On the orbits of Singer groups and their subgroups

Keldon Drudge*

Submitted: January 6, 2001; Accepted: March 5, 2001.
MR Subject Classifications: 05C88, 05C89

Abstract

We study the action of Singer groups of projective geometries (and their subgroups) on $(d-1)$-flats for arbitrary d. The possibilities which can occur are determined, and a formula for the number of orbits of each possible size is given. Motivated by an old problem of J.R. Isbell on the existence of certain permutation groups we pose the problem of determining, for given q and h, the maximum co-dimension $f_q(n,h)$ of a flat of $PG(n-1,q)$ whose orbit under a subgroup of index h of some Singer group covers all points of $PG(n-1,q)$. It is clear that $f_q(n,h) < n - log_q(h)$; on the other hand we show that $f_q(n,h) \geq n-1-2\log_q(h)$.

1 Introduction

A *Singer cycle* of a finite projective space $\Sigma_{n-1} = \mathrm{PG}(n-1,q)$ is a collineation σ such that the group $\langle\sigma\rangle$ acts regularly on the points (and hyperplanes) of Σ_{n-1} (the group is then called a *Singer group*). The existence of Singer cycles is derived in [10] from the fact that the multiplicative group of the field $\mathrm{GF}(q^n)$ is cyclic. These distinguished elements of the collineation group of Σ_{n-1} have been used to construct many geometrically interesting subsets of projective spaces (see, for example, [4], [9] and [6]). Glynn's construction in [9], in particular, amounts essentially to the determination of the orbits of such a cycle on the set of lines of $PG(3,q)$, and the basic geometrical structure of the sets of lines which comprise orbits. This suggests the rather natural general problem of studying the orbits of $\langle\sigma\rangle$ on the set of $(d-1)$-flats of Σ_{n-1} for any d, $2 \leq d \leq n-2$ (a $d-1$-*flat* is a subspace of vector space dimension d). Here, motivated primarily by a problem in permutation group theory (see Section 3), we determine, for arbitrary d and n, which sizes of orbit are possible, and how many of each type occur. We also use the results so obtained to gain some information on the orbits of subgroups of Singer groups.

Throughout, q will represent an arbitrary prime power, $n \geq 4$ a fixed integer and σ an arbitrary Singer element of Σ_{n-1}. $G = \langle\sigma\rangle$ will denote the cyclic group generated by σ. For any $r \geq 1$ we will write θ_r for the number of points of $\mathrm{PG}(r-1,q)$, that is

*Research supported by an N.S.E.R.C. of Canada post-doctoral fellowship.

$\theta_r = q^{r-1}+q^{r-2}+\cdots+1$. As is well known, the function θ so defined satisfies $(\theta_r, \theta_s) = \theta_{(r,s)}$ where (a, b) is the greatest common divisor of the integers a and b. Also, θ_r^t will denote the number of points of $\mathrm{PG}(r-1, q^t)$. Note that we have $\theta_n/\theta_r = \theta_{n/r}^r$ whenever $r|n$. As usual, we will use $\begin{bmatrix} n \\ d \end{bmatrix}_q$ to denote the number of $(d-1)$-flats in $PG(n-1, q)$.

Recall that an $(r-1)$-*spread* of Σ_{n-1} is a set of $(r-1)$-flats which partition the points of the space; an $(r-1)$-spread exists if and only if $r|n$. We define a $(k, r-1)$-*cover* of Σ_{n-1} to be a set S of $(r-1)$-flats such that every point of Σ_{n-1} is on exactly k elements of S (so an $(r-1)$-spread is the same thing as a $(1, r-1)$-cover). Counting flags shows that for a $(k, r-1)$-cover to exist, k must be a multiple of $\theta_r/\theta_{(r,n)}$. Since G acts transitively on the points of Σ_{n-1}, all orbits of $(r-1)$-flats, $r \geq 2$ are $(k, r-1)$-covers for some k, and the previous sentence becomes the statement that the G-stabilizer of any $(d-1)$-flat is contained in $\langle \sigma^{\theta_n/\theta_{(n,d)}} \rangle$. The following lemma generalises this observation slightly.

