Incidence matrices, permutation characters and the minimal genus of a permutation group

Daniel Frohardt
Robert Guralnick
Kay Magaard

September 2, 2004

1 Introduction

Let V be a non-degenerate symplectic, orthogonal, or unitary space of dimension n over $GF(q)$. Let $\mathcal{X}$ be the collection of all totally singular points (1-spaces) of V, and let $\mathcal{U}$ be the collection of all k-subspaces of V of a given isometry type, either totally singular or non-degenerate. Let H be the incidence matrix of $\mathcal{X}$ with $\mathcal{U}$ and let $M = HH^t$. Our purpose here is to prove the following.

Theorem 1.1 *Assume that $2 \leq k < n$. Then either M is non-singular or one of the following is true.*

1. *$\mathcal{U}$ consists of totally singular subspaces of maximal dimension.*
2. *V is orthogonal or unitary, and the elements of $\mathcal{U}$ are non-degenerate hyperplanes of V.*
3. *V is orthogonal of even dimension and type ϵ for some ϵ, and the elements of $\mathcal{U}$ have codimension 2 in V and type $-\epsilon$.*
4. *$M = 0$. [V is orthogonal, $k = 2$, and the elements of $\mathcal{U}$ contain no singular points.]*

Corollary 1.2 *Let G be an almost simple classical group with natural module V of dimension n. If G is linear, assume that G does not contain a graph automorphism. Let $2 \leq k < n - 1$, and let K be the stabilizer of a non-degenerate or totally singular k-space of V. Let P be the stabilizer of a singular 1-space of V. Then the permutation module 1_P^G is a submodule of 1_K^G unless one of the following holds.*

1. *K is the stabilizer of a maximal totally singular subspace of V.*
2. *K is the stabilizer of a 2-space containing no singular points or the orthogonal complement of such.*

The next result is about monodromy groups of coverings of smooth projective curves over an algebraically closed field k of characteristic $p \geq 0$. We will define the terms in the corollary later in the paper (see §8).

Corollary 1.3 *Fix an algebraically closed field of characteristic $p \geq 0$. Let S be a simple classical group with natural module V of dimension d. The minimal genus among all almost simple groups G with given socle S is realized on one of the following permutation actions:*

1. *Action on 1-spaces of V.*
2. *Action on maximal totally singular subspaces of V.*
3. *S is orthogonal and the action is on minus type 2-spaces.*
4. *S is linear, d is even and G contains a graph automorphism and the action is on $d/2$-spaces or pairs of complementary $d/2$-spaces.*
5. *A non-k-space action.*

We prove our theorem by computing eigenvectors and eigenvalues for the matrix M. We shall also obtain the dimensions of the eigenspaces. Corollary 1.2 follows from an elementary argument using linear algebra. Corollary 1.3 follows from a classical result that characterizes the genus of a curve X as one half the dimension of the ℓ-torsion points of the Jacobian of X and Frobenius reciprocity.

Let G be the group of all isometries of V. The action of G commutes with M.

The cases we consider are as follows:

1. $\mathcal{U}$ consists of totally singular k-subspaces, $1 \leq k \leq w(V)$, where $w(V)$ is the largest dimension of a totally singular subspace of V.
2. $\mathcal{U}$ consists of non-degenerate k-subspaces, $2 \leq k < n-1$ and $M \neq 0$.

Remark. The condition $M \neq 0$ in case 2 excludes only the situation where V is orthogonal, $k = 2$, and members of $\mathcal{U}$ are of $-$ type.
Remark. The action of G on $\mathcal{X}$ is doubly transitive when G has Lie rank 1. Otherwise, the action of G on $\mathcal{X}$ is a rank 3 permutation action.

The second and third authors thank the Mathematical Sciences Research Institute for its generous hospitality and support. The second author acknowledges the support of NSF and the third author acknowledges the support of NSA. The third author also acknowledges support by a career development chair from Wayne State University.

2 Notation

For $\alpha \in \mathcal{X}$, set $\mathcal{X}_0(\alpha) = \{\beta \in \mathcal{X} : \beta \subseteq \alpha^\perp, \beta \neq \alpha\}$. $\mathcal{X}_1(\alpha) = \{\beta \in \mathcal{X} : \beta \not\subseteq \alpha^\perp\}$. $\mathcal{X}_\infty(\alpha) = \{\alpha\}$. Let $\alpha_\infty \in \mathcal{X}$ be fixed and set $\mathcal{X}_i = \mathcal{X}_i(\alpha_\infty)$. Set $I = \{i \in \{\infty, 0, 1\} : \mathcal{X}_i \neq \emptyset\}$, and choose $\alpha_i \in \mathcal{X}_i$ for each $i \in I$.

For each $i \in I$, set

$$\mathcal{U}_i(\alpha) = \{U \in \mathcal{U} : \alpha, \alpha_i \sim U\},$$

$$x = |\mathcal{X}|,$$

$$x_i = |\mathcal{X}_i(\alpha)|, \text{ and}$$

$$m_i = |\mathcal{U}_i(\alpha)|.$$

Note that x_i and m_i are independent of the choice of α because G acts transitively on $\mathcal{X}$.

Let $\mathbf{X}$ be a complex vector space with basis $\mathcal{X}$, so that $\mathbf{X}$ is a permutation module for G.

For $i \in I$, define the linear transformation T_i on $\mathbf{X}$ by

$$T_i(\alpha) = \sum_{\beta \in \mathcal{X}_i(\alpha)} \beta,$$

and set

$$T = \sum_{i \in I} m_i T_i.$$

Since $g(\mathcal{X}_i(\alpha)) = \mathcal{X}_i(g(\alpha))$ for all $g \in G$, it follows that T_i is G-equivariant for all $i \in I$ and so is T.

