subplanes ($k = q+q^{1/2}+1$, $a = 1$, $b = q^{1/2} + 1$, q a square). See [6] and its bibliography for various constructions and results.

For higher dimensions an extensive survey can be found in [1]. The paper also surveys the relationships between k-sets of type (a, b), strongly regular graphs and two weight codes.

The aim of the current paper is to give a construction of k-sets of type (a, b) which both provides new examples and unifies certain of those previously known. In Section 2, k-sets of type (a, b) are constructed using suitable powers of Singer cycles. The parameters of the sets are calculated, and disjoint unions of such sets are shown to give more k-sets with two intersection numbers. In Section 3, the sets constructed in $PG(2, q)$ are studied and some of them are shown to be isomorphic to those arising from previously known constructions. In Section 4 the relationship of this work to a theorem of Foulser and Kallaher is examined.

In the following we will use the notation: $x \mid y$ to denote that x divides y; $gcd(x, y)$ to denote the greatest common divisor of x and y; $x \equiv y(z)$ to denote that x is congruent to y modulo z; $|x|_y = z$ to denote the order of x modulo y is z; for integer x, y and z.

2. Construction of *k*-sets of type (*a*, *b*) in projective spaces

In this Section sets of type (a, b) are constructed in projective spaces using certain powers of Singer cycles.

Consider $GF(q^n)$ as an $n-1$-dimensional projective space $PG(n-1, q)$ over $GF(q)$. The points of $PG(n-1, q)$ are represented as elements of $GF(q^n)^*/GF(q)^*$, with two elements w_1 and w_2 of $GF(q^n)$ representing the same point if and only if $w_1 = kw_2$ for some k in $GF(q)$. Let w be a generator of the multiplicative group of $GF(q^n)^*$. Then w has order $q^n - 1$ and acts linearly on $GF(q^n)^*$ by multiplication, i.e. $x \mapsto wx$. Further w^{q-1} acts regularly on the points of $PG(n-1, q)$, i.e. it is a Singer cycle on $PG(n-1, q)$.

In the following we will take certain powers of w and show that their orbits are k-sets of type (a, b) with respect to hyperplanes in $PG(n-1, q)$. The main theorem we use to show that these are sets of type (a, b) is that if a group acting on a projective space has two orbits on points then it has two orbits on hyperplanes (see for instance [2,2.3.1]). Having two orbits on hyperplanes then means that the set stabilised has at most two intersection numbers with respect to hyperplanes.

The simplest case we can consider is orbits of w^2. Suppose that n is even and q is odd, then $q^n - 1$ and $(q^n - 1)/(q - 1) = q^{n-1} + q^{n-2} + \cdots + q + 1$ are even. The group $\langle w^2 \rangle$ then has two orbits $\{1, w^2, w^4, \ldots, w^{q^n-3}\}$ and $\{w, w^3, w^5, \ldots, w^{q^n-2}\}$ on $GF(q^n)$. Further the group $\langle w^{2(q-1)} \rangle$ acts as a Singer cycle on $PG(n-1, q)$ with two orbits on points, and we have the following Theorem.

Theorem 1 *Let $n \geq 4$ be an even integer and q an odd prime power, then there exists a $(q^n - 1)/2(q - 1)$-set of type (a, b) in $PG(n-1, q)$ for some integers a and b.*

The values of a and b will be calculated below. More generally we can consider orbits of w^r where r is prime as follows.

Theorem 2 *Let $n \geq 2$ be an integer, p be a prime, h a positive integer, and $r \neq 2$ a prime such that p is a primitive root modulo r, and $p^{nh} \equiv 1(r)$. Suppose that either $p^h \not\equiv 1(r)$ or r divides $gcd(n, p^h - 1)$.*

Let g be a Singer cycle of $PG(n-1, p^h)$ and $\mathcal{K}$ an orbit of $\langle g^r \rangle$. Then $\mathcal{K}$ is a $(p^{nh} - 1)/r(p^h - 1)$-set of type (a, b) in $PG(n-1, p^h)$ for some integers a and b.