Lemma 1.1 *If a flag $X \leq Y$ with X a $(d-1)$-flat and Y a $(r-1)$-flat is fixed by some subgroup $\langle \sigma^k \rangle$ of G then k is a multiple of $\theta_n/\theta_{(n,d,r)}$.*

The $(k, r-1)$-covers generalize to flats of arbitrary dimension the k-covers of lines introduced by Ebert in [5].

We will say that an $(r-1)$-spread $\mathcal{S}$ of Σ_{n-1} *fills* a $(d-1)$-flat X $(d \geq r)$ if any element of $\mathcal{S}$ is either contained in X or disjoint from X—that is, if $\mathcal{S}$ defines a $(r-1)$-cover of X. For this to happen, of course, it is necessary that $r|d$. Also, an $(r-1)$-spread $\mathcal{S}$ of Σ_{n-1} is said to be *geometric* if, for any two elements $X_1, X_2 \in \mathcal{S}$, $\mathcal{S}$ fills the $(2r-1)$-flat $X_1 \vee X_2$. The choice of language is due to the fact that

Lemma 1.2 *An $(r-1)$-spread $\mathcal{S}$ is geometric if and only if taking as $(k-1)$-flats the set of $(kr-1)$-flats filled by $\mathcal{S}$, for $k = 1, 2, \ldots, n/r$, and the inclusion inherited from Σ_{n-1} gives a projective space $PG(n/r-1, q^r)$.*

2 Counting orbits

As we mentioned in the introduction, Glynn determines the orbits of a Singer cycle of Σ_3 on the set of lines (1-flats) of that space; his result is that there is one orbit which is a (regular) spread, and that the other orbits are all $(q+1)$-covers. This is indicative of the following lemma, which provides the basis for Theorem 2.1.

Lemma 2.1 *A Singer cycle of Σ_{n-1} has an orbit which is a $(d-1)$-spread if and only if $d|n$. In this case there is exactly one such orbit $\mathcal{S}$; the G-stabilizer of any $S \in \mathcal{S}$ is $Stab_G S = \langle \sigma^{\theta_n/\theta_d} \rangle$. $\mathcal{S}$ is a geometric $(d-1)$-spread and the factor group $G/Stab_G S$ is a Singer group of the corresponding $PG(n/d-1, q^d)$.*

Proof: The condition $d|n$ is clearly necessary. On the other hand, if $d|n$, it is easy to see that any subspace of (vector space) dimension d which is closed under multiplication by a primitive θ_dth root of unity is a multiplicative translate of a subfield $GF(q^d)$, so the fact that the Galois group of the extension $GF(q^n)/GF(q)$ is cyclic of order n implies that in this case exactly one orbit $\mathcal{S}$ of G is a $(d-1)$-cover; the stabilizer of any of its elements is $\langle \sigma^{\theta_n/\theta_d} \rangle$ and the factor group $G/Stab_G(S)$ acts regularly on $\mathcal{S}$. Now if S_1, S_2, S_3 are distinct elements of $\mathcal{S}$ and the $(2d-1)$-flat $S_1 \vee S_2$ intersects S_3 non-trivially, say in a $(r-1)$-flat then this flat is fixed by $\langle \sigma^{\theta_n/\theta_d} \rangle$. But Lemma 1.1 shows that its stabilizer is contained in $\langle \sigma^{\theta_n/\theta_{(d,r)}} \rangle$, so we must have $d = r$. Therefore $S_1 \vee S_2$ is filled by $\mathcal{S}$, so $\mathcal{S}$ is a geometric $(r-1)$-spread. □

The following lemma strengthens the statement immediately before Lemma 1.1. It shows that the action of a Singer group of Σ_{n-1} on the $(d-1)$-flats is similar to the action of a n-cycle of the symmetric group on n elements on the set of d-element subsets.