The eigenvalues for T are easily seen to be the same as the eigenvalues for M. We shall find a complete set of eigenspaces for T that are spanned by elements of $\mathbf{X}$ of the form $\gamma_i(\alpha), \alpha \in \mathcal{X}, i \in I$, where

$$\gamma_i(\alpha) = \sum_{\beta \in \mathcal{X}_i(\alpha)} \beta.$$

Let $\alpha = \alpha_\infty$ and set $\mathcal{X}_j = \mathcal{X}_j(\alpha)$ and $\gamma_j = \gamma_j(\alpha)$. For $k, i, j \in I$, set

$$t_{kij} = |\mathcal{X}_j \cap \mathcal{X}_i(a_k)|.$$

Lemma 2.1 $T_i(\gamma_j) = \sum_{k \in I} t_{kij} \gamma_k, \quad i, j \in I.$

Proof. If $\beta \in \mathcal{X}_i$, then

$$\sum_{g \in G_\alpha} g(\beta) = |G_{\alpha,\alpha_i}| \, \gamma_i.$$

For $g \in G_\alpha$, we have $T_i(g(\gamma_j)) = T_i(\gamma_j)$. Also,

$$T_i(\gamma_j) = \sum_{\gamma \in \mathcal{X}_j} \sum_{k \in I} \sum_{\beta \in \mathcal{X}_k \cap \mathcal{X}_i(\gamma)} \beta.$$

Because $\gamma \in \mathcal{X}_k(\delta)$ if and only if $\delta \in \mathcal{X}_k(\gamma)$ we have

$$|\mathcal{X}_j| \, |\mathcal{X}_k \cap \mathcal{X}_i(\alpha_j)| \, = \, |\mathcal{X}_k| \, |\mathcal{X}_j \cap \mathcal{X}_i(\alpha_k)| \, . \tag{1}$$

Counting $|\{(\alpha, \beta, \gamma) : \beta \in \mathcal{X}_j(\alpha), \gamma \in \mathcal{X}_k(\alpha), \gamma \in \mathcal{X}_i(\beta)\}|$ in two ways, it follows that

$$\begin{array}{rcl} |G_\alpha| \, T_i(\gamma_j) & = & \sum_{\gamma \in \mathcal{X}_j} \sum_{k \in I} \sum_{\beta \in \mathcal{X}_k \cap \mathcal{X}_i(\gamma)} \sum_{g \in G_\alpha} \beta \\ & = & \sum_{k \in I} \sum_{\gamma \in \mathcal{X}_j} |\mathcal{X}_k \cap \mathcal{X}_i(\gamma)| \, |G_{\alpha,\alpha_i}| \, \gamma_k \\ & = & \sum_{k \in I} |\mathcal{X}_j| \, |\mathcal{X}_k \cap \mathcal{X}_i(\alpha_j)| \, (\, |G_\alpha| \, / \, |\mathcal{X}_k| \,) \gamma_k \\ & = & |G_\alpha| \, \sum_{k \in I} |\mathcal{X}_j \cap \mathcal{X}_i(\alpha_k)| \, \gamma_k. \end{array}$$

■

Lemma 2.2 *1.* $t_{kij} = t_{kji}, \quad k, i, j \in I.$

2. $x_k t_{kij} = x_i t_{ikj}, \quad k, i, j \in I$

3. $\sum_{j \in I} t_{kij} = x_i, \quad k, i \in I.$

4. $t_{\infty ii} = x_i, \quad i \in I.$

5. $t_{k \infty k} = t_{kk \infty} = 1, \quad k \in I.$

6. $t_{\infty ij} = t_{i \infty j} = t_{ij \infty} = 0, \quad i \neq j, \quad i, j \in I.$

Proof. The second statement follows from the first statement and equation (1), above. The remaining statements follow easily from the definitions. ■

Set $\sigma(n, k)$ equal to the number of totally singular k-subspaces in n-space, and $\nu(n, k)$ equal to the number of non-degenerate k-spaces of n-space. When the spaces are orthogonal, we really mean k^δ-spaces of n^ϵ-space.

We dispose of the situation $\mathcal{X}_0 = \emptyset$ before considering the general case.

3 The doubly transitive case

Suppose $\mathcal{X}_0 = \emptyset$. Then V contains no totally singular lines. Therefore G has Lie rank 1. The hypothesis implies that $\dim V > 2$. Therefore V must be one of the following: orthogonal of dimension 3, orthogonal of dimension 4 and type $-$, or unitary of dimension 3. We have $x = q^r + 1$ and $x_1 = q^r$, where $r = 1, 2, 3/2$ in the respective cases. Furthermore, the members of $\mathcal{U}$ must be non-degenerate because V contains no totally singular 2-spaces. This implies that $m_\infty = \nu(n, k)\sigma(k, 1)/\sigma(n, 1)$, and $m_1 = \nu(n-2, k-2) = q^{-(n-k)} m_\infty$.

We have

$$T = m_\infty T_\infty + m_1 T_1,$$

$$T_0(\gamma_\infty) = \gamma_1,$$
$$T_0(\gamma_1) = x_1\gamma_\infty + (x_1 - 1)\gamma_1.$$

Set $\mathbf{x}_1 = \gamma_\infty + \gamma_1$ and $\mathbf{x}_2 = \mathbf{x}_2(\alpha) = x_1\gamma_\infty - \gamma_1$. Set $\mathbf{X}_1 = \langle \mathbf{x}_1 \rangle$ and $\mathbf{X}_2 = \langle \mathbf{x}_2(\beta) : \beta \in \mathcal{X} \rangle$.