Proof: It is worth while first explaining some of the assumptions of the Theorem. We require r to divide $(p^{nh} - 1)/(p^h - 1)$, the number of points in $PG(n-1, q)$. Hence in the statement we have first assumed that $p^{nh} \equiv 1(r)$, i.e. that r divides $p^{nh} - 1$. But $p^{nh} - 1 = (p^h - 1)(p^{h(n-1)} + \cdots + p^h + 1)$ so we also require that either r does not divide $p^h - 1$ or that it divides the greatest common divisor of $(p^h - 1)$ and $(p^{hn} + p^{h(n-1)} + \cdots + p^h + 1)$ which is $gcd(n, p^h - 1)$. Hence the assumptions that $p^h \not\equiv 1(r)$ or r divides $gcd(n, p^h - 1)$.

First suppose that $p^h \not\equiv 1(r)$. Let g be a Singer cycle of $PG(n-1, p^h)$ and $\mathcal{K}$ be an orbit of $\langle g^r \rangle$. All orbits of $\langle g^r \rangle$ are equivalent under powers of g. Let w be a generator of $GF(p^{nh})^*$. Without loss of generality, g is given by multiplication by w^r.

Let G be the semidirect product of $\langle w^r \rangle$ and $AutGF(p^{nh})$. Notice that elements of G map powers of w^r to powers of w^r. Hence one orbit of G is given by the set of powers of w^r. The complement of this also corresponds to an orbit of G, since p is a primitive root modulo r as follows. The set $\langle w^r \rangle w^i$ is given by $\{w^{ar+i} : a \in \mathbf{Z}\}$ and the images of w^i under the group generated by the Frobenious automorphism is the set $\{w^{ip^j} : j \in \mathbf{Z}\}$. So the set Gw is the complement of $\{w^{ar} : a \in \mathbf{Z}\}$ since $1, p, p^2, \ldots, p^{r-1}$ are all the non-zero elements modulo r.

Thus G has two orbits on points of $PG(n-1, p^h)$ and so two orbits on hyperplanes of $PG(n-1, p^h)$. It follows that each of the orbits on points is a set of type (a, b) with respect to hyperplanes, for some (a, b).

Now suppose that $r \mid gcd(n, p^h - 1)$. Let G be the semidirect product of $\langle w^{(p^h-1)r} \rangle$ and $Aut(GF(p^{nh}))$. Note that $p^h \equiv 1(r)$ implies $(p^{nh}-1)/(p^h-1) \equiv 0(r)$. Proceeding as above gives the required result. □

2.1. Parameter calculations

We now calculate the values for a and b in Theorems 1 and 2. The following is a straight forward generalisation of counts for k-sets of type (a, b) in projective planes found in [9] and [10].

For ease of notation we write $\tau_n = (q^n - 1)/(q-1)$, where $q = p^h$. Let $\mathcal{K}$ be one of the sets constructed in Theorems 1 or 2. The size of $\mathcal{K}$ is then given by $k = \tau_n / r$ (where $r = 2$ in the case of Theorem 1). The complement of $\mathcal{K}$ then has size $(r-1)\tau_n/r$. Let t_a and t_b be the numbers of hyperplanes that meet $\mathcal{K}$ in a and b points, respectively. Then

$$t_a + t_b = \tau_n. \tag{1}$$

Counting ordered pairs (P, Σ) such that P is a point of $\mathcal{K}$ and Σ is a hyperplane containing P in two ways gives

$$at_a + bt_b = k\tau_{n-1}. \tag{2}$$

Counting ordered triples (P, Q, Σ) such that P and Q are points of $\mathcal{K}$ and Σ is a hyperplane containing P and Q in two ways gives