Lemma 2.2 *The G-stabilizer of any $(d-1)$-flat has size θ_u, and is therefore $\langle \sigma^{\theta_n/\theta_u} \rangle$ for some $u|(d,n)$. In other words, each orbit of G on $(d-1)$-flats is a $(d-1, \theta_n/\theta_u)$-cover of Σ_{n-1} for some $u|(d,n)$.*

Proof: By the above, the stabilizer of any such flat has size dividing $\theta_{(d,n)}$. If $(d,n) = 1$, all $(d-1)$-flats have trivial stabilizer, so the lemma certainly holds in this case. This is the base of an induction on the number of divisors of (d,n) (counted with multiplicity). Therefore given a $(d-1)$-flat X whose stabilizer is $\langle \sigma^{\theta_n/k} \rangle$ for some $k > 1$, let $u > 1$ be the least integer such that $k|\theta_u$. Since $k|\theta_{(d,n)}$, we have $u|(d,n)$ by the minimality of u. Now the stabilizer of X is contained in the stabilizer of the elements of the $(u-1)$-spread orbit $\mathcal{S}$, which is isomorphic to $PG(n/u-1, q^u)$. In fact, this spread fills X—if any $Y \in \mathcal{S}$ intersects X in a $(t-1)$-flat, that flat would be fixed by $\langle \sigma^{\theta_n/k} \rangle$, but its stabilizer is contained in $\langle \sigma^{\theta_n/\theta_{(n,d,t)}} \rangle$, so $k|\theta_{(n,d,t)}$. Thus by the minimality of u, we must have $(n,d,t) = u$, but $t \leq u$ so $t = u$ and X is filled by $\mathcal{S}$ as asserted. This implies that X corresponds to a $(d/u-1)$-flat of $PG(n/u-1, q^u)$. By the induction hypothesis, the orbit of X under the Singer cycle of this group is a $(d/u-1, \theta^u_{d/u}/\theta^u_r)$-cover of $PG(n/u-1, q^u)$ for some $r|(d/u, n/u)$. Thus the orbit of X under G has size $\theta_u \theta^u_r = \theta_{ru}$, and since $ru|(d,n)$ we're finished. □

In the statement of the following theorem, μ denotes the Möbius function, the basic properties of which can be found in, for example, [1].

Theorem 2.1 *The number of orbits of a Singer group of Σ_{n-1} on the set of $(d-1)$-flats of Σ_{n-1} is*

$$\frac{1}{\theta_n} \sum_{t|(d,n)} \left[\begin{array}{c} n/t \\ d/t \end{array} \right]_{q^t} \left(\sum_{u|t} \mu(t/u) \theta_u \right). \tag{1}$$

If $u|(d,n)$, there are exactly

$$\frac{\theta_u}{\theta_n} \left(\sum_{t:u|t|(d,n)} \mu(t/u) \left[\begin{array}{c} n/t \\ d/t \end{array} \right]_{q^t} \right) \tag{2}$$

orbits of any Singer cycle of Σ_{n-1} on $(d-1)$-flats which form θ_d/θ_u fold covers of Σ_{n-1}; any $(d-1)$ flat occurs in this way for some $u|(d,n)$.

Proof: The formula (1) follows from (2) on summing over all divisors of (d,n) and switching the order of summation, so we need only prove the latter.

Once again, we proceed by induction on the number of prime divisors of (n,d). In the case $(n,d)=1$, the formula is clearly correct since every $(d-1)$-flat has trivial stabilizer. Assume then that $(n,d)>1$. Lemma 2.2 implies that every orbit of $(d-1)$-flats is a (θ_d/θ_u)-cover for some $u|(d,n)$. This, together with the summation property of the Möbius function, imply after a little manipulation that the truth of (2) for $u=1$ follows from the truth of the same formula for every $u>1$. Thus we may assume that $u>1$. Now any $(d-1)$-flat X whose stabilizer is $\langle\sigma^{\theta_n/\theta_u}\rangle$ is fixed by exactly the stabilizer of the unique orbit $\mathcal{S}$ of $(u-1)$-flats which forms a spread of Σ_{n-1}. This flat is therefore filled by $\mathcal{S}$ (as in the proof of Lemma 2.2), so X is a $(d/u-1)$-flat of the $PG(n/u-1,q^u)$ corresponding to $\mathcal{S}$. Now the orbit of X as a $(d-1)$-flat of $PG(n-1,q)$ is the same size as the orbit of X as a $(d/u-1)$-flat of $PG(n/u-1,q^u)$ under the factor group which acts as a Singer group of the latter space. Thus the orbits of G on $(d-1)$-flats whose stabilizer is $\langle\sigma^{\theta_n/\theta_u}\rangle$ are in one to one correspondence with the orbits of the factor group $G/\langle\sigma^{\theta_n/\theta_u}\rangle$ on $(d/u-1)$-flats of $PG(n/u-1,q^u)$ which have trivial stabilizer. By the induction hypothesis there are exactly