We have $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2$,

$$T_1(\mathbf{x}_1) = x_1\mathbf{x}_1$$

and

$$T_1(\mathbf{x}_2) = -\mathbf{x}_2.$$

Proposition 3.1 *If G has Lie rank 1, V is non-degenerate, and $\mathcal{U}$ consists of non-degenerate k-spaces, then $\mathbf{X}_1$ and $\mathbf{X}_2$ are eigenspaces with respective eigenvalues $(q^{n-k}+q^r)\nu(n-2,k-2)$ and $(q^{n-k}-1)\nu(n-2,k-2)$ and dimensions 1 and q^r, r as above.*

Proof. $\mathbf{X}_1$ and $\mathbf{X}_2$ are eigenspaces for T_1 by the previous calculation. The eigenvalue of T on $\mathbf{X}_1$ is $m_\infty + m_1 x_1 = (q^{n-k} + q^r)\nu(n-2, k-2)$ and the eigenvalue of T on $\mathbf{X}_2$ is $m_\infty - m_1 = (q^{n-k} - 1)\nu(n-2, k-2)$. ∎

M is therefore nonsingular when $2 \leq k < n$.

For the remainder of this section we assume that G is linear with natural module V of dimension n. Since, in this case we do not have a form, we set $\mathcal{X}_1 = \emptyset$. We let $\mathcal{U}$ be the collection of all k-spaces of V.

We have $x = \frac{q^d-1}{q-1}$ and $x_1 = x - 1$. Furthermore, the members of $\mathcal{U}$ are totally singular because G stabilizes no form on V. This implies that $m_\infty = \lambda(n,k)\lambda(k,1)/\lambda(n,1) = \lambda(n-1,k-1)$, and $m_0 = \lambda(n-2,k-2) = \frac{(q^{k-1}-1)}{(q^{n-1}-1)}m_\infty$, where $\lambda(n,k)$ denotes the number of k-subspaces of n-space.

We have

$$T = m_\infty T_\infty + m_0 T_0,$$
$$T_0(\gamma_\infty) = \gamma_0,$$
$$T_0(\gamma_0) = x_0\gamma_\infty + (x_0 - 1)\gamma_0.$$

Set $\mathbf{x}_1 = \gamma_\infty + \gamma_0$ and $\mathbf{x}_2 = \mathbf{x}_2(\alpha) = x_0\gamma_\infty - \gamma_0$. Set $\mathbf{X}_1 = \langle \mathbf{x}_1 \rangle$. and $\mathbf{X}_2 = \langle \mathbf{x}_2(\beta) : \beta \in \mathcal{X} \rangle$.

Proposition 3.2 *If G is linear with natural module V, and $\mathcal{U}$ consists of k-spaces, with $2 \leq k \leq n-2$, then $\mathbf{X}_1$ and $\mathbf{X}_2$ are eigenspaces with respective eigenvalues $[\frac{q^{n-1}-1}{q^{k-1}-1} + \lambda(n,1) - 1]\lambda(n-2,k-2)$ and $[\frac{q^{n-1}-1}{q^{k-1}-1} - 1]\lambda(n-2,k-2)$ and dimensions 1 and $\lambda(n,1) - 1$.*

Proof. The argument is identical to that of the proposition above. ∎

4 The generic case

Now suppose that $\mathcal{X}_0 \neq \emptyset$, so G has Lie rank at least 2. $\mathcal{X}_0$ consists of all totally singular points in $\alpha^\perp$ distinct from α, and $\mathcal{X}_1$ consists of all totally singular points in V lying outside $\alpha^\perp$. It follows from Witt's Theorem that G_α is transitive on $\mathcal{X}_0$ and $\mathcal{X}_1$.

We have $|\mathcal{X}| = \sigma(n,1)$. Every totally singular 2-space U containing a contains exactly q elements of $\mathcal{X}_0$, and every element of $\mathcal{X}_0$ generates, with a, a unique totally singular 2-space. The totally singular 2-spaces containing a are in one-to-one correspondence with the totally singular 1-spaces in $\langle a\rangle^\perp/\langle a\rangle$. Therefore

$$x_0 = q\sigma(n-2,1).$$

We have $\sigma(n,1) = (Aq-1)(Bq+1)/(q-1)$ and $\sigma(n-2,1) = (A-1)(B+1)/(q-1)$ where $A = q^{n/2-1-a}$ and $B = q^{n/2-1-b}$, and a and b are given in the following table.

type	S	O^+	O^-	O°	U, n even	U, n odd
a	0	0	1	1/2	0	1/2
b	0	1	0	1/2	1/2	0

Therefore

$$x = \frac{(Aq-1)(Bq+1)}{q-1}, \text{and}$$

$$x_0 = \frac{(A-1)(B+1)}{q-1}q.$$

It follows that

$$x_1 = x - x_0 - 1 = qAB.$$

Since $\langle a, a_1\rangle$ is non-degenerate, it follows that $\langle a, a_1\rangle^\perp$ is a non-degenerate $n-2$-space (and of the same type as V in the orthogonal case). Therefore

$$t_{100} = \sigma(n-2,1) = \frac{(A-1)(B+1)}{q-1}.$$

It follows that

$$t_{001} = \frac{t_{100}x_1}{x_0} = AB;$$

$$t_{101} = x_0 - t_{100} = (A-1)(B+1);$$

$$t_{000} = x_0 - t_{001} - 1 = \frac{AB + q(A-B) - 2q + 1}{q-1};$$

$$t_{011} = \frac{t_{101}x_1}{x_0} = (q-1)AB;$$

$$t_{111} = x_1 - t_{101} - 1 = (q-1)AB - (A-B).$$

We have

$$T = m_\infty T_\infty + m_0 T_0 + m_1 T_1$$

Table 1: Eigenvalues for T_h, totally singular points

vector	T_∞	T_0	T_1
$\mathbf{x}_1$	1	$(A-1)(B+1)q/(q-1)$	qAB
$\mathbf{x}_2$	1	$-B-1$	B
$\mathbf{x}_3$	1	$A-1$	$-A$