$$a(a-1)t_a + b(b-1)t_b = k(k-1)\tau_{n-2}. \tag{3}$$

The action on hyperplanes is the same as that on points. One hyperplane of $GF(q^n)$ over $GF(q)$ is $K = \{x \mid T(x) = 0\}$ where T is the trace map from $GF(q^n)$ to $GF(q)$. Define ϕ by $\phi(x) = x^{-1}K$ and $\phi(yK) = y^{-1}$. Now x is incident with yK if and only if $T(xy^{-1}) = 0$ and $\phi(x)$ is incident with $\phi(yK)$ if and only if y^{-1} is incident with $x^{-1}K$ if and only if $T(xy^{-1}) = 0$. So ϕ is a polarity. Let g be the Singer cycle $w \mapsto wx$. Then g maps

yK to wyK. So $\phi g \phi^{-1} = g^{-1}$. So ϕ normalises $\langle g \rangle$. Since the normaliser of $\langle g \rangle$ in the correlation group contains a duality ϕ, ϕ interchanges the orbits on points of the normaliser N of $\langle g \rangle$ in the collineation group with the orbits of N on hyperplanes. Therefore we can choose $t_a = k$ and $t_b = (r-1)k$.

Solving (2) and (3) for a and b then gives

$$a = \frac{c(1-r) + r(q^{n-1}-1)}{r(q-1)} \quad \text{and} \quad b = \frac{c}{r(q-1)}$$

where c is a root of

$$x^2 + 2(1-q^{n-1})x + q^{2n-2} - q^{n-2} - q^n + 1 = 0.$$

This has solutions

$$c = (q^{n-1}-1) \pm q^{\frac{n-2}{2}}(q-1)$$

giving

$$a = \frac{(q^{n-1}-1) \pm q^{\frac{n-2}{2}}(q-1)(1-r)}{r(q-1)} \quad \text{and} \quad b = \frac{(q^{n-1}-1) \pm q^{\frac{n-2}{2}}(q-1)}{r(q-1)}.$$

Notice that the difference of the two solutions for b is $2q^{\frac{n-2}{2}}/r$. Both of the solutions for b may not simultaneously be integers unless $r = 2$. Similarly for a. Hence for given $r \neq 2$, n and q we have unique solutions for a and b.

When $r = 2$, we get

$$a = \frac{(q^{n-1}-1) - \left(\pm q^{\frac{n-2}{2}}\right)(q-1)}{2(q-1)} \quad \text{and} \quad b = \frac{(q^{n-1}-1) \pm q^{\frac{n-2}{2}}(q-1)}{2(q-1)}$$

giving a unique solution (up to interchange of a and b).

2.2. Disjoint sets of type (a, b)

Let $\mathcal{K}$ and $\mathcal{M}$ be disjoint k-sets of type (a, b) with parameters as is the previous Section. We show that the union $\mathcal{K} \cup \mathcal{M}$ is a $2k$-set of type $(a+b, 2b)$ with respect to hyperplanes. The counts that we use to do this are a generalisation to higher dimensions of counts for $PG(2, q)$ in [5].

First, let λ be the number of b-secants to $\mathcal{K}$ on a point not on $\mathcal{K}$. Then counting the set of pairs (P, Σ) such that $P \notin \mathcal{K}$, Σ a hyperplane containing P and meeting $\mathcal{K}$ in b points in two ways gives

$$(|PG(n-1, q) - \mathcal{K}|)\lambda = (|PG(n-1, q)| - b)t_b.$$

Substituting the above values of b, t_b and k and solving for λ then gives

$$\lambda = \frac{q^{n-1}-1}{q-1} - \frac{(q^{n-1}-1) \pm q^{\frac{n-2}{2}}(q-1)}{r(q-1)}.$$