$$\frac{\theta_1^u}{\theta_{n/u}^u}\left(\sum_{t|(d/u,n/u)}\mu(t)\begin{bmatrix} n/tu \\ d/tu \end{bmatrix}_{q^{tu}}\right) \tag{3}$$

orbits of $(d/u-1)$-flats which are $\theta_{d/u}^u/\theta_1^u=\theta_d/\theta_u$ covers. Since the assignment $t\mapsto ut$ gives a one to one correspondence between divisors of $(d/u,n/u)$ and divisors of (d,n) which are divisible by u, the sum (3) is equal to (2), and we are finished. $\square$

Remark: Theorem 2.1 shows that, perhaps as expected, 'most' orbits of $(d-1)$-flats are acted on regularly by a given Singer group, since the term corresponding to $t=1$ in the sum in (2), which only occurs in the sum for $u=1$ (that is, trivial stabilizer) is far larger than any other term in the sum. This implies that, although when $(d,n)>1$ there will be more than $\frac{1}{\theta_n}\begin{bmatrix} n \\ d \end{bmatrix}_q$ orbits of G on $(d-1)$-flats, this number is certainly a very good approximation to the number of orbits in any case.

3 Permutation Groups

We now turn to the problem in permutation group theory which motivated both the preceding and the following work on Singer groups.

It is a direct consequence of the orbit-counting lemma for permutation groups (see [2]) that every transitive permutation group G contains a fixed-point free element. A rather more delicate question, however, is what can be said about such elements. In particular, under what circumstances can it be asserted that there exists a fixed-point free element of order a given prime or prime power dividing the order of G? It was conjectured by J.R. Isbell in 1959 that if the order of G is 'dominated' by a power of two, then G must contain a fixed point free element of two-power order. His conjecture, generalized from 2 to an arbitrary prime p, is that there exists a function f_p from the natural numbers to itself such that, if G is a transitive permutation group of degree $p^a k$ with $(k,p) = 1$ and $a > f_p(k)$ then G contains a fixed point free element whose order is a power of p. Very little progress has been made on this conjecture (see [3] for more detail, further references and some theorems), and in particular it is not known whether or not $f_p(k)$ must tend to infinity with k. The following construction was proposed by P.J. Cameron in an attempt to give examples of transitive groups whose order is divisible by a large power of p but which contain no fixed-point free p elements; I thank him for allowing me to include it here.

Let $V = (\mathbb{Z}/p\mathbb{Z})^k$ with $(k,p) = 1$, τ the automorphism of order k which cyclically permutes the coordinate positions of V, and G the group generated by V and τ (their semi-direct product, since τ normalizes V). Further, let W be a subspace of V, say of co-dimension c, such that the union of all images of W under τ covers all elements of V. Then G acts transitively on the set $W\backslash G$ of right cosets of W in G (of size kp^c) by right multiplication; the stabilizer of the coset W is W and therefore the stabilizer of a coset $W\tau^i$ is the image of W under τ^i. Since such elements cover all elements of V, and since the only elements of p-power order in G are those in V, G has no fixed point free p-power elements. Thus if $g_p(k)$ is the maximum co-dimension of such a W, we have $f_p(k) \geq g_p(k)$. Now the irreducible submodules of V as a $\langle\tau\rangle$ module correspond to the irreducible divisors of $x^k - 1$ over $GF(p)$ (see [8]); if for one of these irreducible submodules V_0 there exists a $\mathbb{Z}/p\mathbb{Z}$-subspace W_0 of co-dimension c in V_0 whose images under $\langle\tau\rangle$ cover V_0 we may take the direct sum of W_0 with the other irreducible submodules to obtain a subspace W of co-dimension c in V whose images under $\langle\tau\rangle$ cover V, so we may reduce to the consideration of the irreducible submodules, although it may not be the case that a W with the largest possible co-dimension always arises in this way. The advantage of the reduction, however, is as follows. Suppose that V_0 is an irreducible submodule of $\mathbb{Z}/p\mathbb{Z}$-dimension n. Then V_0 is isomorphic to $GF(p^n)$ (see [8]); the action of τ on V_0 corresponds to multiplication by a primitive kth root of unity. since $k|(p^n - 1)$, $\langle\tau\rangle$ acts on V_0 as a subgroup of a Singer group of $PG(n-1,p)$ of index $\theta_n/(k/(k,p-1))$.