where T_∞ is the identity matrix,

$$T_0(\gamma_X) = \begin{cases} \gamma_0 & X=\infty \\ \frac{(A-1)(B+1)}{q-1}q\gamma_\infty + \frac{AB+q(A-B)-2q+1}{q-1}\gamma_0 + \frac{(A-1)(B+1)}{q-1}\gamma_1 & X=0 \\ AB\gamma_0 + (A-1)(B+1)\gamma_1 & X=1 \end{cases}$$

$$T_1(\gamma_X) = \begin{cases} \gamma_1 & X=\infty \\ AB\gamma_0 + (A-1)(B+1)\gamma_1 & X=0 \\ qAB\gamma_\infty + (q-1)AB\gamma_0 + ((q-1)AB - A + B)\gamma_1 & X=1. \end{cases}$$

Set

$$\mathbf{x}_1 = \gamma_\infty + \gamma_0 + \gamma_1,$$
$$\mathbf{x}_2 = qA(A-1)\gamma_\infty - (q-1)A\gamma_0 + (A-1)\gamma_1, \text{ and}$$
$$\mathbf{x}_3 = qB(B+1)\gamma_\infty + (q-1)B\gamma_0 - (B+1)\gamma_1.$$

A straightforward computation shows that $\mathbf{x}_1$, $\mathbf{x}_2$, and $\mathbf{x}_3$ are simultaneous eigenvectors for T_0 and T_1 with eigenvalues as shown in Table 1.

Set $\mathbf{X}_1 = \langle \mathbf{x}_1 \rangle$, $\mathbf{X}_2 = \langle \mathbf{x}_2(\beta) : \beta \in \mathcal{X} \rangle$, and $\mathbf{X}_3 = \langle \mathbf{x}_3(\beta) : \beta \in \mathcal{X} \rangle$. Then $\mathbf{X}_1$, $\mathbf{X}_2$, and $\mathbf{X}_3$ are eigenspaces for T and $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3$.

Proposition 4.1 *1. If $v \in \mathbf{X}_i$, then $T(v) = \lambda_i v$ where*

$$\lambda_i = \begin{cases} m_\infty + x_0 m_0 + x_1 m_1 & i=1 \\ m_\infty - m_0 - B(m_0 - m_1) & i=2 \\ m_\infty - m_0 + A(m_0 - m_1) & i=3. \end{cases}$$

2.

$$\dim \mathbf{X}_i = \begin{cases} 1 & i=1 \\ \dfrac{qA(qB+1)(A-1)}{(q-1)(A+B)} & i=2 \\ \dfrac{qB(B+1)(qA-1)}{(q-1)(A+B)} & i=3. \end{cases}$$

Proof. The assertion about λ_i follows from the previous discussion.

We have

$$\begin{aligned} \dim \mathbf{X} &= \dim \mathbf{X}_1 + \dim \mathbf{X}_2 + \dim \mathbf{X}_3 \\ &= 1 + \dim \mathbf{X}_2 + \dim \mathbf{X}_3, \quad \text{and} \end{aligned}$$
$$\mathrm{Tr}T = m_\infty x = \lambda_1 + \lambda_2 \dim \mathbf{X}_2 + \lambda_3 \dim \mathbf{X}_3.$$

These equations hold when $\mathcal{U}$ is the set of singular 2-spaces, that is, when $m_0 = 1$ and $m_1 = 0$. Set $\mu_i = \dim \mathbf{X}_i$. Therefore

$$x_0 - (B+1)\mu_2 + (A-1)\mu_3 = 0, \text{ and}$$

$$1 + \mu_2 + \mu_3 = x.$$

It follows that

$$\mu_2 = \frac{qA(qB+1)(A-1)}{(q-1)(A+B)}$$

$$\mu_3 = \frac{qB(B+1)(qA-1)}{(q-1)(A+B)}.$$

■

When V is symplectic,

$$\mu_2 = \frac{q(q^{n/2}+1)(q^{n/2-1}-1)}{2(q-1)}$$

$$\mu_3 = \frac{q(q^{n/2-1}+1)(q^{n/2}-1)}{2(q-1)}.$$

5 Totally singular subspaces

Lemma 5.1 *Let $\lambda(n,k)$ denote the number of k-subspaces of n-space, $\sigma(n,k)$ the number of totally singular k-subspaces of n-space, and $\nu(n,k)$ the number of non-degenerate k-subspaces of n-space.*

1. $\sigma(n,k)\lambda(k,1) = \sigma(n,1)\sigma(n-2,k-1)$.
2. $\nu(n,k)\sigma(k,1) = \sigma(n,1)\nu(n-2,k-2)q^{n-k}$.

Proof. To prove the first statement, count the number of pairs (U,x) where U is a totally singular k-subspace and x is a totally singular point in U in the two obvious ways. To prove the second by a similar argument, it is necessary to note that if x is a totally singular point and $x \in U$, where U is a non-degenerate k-space, then $U^\perp$ is a non-degenerate $n-k$-subspace of $x^\perp$. Thus $(U^\perp + x)/x$ is a non-degenerate $n-k$-subspace of the non-degenerate $n-2$ space $x^\perp/x$. The number of such $n-k$-subspaces of $x^\perp/x$ is $\nu(n-2,k-2)$. For each choice of $U^\perp + x$, there are q^{n-k} complements to x, each of which corresponds to a different U. ■

Since the number of totally singular points in n-space is given by $(q^{n/2-a}-1)(q^{n/2-b}+1)/(q-1)$, we have the following corollary.