Let x be the number of hyperplanes that are b-secant to $\mathcal{K}$ and a-secant to $\mathcal{M}$. Then counting the set of pairs (P, Σ) such that $P \in \mathcal{M}$, Σ a hyperplane containing P and meeting $\mathcal{K}$ in b points in two ways gives

$$|\mathcal{M}|\lambda = xa + b(t_b - x)$$

and hence

$$x = \frac{|\mathcal{M}|\lambda - bt_b}{a-b}.$$

Substituting for the above values of a, b, t_b and λ and simplifying gives

$$x = \frac{q^n - 1}{(q-1)r}.$$

But this is exactly the number of hyperplanes that are a-secants to $\mathcal{M}$. Hence every a-secant to $\mathcal{M}$ is a b-secant to $\mathcal{K}$. Similarly, every a-secant to $\mathcal{K}$ is a b-secant to $\mathcal{M}$. Hence every hyperplane meets the set $\mathcal{K} \cup \mathcal{M}$ in either $a + b$ or $2b$ points. Thus $\mathcal{K} \cup \mathcal{M}$ is a $2k$-set of type $(a + b, 2b)$.

More generally it follows that a union of s (disjoint) orbits gives an sk-set of type $(a + b(s - 1), sb)$ and we have the following Theorem.

Theorem 3 *Let $n \geq 2$ be an integer, p be a prime, h a positive integer, and $r \neq 2$ a prime such that p is a primitive root modulo r and $p^{nh} \equiv 1(r)$. Suppose that either $p^h \not\equiv 1(r)$ or r divides $\gcd(n, p^h - 1)$. Then for every $s \in \{1 \ldots r-2\}$ there exist $s(p^{nh}-1)/r(p^h-1)$-sets of type $(a + b(s - 1), sb)$ with respect to hyperplanes in $PG(n - 1, p^h)$, with a and b as given in the previous Section.*

Proof: Apply Theorem 2 and take a union of any s of the orbits of the rth power of a Singer cycle. □

2.3. Strongly regular graphs

Associated with every set of type (a, b) with respect to hyperplanes in $PG(n - 1, q)$ are strongly regular graphs, see [1] for details. We conclude this section by calculating the parameters of the strongly regular graphs arising from the sets of type (a, b) constructed in the previous subsections.

Theorem 4 *The sets of type (a, b) constructed in Theorems 1 and 2 give rise to strongly regular graphs with parameters $v = q^n$, $k = (q^n - 1)/r$,*

$$\lambda = \frac{q^n - 3r + 1 \pm q^{n/2}(3r - r^2 - 2)}{r^2}, \quad \textit{and} \quad \mu = \frac{q^n - r + 1 \pm q^{n/2}(r - 2)}{r^2}.$$

Proof: Straight forward calculation using the parameter correspondence for sets of type (a, b) and strongly regular graphs given in [1] yields the result. □

Theorem 5 *The sets of type $(a + b(s - 1), sb)$ constructed in Theorem 3 give rise to strongly regular graphs with parameters $v = q^n$, $k = s(q^n - 1)/r$,*

$$\lambda = \frac{s^2(q^n + 1) - 3rs \pm q^{n/2}(3rs - r^2 - 2s^2)}{r^2},$$
$$\mu = \frac{s(sq^n - r + s \pm q^{n/2}(r - 2s))}{r^2}.$$

3. Sets of type (a, b) in $PG(2, q)$

In this Section we examine the sets constructed by Theorem 2 in $PG(2, q)$. Note that Theorem 1 does not apply as 2 does not divide $q^2 + q + 1$.

The assumptions of Theorem 2 are that p is prime, h a positive integer, $q = p^h$, such that p is a primitive root modulo r, $p^{3h} \equiv 1(r)$ and that either $p^h \not\equiv 1(r)$ or r divides $gcd(3, p^h - 1)$. The values for a and b become:

$$a = \frac{q + 1 \pm q^{1/2}(1 - r)}{r} \quad \text{and} \quad b = \frac{q + 1 \pm q^{1/2}}{r}$$

First note that since we require $q^{1/2} = p^{h/2}$ to be an integer, h must be even.