Therefore we are led to the following problem: given a projective space $\Sigma = PG(n-1,q)$ where $(n,q) = 1$, and a subgroup H of index h in a Singer group of Σ, what is the maximum co-dimension of a subspace of Σ which has the property that its images under H cover all points of Σ? We denote this maximum co-dimension by $f_q(n,h)$. The case $q = p$ is prime and $h = \theta_n/(k/(k,p-1))$ with $n = \mathrm{ord}_k p$ the order of p modulo k corresponds to the irreducible submodules of $(\mathbb{Z}/p\mathbb{Z})^k$, so we have $g_p(k) \geq f_p(\mathrm{ord}_k p, \theta_n/(k/(k,p-1)))$. Since a set of $(d-1)$-flats of Σ whose union contains all points of Σ contains at least θ_n/θ_d flats, we must have $h \leq \theta_d$; this implies that $f_q(n,h) < n - \log_q(h) - \log_q(q-1)$. Note that the order of q modulo k is crucial to the decomposition of $V = (\mathbb{Z}/p\mathbb{Z})^k$ into irreducible submodules, and therefore to the index of the subgroup H which arises. For example, if $k = q^n - 1$, there are irreducible submodules of dimension n, and the subgroup H acting on such a submodule considered as a $PG(n-1,q)$ is actually equal to the full Singer group. At the other extreme, if q is a primitive root modulo k, there are only two irreducible submodules: one of dimension one and one of dimension $k-1$. The subgroup of the Singer group of $PG(k-2,q)$ which arises in this case has size just $(k-1)/(k-1,p-1)$. In order, then, to use $f_p(n,h)$ to show that $g_p(k)$ and therefore Isbell's function $f_p(k)$ tends to infinity with k, it would be necessary that the actual value of $f_p(n,h)$ is very close to $n - \log_p(h)$, at least in the case $n = k-1$, $h = \theta_n/((k-1)/(k-1,p-1))$ which corresponds to p a primitive root modulo k. In the next section it is proven that, in all cases, $f_q(n,h) \geq n - 1 - 2\log_q(h)$.

4 Orbits of subgroups of Singer groups

We begin with a simple combinatorial observation.

Lemma 4.1 *If $g \in PGL(n,q)$ acts fixed point freely then for any d, $2 \leq d \leq n-1$ we have*

$$\sum_X |X \cap Xg| = \theta_n \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q, \tag{4}$$

where the sum is over all $(d-1)$-flats X.

Proof: If $d = 2$, the right hand side of (4) is just θ_n. Since g acts fixed point freely on Σ, for each point P of Σ there is at most one line (2-flat) ℓ such that $\ell \cap \ell g = \{P\}$. On the other hand, for each P, the line $\ell = Pg^{-1} \vee P$ clearly has the property that $\ell \cap \ell g = P$. Thus to each point P there is associated a unique line $\ell = \ell(P)$ such that $\ell \cap \ell g = P$, and (4) is true for $d = 2$. Now for arbitrary d, we see that for a $(d-1)$-flat X which contains a point P, if Xg contains P then X must contain $\ell(P)$, since otherwise we would have $P = X \cap \ell = Xg \cap \ell g = Pg$. On the other hand, any $(d-1)$ flat on P which contains ℓ certainly has the property that $P \in X \cap Xg$. Since the number of $(d-1)$-flats on ℓ is $\begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q$ the result follows. □

Now let $G = \langle \sigma \rangle$ be a Singer group of $\Sigma = PG(n-1,q)$. Then for any $(d-1)$-flat X, the orbit $\mathcal{B}$ of X under G forms a $(\theta_d/\theta_u, d-1)$-cover of Σ for some $u|(n,d)$, by Lemma 2.2. For each such orbit $\mathcal{B}$, we define a function $f_{\mathcal{B}} : G \to \mathbb{N}$ by

$$f_{\mathcal{B}}(g) = \sum_{X \in \mathcal{B}} |X \cap Xg|. \tag{5}$$

Note that, since G is abelian, $f_{\mathcal{B}}(g) = |\mathcal{B}||X \cap Xg|$ for any $X \in \mathcal{B}$. Since the set of $(d-1)$-flats is partitioned into G-orbits and any element of G acts non-trivially, Lemma 4.1 says that for any non-identity $g \in G$ we have

$$\sum_{\mathcal{B}} f_{\mathcal{B}}(g) = \theta_n \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q, \tag{6}$$

where the sum is over all G-orbits of $(d-1)$-flats.