Corollary 5.2 1. $\sigma(n,k)(q^k-1) = (q^{n/2-a}-1)(q^{n/2-b}+1)\sigma(n-2,k-1)$.

2. $\nu(n,k)(q^{k/2-a}-1)(q^{k/2-b}+1) = (q^{n/2-a}-1)(q^{n/2-b}+1)q^{n-k}\nu(n-2,k-2)$.

Proposition 5.3 *When $\mathcal{U}$ consists of totally singular subspaces,*

$$\lambda_1 = \frac{q^k - 1}{q - 1}\sigma(n-2, k-1)$$

$$\lambda_2 = \frac{A - q^{k-1}}{A - 1}\sigma(n-2, k-1)$$

$$\lambda_3 = \frac{B + q^{k-1}}{B + 1}\sigma(n-2, k-1)$$

Proof.

$$m_\infty = \sigma(n-2, k-1),$$

$$m_0 = \sigma(n-4, k-2) = \frac{q^{k-1} - 1}{(A-1)(B+1)}m_\infty,$$

and

$$m_1 = 0.$$

Therefore

$$\lambda_1 = (1 + \frac{q}{q-1}(q^{k-1} - 1))m_\infty = \frac{q^k - 1}{q-1}m_\infty,$$

$$\lambda_2 = (1 - \frac{q^{k-1} - 1}{A-1})m_\infty = \frac{A - q^{k-1}}{A-1}m_\infty,$$

$$\lambda_3 = (1 + \frac{q^{k-1} - 1}{B+1})m_\infty = \frac{B + q^{k-1}}{B+1}m_\infty.$$

■

It is apparent that $\lambda_1 \neq 0$ and $\lambda_3 \neq 0$ whenever $1 \leq k \leq n/2$. Therefore M is nonsingular if and only if $\lambda_2 \neq 0$. We have $\lambda_2 = 0$ exactly when $q^{k-1} = A$, that is, when $k - 1 = n/2 - a - 1$. In other words, when $k = n/2 - a$.

If V is symplectic, orthogonal of + type, or unitary of even dimension, then $a = 0$, so M is singular if and only if $k = n/2$.

If V is orthogonal or unitary of odd dimension, then $a = 1/2$, so M is singular if and only if $k = (n-1)/2$.

If V is orthogonal of $-$ type, then $a = 1$, so M is singular if and only if $k = n/2 - 1$.

6 Non-degenerate subspaces

Proposition 6.1 *Suppose $\mathcal{U}$ consists of non-degenerate subspaces. Then the respective eigenvalues λ_i on the spaces $\mathbf{X}_i$ described above are*

$$\lambda_1 = \frac{q^2AB - K^2 + qK(A' - B')}{q-1}\nu(n-2, k-2)$$

$$\lambda_2 = \frac{(AK - A')(A'K + B)}{A'(A-1)}\nu(n-2, k-2)$$
$$\lambda_3 = \frac{(BK - B')(B'K + A)}{B'(B+1)}\nu(n-2, k-2)$$

Proof. We have $m_\infty = \nu(n,k)\sigma(k,1)/\sigma(n,1)$, $m_0 = \nu(n,k)\sigma(k,2)/\sigma(n,2)$, and $m_1 = \nu(n-2, k-2)$.

$$\begin{aligned} m_\infty &= \frac{\sigma(k,1)\sigma(n,2)}{\sigma(k,2)\sigma(n,1)}m_0 \\ &= \frac{(q^{n/2-1-a}-1)(q^{n/2-1-b}+1)}{(q^{k/2-1-a'}-1)(q^{k/2-1-b'}+1)}m_0 \\ &= \frac{(A-1)(B+1)}{(A'/K-1)(B'/K+1)}m_0 \end{aligned}$$

where $K = q^{(n-k)/2}$, $A' = q^{n/2-1-a'}$, and $B' = q^{n/2-1-b'}$. [a' and b' depend on the type of the k-space.]

We have

$$m_0 = \frac{(A'-K)(B'+K)}{(A-1)(B+1)K^2}m_\infty = \frac{(A'-K)(B'+K)}{(A-1)(B+1)}m_1, \text{ and}$$

$$m_\infty = q^{n-k}m_1 = K^2 m_1.$$

Therefore,

$$\begin{aligned} \lambda_1 &= m_\infty + m_0 x_0 + m_1 x_1 \\ &= \frac{q^2AB - K^2 + qK(A'-B')}{q-1}m_1. \end{aligned}$$

$$\begin{aligned} \lambda_2 &= m_\infty - (B+1)m_0 + Bm_1 \\ &= (K^2 - \frac{(A'-K)(B'+K)}{A-1} + B)m_1 \\ &= \frac{(AK-A')(A'K+B)}{A'(A-1)}m_1 \end{aligned}$$

$$\begin{aligned} \lambda_3 &= m_\infty + (A-1)m_0 - Am_1 \\ &= (K^2 + \frac{(A'-K)(B'+K)}{B+1} - A)m_1 \\ &= \frac{(BK-B')(B'K+A)}{B'(B+1)}m_1 \end{aligned}$$

■

Corollary 6.2 *If $\mathcal{U}$ consists of nondegenerate spaces and $2 \leq k < n$ then either M is non-singular or one of the following is true.*

1. *$k = 2$ and $\mathcal{U}$ consists of orthogonal 2-spaces of $-$-type.*
2. *$k = n - 1$ and V is either orthogonal or unitary.*
3. *$k = n - 2$, V is orthogonal, and the orthogonal complement of a member of $\mathcal{U}$ is an orthogonal 2-space of $-$-type.*

Conversely, M is singular in each of these situations.