We consider two cases of the Theorem:

(I) r *divides* $gcd(3, p^h - 1)$. In this case $r = 3$. Now p has order 2 modulo 3, and so equivalently $p \equiv -1(3)$. Hence the assumptions are equivalent to the conditions that h be even and $p \equiv -1(3)$, and we have the Corollary:

Corollary 1 *Suppose that h is an even integer and p is a prime such that $p \equiv -1(3)$. Put $q = p^h$, then there exists a $(q^2 + q + 1)/3$-set of type (a, b) in $PG(2, q)$. If 4 divides h then $(a, b) = (\frac{1}{3}(q - 2q^{1/2} + 1), \frac{1}{3}(q + q^{1/2} + 1))$ else $(a, b) = (\frac{1}{3}(q + 2q^{1/2} + 1), \frac{1}{3}(q - q^{1/2} + 1))$.*

The choices for a and b follow from the fact that since $p \equiv -1(3)$, 3 divides $q + q^{1/2} + 1 = p^h + p^{h/2} + 1$ if and only if $h/2$ is even.

These k-sets of type (a, b) were previously known, and are a subclass of a class credited in [1] to an unpublished paper of R. Metz.

(II) $p^h \not\equiv 1(r)$. Now $p^{(h/2)^6} = p^{3h} \equiv 1(3)$, but $p^h \not\equiv 1(3)$, and so $p^{h/2}$ either has order 3 or 6 modulo r. We consider these two cases:

(II) (a) $p^{h/2}$ *has order* 6 *modulo* r. Note that $q^2+q+1 = (q+q^{1/2}+1)(q-q^{1/2}+1)$, so either $r \mid (q+q^{1/2}+1)$ or $r \mid (q-q^{1/2}+1)$, but not both. Since $r \neq 3$, $r \mid q+q^{1/2}+1 \iff r \mid q^{3/2} - 1 \iff q^{3/2} \equiv 1(3) \iff p^{3h/2} \equiv 1(r) \Rightarrow p^{h/2} \equiv 3(r)$. So for the current case $r \mid q - q^{1/2} + 1$, and we get the following result.

Corollary 2 *Let p be a prime, h an even positive integer, and $r \neq 3$ a prime such that p is a primitive root modulo r and $p^{3h} \equiv 1(r)$. Suppose that $p^h \not\equiv 1(r)$ and $p^{h/2}$ has order* 6 *modulo r. Then there exists a $(q^2 + q + 1)/r$-set of type $(\frac{1}{r}(q + 1 - q^{1/2}(1 - r)), \frac{1}{r}(q + 1 - q^{1/2}))$ in $PG(2, q)$, $q = p^h$.*

Since r divides $q - q^{1/2} + 1$, it follows that the order of the power of the Singer cycle g^r that we are taking is some integer multiple, x say, of $q + q^{1/2} + 1$. Hence the subgroup of $\langle g^r \rangle$ generated by g^{rx} has order $q + q^{1/2} + 1$. It is well known that the orbits of such a subgroup of a Singer cycle are *Baer subplanes* (subplanes of order $q^{1/2}$) of the plane. Hence the sets constructed in the Corollary are unions of Baer subplanes. In [3], M. de Finis constructed partitions of $PG(2, q)$ into Baer subplanes, q a square, using powers of Singer cycles and noted that the union of any subset of the partition gives rise to k-sets of type (m, n). Hence the sets of the Corollary are a subclass of those constructed by de Finis.

(II)(b) $p^{h/2}$ *has order* 3 *modulo* r. In this case $r \mid q + q^{1/2} + 1$. Since p has order $r - 1$ modulo r it follows that $r - 1 \mid (3h/2)$, and so $h/2$ is even, and we get the Corollary:

Corollary 3 *Let p be a prime, h a positive integer such that* $4 \mid h$, *and $r \neq 3$ a prime such that p is a primitive root modulo r and $p^{3h} \equiv 1(r)$. Suppose that $p^h \not\equiv 1(r)$ and $p^{h/2}$ has order* 3 *modulo r. Then there exists a $(q^2 + q + 1)/r$-set of type $(\frac{1}{r}(q + 1 + q^{1/2}(1 - r)), \frac{1}{r}(q + 1 + q^{1/2}))$ in $PG(2, q)$, $q = p^h$.*