Theorem 4.1 *Let G be a Singer group of $\Sigma = PG(n-1,q)$ and $H \leq G$ a subgroup of index h. If for some d we have $h \leq \sqrt{\theta_d}$ then there exists an H-orbit of $(d-1)$-flats whose union contains all points of Σ.*

Proof: Since we don't have any information on the intersection of H with the various subgroups which occur as stabilizers of $(d-1)$-orbits, we wish to restrict our attention to the orbits on $(d-1)$-flats with trivial stabilizers. As mentioned in the remark after Theorem 2.1, almost all $(d-1)$-flats occur in such orbits. We wish to find an orbit $\mathcal{B}$ with trivial stabilizer for which

$$\sum_{g\in H\setminus\{e\}} f_{\mathcal{B}}(g) \tag{7}$$

is reasonably small. Now Lemma 4.1 shows that

$$\sum_{\mathcal{B}} \sum_{g\in H\setminus\{e\}} f_{\mathcal{B}}(g) = \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q \theta_n \left(\frac{\theta_n}{h} - 1\right). \tag{8}$$

Even if it were the case that for every orbit with a non-trivial stabilizer the sum (7) was equal to zero, there would still be an orbit $\mathcal{B}$ with trivial stabilizer for which (7) was at most

$$\frac{\begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q \theta_n \left(\frac{\theta_n}{h} - 1\right)}{\frac{1}{\theta_n}\left(\sum_{t|(d,n)} \mu(t) \begin{bmatrix} n/t \\ d/t \end{bmatrix}_{q^t}\right)} \tag{9}$$

by (8) and (2) (with $u=1$). We claim that the sum (7) for this chosen orbit $\mathcal{B}$ actually satisfies

$$\sum_{g\in H\setminus\{e\}} f_{\mathcal{B}}(g) \leq \frac{\theta_d\theta_{d-1}(\theta_n)^2}{\theta_{n-1}h}, \tag{10}$$

that is that the right hand side of (10) is at least as large as the rather unpleasant looking (9). This can be verified directly in the case $d=2$ (using the assumption that $h \leq \sqrt{\theta_2}$). If $d \geq 3$ we proceed as follows. It is easily verified that the right hand side of (10) is obtained from (9) by substituting θ_n/h for $\theta_n/h - 1$, $\frac{1}{\theta_n}\begin{bmatrix} n \\ d \end{bmatrix}_q$ for the denominator of (9), and simplifying; the point is that (2) shows that the number of $(d-1)$-orbits with trivial stabilizer is close enough to $\frac{1}{\theta_n}\begin{bmatrix} n \\ d \end{bmatrix}_q$ that these two substitutions result in a net increase in quantity. This last claim follows from our assumption $d \geq 3$ and the fact that for any n and d, $\begin{bmatrix} n \\ d \end{bmatrix}_q$ is a polynomial of degree $n(n-d)$ in q.

Thus we have shown that there exists at least one G-orbit $\mathcal{B}$ of $(d-1)$-flats with trivial G-stabiliser which satisfies (10). Let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_h$ denote the orbits of H on the points of Σ, and $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_h$ the suborbits of H on the $(d-1)$-flats of B . We define for each j a function $f_j = f_{\mathcal{B}_j}(g)$ on H, by analogy with the definition of the $f_{\mathcal{B}}$. Now the $\mathcal{P}_i$ and $\mathcal{B}_j$ form a symmetric tactical decomposition of the tactical configuration whose points are the points of Σ_{n-1} and whose blocks are the elements of $\mathcal{B}$. Therefore if we define a_{ij} to be the number of points of $\mathcal{P}_i$ which are contained in a given $X \in \mathcal{B}_j$, a_{ij} is also the number of $(d-1)$-flats in $\mathcal{B}_j$ which contain a given $P \in \mathcal{P}_i$, and counting flags gives, for each j,

$$\begin{aligned} \sum_{i=i}^{h} a_{ij} &= \theta_d \\ \sum_{i=1}^{h} a_{ij}(a_{ij}-1) &= \frac{h}{\theta_n} \sum_{g \in H \setminus \{e\}} f_j(g). \end{aligned}$$