Proof. If members of $\mathcal{U}$ contain no totally singular points, then $M = 0$ and the first condition holds. We may therefore assume that members of $\mathcal{U}$ contain totally singular points. We have that M is singular if and only if $\lambda_i \neq 0$ for some $i \in \{1, 2, 3\}$.

In all cases, $\lambda_1 > 0$ because λ_1 is a sum of positive integers. Since $k \geq 2$, we have $\lambda_2 = 0$ exactly when $AK = A'$ and $\lambda_3 = 0$ exactly when $BK = B'$.

The condition $AK = A'$ is equivalent to $a' + (n-k)/2 = a$, or $k = n - 2(a - a')$. Similarly, the condition $BK = B'$ is equivalent to $b' + (n - k)/2 = b$, or $k = n - 2(b - b')$.

In the symplectic case, we have $a = a' = 0$, so $AK = A'$ only when $n = k$.

In the unitary case, we have $0 \leq a \leq 1/2$ and $0 \leq a' \leq 1/2$, so $n - 2(a - a') \geq n - 1$. Thus λ_2 and λ_3 are non-zero whenever $k \leq n - 2$, and M is nonsingular in this case. Suppose $k = n - 1$. We have $a' - a = b - b' = \pm 1/2$, so either $AK = A'$ or $BK = B'$. Either way, M is singular.

In the orthogonal case, since $0 \leq a \leq 1$ and $0 \leq a' \leq 1$, we have that λ_2 and λ_3 are non-zero (whence M is nonsingular) whenever $k < n - 2$. The argument for $k = n - 1$ is the same as in the unitary case. Suppose $k = n - 2$. If U and V are of the same type, then $a = a'$ and $b = b'$, whence $AK = A'$ if and only if $k = n$. If U and V are of different types, then $a' - a = b - b' = \pm 1$, so either $AK = A'$ or $BK = B'$. Either way, M is singular. ∎

7 Proof of the first corollary

Let G be a finite group with K and P subgroups. Let $\mathcal{U}$ denote the set of cosets of K and $\mathcal{X}$ the set of cosets of P. Let H denote the incidence matrix of $\mathcal{X}$ with $\mathcal{U}$. Let $W = 1_K^G$ be the permutation module (over $\mathbb{C}$). Let $\{w_u\}$ be a permutation basis of W. Let P be the stabilizer of $x \in \mathcal{X}$ and let $\mathcal{U}(x)$ be the collection of those members of $\mathcal{U}$ intersecting x. By v_x we denote the vector $\sum_{u \in \mathcal{U}(x)} w_u$. We consider the submodule of W generated by the G-orbit of v_x. We observe that v_x^G is spanned by the vectors v_y, where $y \in \mathcal{X}$. We now want to know when this set is linearly independent. So suppose that

$$0 = \sum_{y \in \mathcal{X}} \alpha_y v_y$$

$$= \sum_{y \in \mathcal{X}} \alpha_y \sum_{u \in \mathcal{U}(y)} w_u$$

$$= \sum_{u \in \mathcal{U}} (\sum_{y \in u} \alpha_y) w_u.$$

Now $\sum_{y \in u} \alpha_y = 0$ for all $u \in \mathcal{U}$ if and only if

$$H^t[\alpha_y] = 0,$$

where $[\alpha_y]$ is a column vector. So $\{v_x^G\}$ is linearly independent if and only if H has full rank. Since P fixes the vector v_x, this implies that $\{v_x^G\}$ is isomorphic to 1_P^G. So we have shown that:

Lemma 7.1 *1_P^G embeds in 1_K^G if and only if H has full rank $|G : P|$.*

Since M and H have the same rank (via an elementary linear algebra argument), corollary 1.2 follows in all cases.

For comparison we include a purely character theoretic proof of the totally singular case of corollary 1.2 (as well as the linear case). See [GLMS] for a slightly stronger result in the linear case.

Lemma 7.2 *Let G be an almost simple classical group. If G is linear, assume that G does not contain a graph automorphism. Let P_j denote the stabilizer of a totally singular j-dimensional subspace of the natural module V for G. Then $1_{P_1}^G$ embeds in $1_{P_j}^G$ unless G is not linear and j is maximal.*

Proof. Let W be the Weyl group of G and W_i the corresponding parabolic subgroup of G. Because of the correspondence between irreducible constitutents of 1_B^G with B a Borel subgroup of G and those of W (cf. [CR], 68.24), it suffices to prove that $1_{W_1}^W$ embeds in $1_{W_j}^W$.

If G is linear, then $(1_{W_1}^W, 1_{W_1}^W) = 2 = (1_{W_1}^W, 1_{W_j}^W)$. Since the trivial character only occurs once in $1_{W_j}^W$, the result follows.

In the remaining cases, $(1_{W_1}^W, 1_{W_1}^W) = 3 = (1_{W_1}^W, 1_{W_j}^W)$ for j not maximal. The trivial character occurs once in each permutation character. Let χ denote the character of the reflection representation of W. Since W_j is a maximal parabolic subgroup of W, we know that $\chi|_{W_j} = 1 \oplus \chi_j$ where χ_j is the reflection representation of W_j. Thus, χ also occurs precisely once in each $1_{W_j}^W$. It follows that the remaining irreducible constitutent of $1_{W_1}^W$ occurs in $1_{W_j}^W$ for every non-maximal j.