Now $p^{h/4}$ must have order 3 or 6 modulo r. We consider these two cases:

(II)(b)(i) $p^{h/4}$ *has order* 6 *modulo* r. In this case, arguing as before, $r \mid q^{1/2} - q^{1/4} + 1$, and $r \not\mid q^{1/2} + q^{1/4} + 1$. It follows that the power of the Singer cycle $\langle g^r \rangle$ has a subgroup of order $q^{1/2} + q^{1/4} + 1$. The orbits of such a subgroup of a Singer cycle are well known to be subplanes of order $q^{1/4}$. Hence the set is a union of subplanes of order $q^{1/4}$.

In [8], M.J. de Resmini constructs $(q^{1/2} + q^{1/4} + 1)(q - q^{1/2} + 1)$-sets of type $(q^{1/4} + 1, q^{1/2} + q^{1/4} + 1)$ in $PG(2, q)$ using powers of Singer cycles. She then takes s disjoint copies, $s \in \{2 \dots q^{1/2} - q^{1/4} + 1\}$, of these sets to give $s(q^{1/2} + q^{1/4} + 1)(q - q^{1/2} + 1)$-sets of type $(s(q^{1/2} + q^{1/4} + 1) - q^{1/2}, s(q^{1/2} + q^{1/4} + 1))$. These can be seen as unions of subplanes of order $q^{1/4}$. The current sets are a subclass of the examples of de Resmini.

(II)(b)(ii) $p^{h/4}$ *has order* 3 *modulo* r. In this case of the Corollary the sets arising were not previously known.

Note that with all of the above Corollaries we may also apply Theorem 3 to construct more k-sets of type (a, b).

In (II)(a) and (II)(b)(i) above it was noted that the sets could be described as unions of subplanes of the plane. In the following we show that many of the sets, including some of those in (II)(b)(ii), can be described as unions of subplanes.

Let $q = p^{m2^i}$, where i and m are integers, m odd. Then the number of points in the plane is $p^{m2^{i+1}} + p^{m2^i} + 1$ which equals

$$(p^{2m} + p^m + 1)(p^{2m} - p^m + 1)(p^{4m} - p^{2m} + 1) \cdots \big(p^{m2^i} - p^{m2^{i-1}} + 1\big).$$

Suppose that r divides the term $p^{m2^j} - p^{m2^{j-1}} + 1$ for some j, and put $x = (p^{m2^j} - p^{m2^{j-1}} + 1)/r$. Then the order of g^r is

$$x\big(p^{m2^j} + p^{m2^{j-1}} + 1\big)\big[\big(p^{m2^{j+1}} - p^{m2^j} + 1\big) \cdots \big(p^{m2^i} - p^{m2^{i-1}} + 1\big)\big].$$

Notice that this has a subgroup of order $(p^{m2^j} + p^{m2^{j-1}} + 1)$. The orbits of such a subgroup are well known to be subplanes of order $p^{m2^{j-1}}$. Hence these such sets can be seen as a union of $((p^{m2^j} - p^{m2^{j-1}} + 1) \cdots (p^{m2^i} - p^{m2^{i-1}} + 1))/r$ subplanes of order $p^{m2^{j-1}}$.

We conclude this Section by giving some examples of the parameters of sets not previously known, i.e. those of (II)(b)(ii) above.

Example Suppose $r = 7$. Then we require that p is congruent to 3 or 5 modulo 7, and h is congruent to 8 or 16 modulo 24. The smallest examples are:

(a) a 6150469-set of type $(868, 949)$ in $PG(2, 3^8)$. Since $7 \mid 3^2 - 3 + 1$ this can be seen as a union of subplanes of order 3.

(b) a 21798325893-set of type $(55268, 55893)$ in $PG(2, 5^8)$. Since $7 \mid 5^2 - 5 + 1$ this can be seen as a union of subplanes of order 5.