Now there exists some j for which

$$\sum_{g \in H \setminus \{e\}} f_j(g) \leq \frac{1}{h} \frac{\theta_d \theta_{d-1} (\theta_n)^2}{\theta_{n-1} h}$$

by (10); adding the two equations above for this j gives

$$\sum_{i=1}^{h} a_{ij}^2 \leq \theta_d \left(1 + \frac{\theta_{d-1}\theta_n}{\theta_{n-1} h}\right).$$

If one assumes that some $a_{ij} = 0$, the variance inequality implies that

$$\sum_{i=1}^{h} a_{ij}^2 \geq \frac{1}{h-1} \left(\sum_{i=1}^{h} a_{ij}\right)^2 = \frac{1}{h-1} (\theta_d)^2;$$

and after some manipulation this implies that $h \geq 1 + \sqrt{\theta_d}$. □

Corollary 4.1 *The function $f_q(n,h)$ defined in the previous section satisfies $f_q(n,h) \geq n - 1 - 2\log_q(h)$.*

Proof: For the stated inequality to be non-trivial, we must have $h^2 < q^{n-1}$. Assuming this, choose the smallest d such that $h \leq \sqrt{\theta_d}$. The inequality $h > \sqrt{\theta_{d-1}}$ yields the result. □

5 Concluding Remarks

As noted in the introduction, many interesting geometric objects arise as orbits of Singer groups or subgroups of Singer groups. It seems, however, that only point (and, in the case of [9], line) orbits have been considered. Thus the question of determining the geometric structure of the orbits of Singer groups on $(d-1)$-flats for arbitrary d arises. The simplest non-trivial case is that of the $(q+1)$-covers of $PG(3,q)$ which arise as the line orbits with trivial stabilizer of a Singer group. It is shown in [9] that these sets have the property that the set of $q+1$ line on a given point form a non-degenerate conic in the quotient plane. Although this property is, for q odd, shared by the set of totally isotropic lines of a symplectic polarity, B. Huppert ([7]) has proven that the largest cyclic subgroup in $PSp(4,q)$ has size q^2+1; this obviously implies that the orbits do not have this structure.

We should also note that the argument in Section 2 goes through unchanged to give the number of orbits of an n-cycle of S_n, the symmetric group on n letters on the set of subsets of size d. Furthermore, Lemma 4.1 can be generalised to arbitrary elements of $PGL(n,q)$, the result being that if $g \in PGL(n,q)$ fixes exactly a points then we have, for any $2 \leq d \leq n-1$,

$$\sum_X |X \cap Xg| = \theta_n \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q + a \left(\begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q - \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q \right).$$

Note that this is independent of the actual configuration of the set of fixed points. The analogous result holds for elements of S_n.

References

[1] T.M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.

[2] P.J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999.

[3] P.J. Cameron, Permutations, submitted to the proceedings of the conference Paul Erdős and his mathematics, held July 4-11 1999, Budapest.

[4] G.L. Ebert, Partitioning projective geometries into caps *Can. J. Math.* **37** (1985), 1163-1175.

[5] G.L. Ebert, The completion problem for partial packings, *Geom. Dedicata* **18** (1985) #2, 261-267.

[6] J.C. Fisher, J.W.P. Hirschfeld and J.A. Thas, Complete arcs in planes of square order *Ann. Discrete Math.* **30** (1986), 243-250.

[7] B. Huppert, Singer-Zyklen in klassischen Gruppen, *Math. Z.* **117** (1970), 141-150.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., Amsterdam, 1977.

[9] D. Glynn, On a set of lines of $PG(3,q)$ corresponding to a maximal cap contained in the Klein quadric of $PG(5,q)$, *Geom. Dedicata* **26** (1988) #3, 273-280.

[10] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Am. Math. Soc.* **43** (1938), 377-385.