■

8 The minimal genus of a classical group

We now come to our second corollary. Let k be an algebraically closed field of characteristic $p \geq 0$. Let G be a finite group, P a core free subgroup of G of

index n and let $x_1, ..., x_r \in G$ be generators of G whose product is one. The index of x_i is defined as $ind(x_i) = n - \text{orb}(x_i)$ where $\text{orb}(x_i)$ is the number of g_i-orbits on the cosets of P. In characteristic 0, we can compute the genus g of $(P, x_1, ..., x_r)$ via the Riemann-Hurwitz formula

$$2(n + g - 1) = \sum_{i=1}^{r} ind(x_i).$$

By Riemann's existence theorem this group theoretic data comes from a genus g covering of the Riemann sphere with monodromy group G.

By minimal genus of G we mean the minimum genus taken over all $(P, x_1, ..., x_r)$. By the minimal composition factor genus of a nonabelian simple group S we shall mean the minimal genus of a group G such that $F^*(G) = S^t$ for some integer $t \geq 1$. Denote this by $\lambda(S)$. Let $\lambda'(S)$ denote the minimum of the minimal genus of all almost simple groups with socle S. By [GT] the minimal genus is realized on a primitive action.

In [GT] Guralnick and Thompson initiated a program to classify all primitive genus zero actions in characteristic 0 that are not of the type where $(F^*(G), F^*(P)) = (Alt_n, Alt_{n-1})$. As a first step we need to identify all pairs $(F^*(G), P)$ that can occur.

By a recent reduction theorem of Guralnick [G2] that is valid for all characteristics, it follows that one of the following occurs:

1. $\lambda(S) = \lambda'(S)$;
2. $\lambda(S) = \lambda'(S) - 1$; or
3. $\lambda(S) = 0$ and $\lambda'(S) = 2$.

Moreover, the reduction theorem indicates that in the last 2 cases, the minimal genus will be realized in an affine action. Since essentially all genus zero affine actions (in characteristic 0) have been classified [N], all possibilities in the last case can be analyzed. In the second case, the reduction theorem also gives more information. In all cases, knowing $\lambda'(S)$ tightly constrains the possibilities for $\lambda(S)$.

If $p = 0$, the sporadic groups and the exceptional groups of Lie type that occur as genus zero composition factors have been classified in [M] and [FM1] respectively. The alternating groups are being investigated by Guralnick and Shareshian to determine which actions are genus zero actions. By [FM] it is known that only finitely many classical groups can be genus zero composition factors. However the exact list is still unknown. The difficulty in eliminating classical groups from the list of possible genus zero composition factors lies in the amount of case analysis involved and in the asymptotic nature of the fixed point ratio estimates that go into the calculations. Our corollary shows that the minimal genus of a classical group is achieved on a restricted set of possible actions. In a subsequent paper we hope to restrict that set of actions further and show that with a very small number of exceptions, the minimal genus in

characteristic 0 is acheived on the action on totally singular 1-spaces (1-spaces in the linear case).

In positive characteristic, there is a more complicated version of the Riemann-Hurwitz formula (cf. [G2]). Fortunately, we will use a representation theoretic interpretation of the genus which allows to apply corollary 1.2.

Suppose that $\phi : X \to Y$ is a Galois cover with group of deck transformations G. Let J_X be the Jacobian of X and let $J_X[\ell]$ be the ℓ-torsion points of J_X. Note that J_X is a characteristic 0 module, even though k may have positive characteristic. The action of G induces an action on J_X and hence on $J_X[\ell]$. The following result is elementary and well known.

Lemma 8.1 [FV] *If ℓ is prime, $(\ell, |G|) = 1$, and P a subgroup of G then,*

$$2g(X/P) = \dim(J_X[\ell]^P).$$

Corollary 8.2 *If $P, K < G$, such that 1_P^G is a submodule of 1_K^G, then $g(X/P) \leq g(X/K)$.*

Proof By the lemma above

$$\begin{aligned} 2g(X/P) &= \dim(J_X[\ell]^P) \\ &= (J_X[\ell]|_P, 1_P) \\ &= (J_X[\ell], 1_P^G) \\ &\leq (J_X[\ell], 1_K^G) \\ &= (J_X[\ell], 1_K) \\ &= \dim(J_X[\ell]^K) \\ &= 2g(X/K). \end{aligned}$$

■

Note that if G acts primitively on a set of subspaces of V, then this action is equivalent to the action on a set of spaces that are either all totally singular or all nondegenerate, combining the corollary with corollary 1.2 yields corollary 1.3 except in the case where G is linear, induces a graph automorphism on the simple group, and the action is on flags of type $k, d-k$ or on pairs of complementary k, $d-k$-spaces. To handle this final case we argue as follows:

Lemma 8.3 *Let A be a finite group with G a subgroup of index 2. Let M be a maximal subgroup of A not contained in G such that $M \cap G$ is properly contained in a maximal subgroup U of G. Assume that M contains no normal subgroup of G and that U does not contain the derived subgroup of G. Suppose that $f : Z \to Y$ is a Galois branched cover of smooth projective curves with monodromy group A. Let $X = Z/M$, $X' = Z/U$, and $Y' = Z/G$.*

1. *If $g(Y') = 0$, then $g(X) \geq g(X')$.*

2. *If* $g(Y') = 1$, *then* $g(X) \geq \mathrm{ind}(s, G/U)/2$ *for some nontrivial* $s \in G$.

3. *If* $g(Y') > 1$, *then* $g(X) \geq |G : U| - 2$.

Proof. Let T be the ℓ-torsion module of the Jacobian of Z for some ℓ not dividing $|A|$.

Let $g \in M \setminus G$. Note that since $g^2 \in G \cap M \leq U \cap U^g$, g interchanges U and U^g. Since M does not contain U, $U \neq U^g$.

Thus, g interchanges $C_T(U)$ and $C_T(U^g)$ and the intersection of these two subspaces is the set of fixed points of $\langle U, U^g \rangle = G$. Thus, $\dim C_T(M) \geq \dim C_T(U) - \dim C_T(G)$ or equivalently, $g(X) \geq g(X') - g(Y')$. This proves the result when $g(Y') = 0$.