Example Suppose $r = 13$. Then we require that p is congruent to 2, 6, 7 or 11 modulo 13, and h is congruent to 16 or 32 modulo 48. The smallest example is a 330387141-set of type $(4805, 5061)$ in $PG(2, 2^{16})$. Since $13 \mid 2^4 - 2^2 + 1$ this can be seen as a union of subplanes of order 4.

4. Subgroups of $\Gamma L(1, p^R)$

In the following we recall work of Foulser and Kallaher ([4]) which classifies subgroups of $\Gamma L(1, p^R)$ that have two orbits on $GF(p^R)^*$. In certain cases these give k-sets of type (a, b) in $PG(n - 1, p^{R/n})$. We show that for a large number of cases (including $PG(2, q)$) the k-sets of type (a, b) obtainable from such subgroups are isomorphic to those constructed in Section 2.

We follow the notation of Foulser and Kallaher in [4]. Let w be a generator of $GF(p^R)^*$ and $\alpha : x \to x^p$ be a generator of the automorphism group of $GF(p^R)$. The group $\langle w, \alpha\rangle$ generated by w and α is then $\Gamma L(1, p^R)$.

Lemma 1 ([4,2.1]) *Let G be a subgroup of $\langle w, \alpha\rangle$. Then G has form $G = \langle w^d, w^e\alpha^s\rangle$, where d e and s can be chosen to satisfy the following conditions*:

$$s \mid R, \quad d \mid p^R - 1, \quad \textit{and} \quad e\left(\frac{p^R - 1}{p^s - 1}\right) \equiv 0(d).$$

Such a subgroup is said to be in *standard form*.

Theorem 6 ([4,3.9]) *Let p be a prime, e an integer, and let m_1, v, s and R be positive integers satisfying:*
(1) *the primes of m_1 divide $p^s - 1$.*
(2) *v is a prime, $v \neq 2$, $|p^{sm_1}|_v = v - 1$.*
(3) $gcd(e, m_1) = 1$.
(4) $m_1 s(v-1)|R$.
Let $d = m_1 v$, $\Delta = (p^R - 1)/d$ and $m_2 = (v-1)m_1$. Then $G = \langle w^d, w^e \alpha^s \rangle$ is in standard form and has two orbits on $GF(p^R)^*$ of length Δm_1 and Δm_2, where $m_1 < m_2$.

A similar theorem is proved for subgroups which have two equal length ($m_1 = m_2$) orbits on $GF(p^R)^*$.

It is worth noting that in the Theorem $G \cap \langle w \rangle = \langle w^d \rangle$, and that the group $\langle w^e \alpha^s \rangle$ acts as a permutation on the orbits of $\langle w^d \rangle$. In fact the orbit of length Δm_1 is a union of m_1 orbits of $\langle w^d \rangle$, and similarly for the orbit of length Δm_2.

If $n \geq 2$ is an integer that divides R then $GF(p^R)$ gives a model for $PG(n-1, p^{R/n})$ as in the previous sections. We now consider when the groups of Theorem 6 act on projective spaces.

Theorem 7 *Suppose $n \mid R$, for integers n and R. Then if a k-set of type (a, b) in $PG(n-1, p^{R/n})$ arises from Theorem 6 it is isomorphic to one of those in Theorem 2.*

Proof: First note that if $\langle w^d, w^e \alpha^s \rangle$ satisfies the conditions of Theorem 6 then so does $\langle w^v, w^e \alpha^s \rangle$ where $d = m_1 v$. This follows immediately since $|p^{sm_1}|_v = v - 1$ implies $|p^s|_v = v - 1$. Further, $\langle w^d, w^e \alpha^s \rangle$ is a subgroup of $\langle w^v, w^e \alpha^s \rangle$. It follows that the groups both have the same orbits.

We consider the group $G = \langle w^v, w^e \alpha^s \rangle$. Note that there are d orbits of w^d on $GF(p^R)$, and the union of m_1 of them make up one orbit of $\langle w^v, w^e \alpha^s \rangle$ and $(v-1)m_1$ of them make up the other orbit. So $m_1 = 1$, $d = v$ means that the k-set of type (a, b) arising from G is a single orbit of w^v.