Suppose that $g(Y') > 1$. By the Riemann-Hurwitz formula, $g(X') - 1 \geq d(g(Y') - 1)$, where $d = |G : U|$. So $g(X) \geq (d-1)g(Y') - d \geq d - 2$, as required.

Finally consider the case that $g(Y') = 1$. Since U does not contain the derived subgroup of G, X' cannot be unramified over the elliptic curve Y'. Again, by the Riemann-Hurwitz formula, $g(X') - 1 \geq \mathrm{ind}(s, G/U)/2$ for some nontrivial element s of G. This completes the proof. ∎

The proof of the next result lemma requires characteristic 0 in the use of Riemann's existence theorem.

Lemma 8.4 *Let* G *be an almost simple group with socle* S *acting primitively on a set* Ω *of cardinality* d. *Let* s *be a nontrivial element of* G. *There exists a subgroup* G_1 *of* G *containing* S *and a* 3*-point branch cover of* $f : X \to \mathbb{P}^1_{\mathbb{C}}$ *of degree* d *with monodromy group* G_1 *so that* $g(X) \leq \mathrm{ind}(s)/2$.

Proof. By [GK], there exists $t \in S$ so that $G_1 := \langle s, t \rangle$ contains S. By Riemann's Existence Theorem, there exists a Galois cover $f : Z \to \mathbb{P}^1$ with Galois group G_1 with 3 branch points with inertia groups generated by s, t and $(st)^{-1}$. Let H be the stabilizer in G_1 of a point of Ω (note that G_1 is transitive on Ω since G is primitive). By the Riemann-Hurwitz formula, the genus of $X := Z/H$ satisfies $2(|G_1 : H| + g(X) - 1) = \mathrm{ind}(s) + \mathrm{ind}(t) + \mathrm{ind}((st)^{-1})$. Since $\mathrm{ind}(u) < |G_1 : H|$, this implies that $g(X) \leq \mathrm{ind}(s)/2$.

Applying lemmas 8.3 and 8.4 to the case that $F^*(A) = L_n(q)$, $G = A \cap \Gamma L_n(q)$ and $[A : G] = 2$, then (in characteristic 0) the genus on the stabilizer of a pair of subspaces of complementary dimensions is at least as great as the genus of the subgroup of index 2 on the corresponding parabolic (and so at least the genus on 1-spaces) unless the action is also primitive for the simple group. This completes the proof of corollary 1.3 in characteristic 0.

One can give a different argument based on fixed point ratios to show that (in the notation of lemma 8.3) we always have $g(X') \geq g(X)$. Thus corollary 1.3 holds in all characteristics. We will give the details of this argument elsewhere.

References

[A] Aschbacher M.: On conjectures of Guralnick and Thompson, *J. Algebra* 135 (1990) no. 2, 277-343.

[CR] Curtis, C. and Reiner, I, Methods of Representation Theory with Applications to Finite Groups and Orders, Vol. II, John Wiley & Sons, New York, 1987.

[FV] Fried, M. and Völklein, H.: Unramified abelian extensions of Galois covers, Proceedings of the Summer Research Institute on Theta Functions (Gunning and Ehrenpreis, editors), Proceedings of Symposia in Pure Mathematics **49** (1989)675-693.

[FM] Frohardt, D. and Magaard, K.: Composition factors of monodromy groups, *Annals Math.*, to appear.

[FM1] Frohardt, D. and Magaard, K.: Monodromy composition factors among exceptional groups of Lie type in *Group Theory, Proceedings of the Biennial Ohio State-Denison Conference*, 134-143(eds. Sehgal and Solomon), World Scientific, Singapore, 1993.

[G1] Guralnick, R.: The genus of a permutation group, in *Groups, Combinatorics and Geometry*, edited by M. Liebeck and J. Saxl, LMS Lecture Note Series 165, Cambridge University Press, London, 1992.

[G2] Guralnick, R.: Composition factors of monodromy groups of branched coverings of curves in all characteristics, preprint.

[GK] Guralnick, R. and Kantor, W. : Probabilistic generation of finite simple groups, *J. Algebra*, to appear.

[GLMS] Guralnick, R., Liebeck, M., Macpherson, D., Seitz, G. : Modules for algebraic groups with finitely many orbits on subspaces, *J. Algebra* 196, (1997), 211–250.

[GN] Guralnick, R. and Neubauer, M.: Monodromy groups of branched coverings: The generic case, in *Recent developments in the inverse Galois problem (Seattle, WA 1993) 325-352*, Comtemp. Math.,186, Amer. Math. Soc., Providence, RI, 1995.

[GT] Guralnick, R. and Thompson, J. Finite groups of genus zero, *J. Algebra*, **131** (1990) 303–341.

[LSh] Liebeck, M. and Shalev, A.: Simple groups, permutation groups and probability, *J. Amer. Math. Soc.***12**(1999),497-520.

[M] Magaard, K., Monodromy and sporadic groups, *Comm. Algebra*, 21(12), 4271-4297 (1993).

[N] Neubauer, M., On monodromy groups of fixed genus *J. Algebra* **153**(1992), 215–261.

[Sh] Shih, T., A note on groups of genus zero, *Comm. in Alg.* 19 no.10, (1991), 2813-2826.

Daniel Frohardt
Department of Mathematics
Wayne State University
Detroit, MI 48202
USA
email: danf@math.wayne.edu

Robert Guralnick
Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113
USA
email: guralnic@math.usc.edu

Kay Magaard
Department of Mathematics
Wayne State University
Detroit, MI 48202
USA
email: kaym@math.wayne.edu