For G, $d = m_1 v = v$, so condition 2 of Theorem 6 becomes that $|p^s|_v = v - 1$. Hence p^s, and so p, are primitive roots modulo v. It follows immediately that a k-set of type (a, b) stabilised by such a group is isomorphic to that obtained by the construction of Theorem 2 with $r = v$ and $h = R/n$. □

As it was mentioned before, Foulser and Kallaher prove a similar result to Theorem 6 for the case when a subgroup of $\Gamma L(1, p^R)$ has two orbits of the same length ($v = 2$). Arguing as in the previous theorem with the group $\langle w^2, w^e \alpha^s \rangle$ containing $\langle w^d, w^e \alpha^s \rangle$ where $d = 2m$ shows that such groups only give rise to the sets of type (a, b) constructed in Theorem 1.

In the previous Theorem we have classified all k-sets of type (a, b) in $PG(n-1, p^{R/n})$ that arise from subgroups of $\Gamma L(1, p^R)$ having two orbits on the points in the natural action. It is worth noting that there are other subgroups of $\Gamma L(1, p^R)$ which have orbits that are k-sets of type (a, b), though the subgroups do not have two orbits on points. For instance, at the recent *Twenty-third Australasian Conference on Combinatorial Mathematics and*

Combinatorial Computing, Batten announced that she and Dover had constructed an 829-set of type $(4, 9)$ in $PG(2, 125)$ and a 3189-set of type $(4, 11)$ in $PG(2, 343)$ by taking the orbits of the 19th and 37th powers of the Singer cycles, respectively. Neither of these are stabilised by a subgroup of $\Gamma L(1, q^3)$ having two orbits, indeed the planes that these occur in do not have square order.

Foulser and Kallaher's results show that the sets of type (a, b) constructed in Theorems 1 and 2 were in some sense known before. However, their results are not well known, the conditions they gave were complicated, and it was not easy to tell when the sets existed, let alone what the actual values for a and b were, or the parameters of the strongly regular graphs arising from them. In [7], Liebeck and Saxl calculate parameters for strongly regular graphs arising from primitive rank three groups except those given in this paper. Our aim here has been to give an easy condition for the existence of these sets of type (a, b) and their parameters, as well as to construct new examples using disjoint sets of type (a, b). In particular, despite their claims to the contrary, these examples of sets of type (a, b) were omitted from [1].

References

1. R. Calderbank and W.M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.* **18** (1986), 97–122.
2. P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.
3. M. de Finis, "On k-sets of type (m, n) in projective planes of square order," in *Finite Geometries and Designs*, P.J. Cameron, J.W.P. Hirschfeld and D.R. Hughes (Eds.), London Math. Soc. Lect. Notes Series, Vol. **49**, 1981, pp. 98–103.
4. D.A. Foulser and M.J. Kallaher, "Solvable, flag transitive, rank 3 collineation groups," *Geom. Ded.* **7** (1978), 111–130.
5. K. Grüning, "A class of unitals of order q which can be embedded in two different planes of order q^2," *J. Geom* **29** (1987), 61–77.
6. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford University Press, Oxford, 1996.
7. M.W. Liebeck and J. Saxl, "The finite primitive permutation groups of rank three," *Bull. Lond. Math. Soc.* **18** (2) (1986), 165–172.
8. M.J. de Resmini, "An infinite family of type (m, n) sets in $PG(2, q^2)$, q a square," *J. Geom* **20** (1983), 36–43.
9. M. Tallini Scafati, "Sui $\{k, n\}-$archi di un piano grafico finito," *Atti Accad. Naz. Lincei Rend.* **40** (1966), 373–378.
10. M. Tallini Scafati, "$\{k, n\}-$archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri. (Note I; II)," *Atti Accad. Naz. Lincei Rend.* **40** (1966), 812–818, 1020–1025.