Most Primitive Groups Have Messy Invariants

W. C. HUFFMAN*

Department of Mathematics, Loyola University, Chicago, Ill. 60626

AND

N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey 07974

Suppose $G$ is a finite group of complex $n \times n$ matrices, and let $R^G$ be the ring of invariants of $G$: i.e., those polynomials fixed by $G$. Many authors, from Klein to the present day, have described $R^G$ by writing it as a direct sum $\sum_{i=1}^{\delta} \eta_i \mathbb{C}[\theta_1, \ldots, \theta_n]$. For example, if $G$ is a unitary group generated by reflections, $\delta = 1$. In this note we show that in general this approach is hopeless by proving that, for any $\epsilon > 0$, the smallest possible $\delta$ is greater than $|G|^{n-1-\epsilon}$ for almost all primitive groups. Since for any group we can choose $\delta \leq |G|^{n-1}$, this means that most primitive groups are about as bad as they can be. The upper bound on $\delta$ follows from Dade's theorem that the $\theta_i$ can be chosen to have degrees dividing $|G|$.

Let $G$ be a finite group of complex $n \times n$ matrices. If $f(x_1, \ldots, x_n)$ is a polynomial in $x_1, \ldots, x_n$ with complex coefficients, and $A = (a_{ij})$ is an element of $G$, then $Af(x_1, \ldots, x_n) = f(\sum a_{ij}x_j, \ldots, \sum a_{nj}x_j)$ is the polynomial obtained by letting $A$ act as a linear transformation on the variables $x_1, \ldots, x_n$. The ring $R^G$ of invariants of $G$ consists of all polynomials $f$ with $Af = f$ for all $A \in G$. The central problem is to find a description of $R^G$ that is concise and easy to use. Several types of bases for $R^G$ have been considered ([4, Ch. XVII], [32]), but we are concerned here with finding a direct sum decomposition

$$R^G = \sum_{j=1}^{\delta} \eta_j \mathbb{C}[\theta_1, \ldots, \theta_n],$$

where $\theta_1, \ldots, \theta_n$ are algebraically independent homogeneous invariants and $\eta_1 = 1$, $\eta_2, \ldots, \eta_\delta$ are certain other homogeneous invariants. It is known from the theory of Cohen-Macaulay rings ([15, Prop. 13]) that $R^G$ always has a direct sum decomposition (1). Then $R^G$ is a finitely generated free $\mathbb{C}[\theta_1, \ldots, \theta_n]$-module of rank $\delta$. We are interested in the smallest value of $\delta$ that can be attained by any choice of $\theta_1, \ldots, \theta_n$; call this value $\delta(G)$. We shall give examples to show that $\delta(G)$ may

* Work done while at Union College, Schenectady, N.Y. 12308.
be large, and then show that for most primitive groups $\delta(G)$ is about as large as it can be.

In [33, Section 3.4.12] T. A. Springer has proved a somewhat similar result for the ring of invariants of binary forms of given degree.

The $\theta_i$ and $\eta_i$ in (1) form a polynomial basis for $R^G$. In the past century polynomial bases have been given for a number of groups ([1], [10], [13], [16], [21], [23]–[25], [27], [30]–[38]). E. Noether had shown in 1916 ([29]; see also [32], [42]) that any group has a polynomial basis containing no more than $(\binom{n}{2} + n)$ invariants, i.e. about $|G|^n/n!$ for large $|G|$. We had always thought that this was a very weak bound (cf. also [13]), but in fact it is not far off, at least for primitive groups.

We make use of the Molien series of $G$, i.e. the generating function

$$\Phi_G(\lambda) = \sum_{j=0}^{\infty} \dim C(R^G)_j \lambda^j,$$

in which the coefficient of $\lambda^j$ is the number of linearly independent homogeneous invariants of degree $j$. Molien ([28]; see also [4], [27], [32]) showed that the series can be calculated from the identity

$$\Phi_G(\lambda) = \frac{1}{|G|!} \sum_{\lambda \in G} \frac{1}{\det(I - \lambda A)},$$

(2)

If $R^G$ has the decomposition (1) then the Molien series may be written as

$$\Phi_G(\lambda) = \frac{\sum^j \lambda^{e_j}}{(1 - \lambda d_1)(1 - \lambda d_2) \cdots (1 - \lambda d_n)},$$

(3)

where

$$\deg \eta_j = e_j, \quad \deg \theta_j = d_j.$$

**Theorem 1.**

$$\delta = \frac{d_1d_2 \cdots d_n}{|G|}$$

(4)

**Proof.** If we equate (2) and (3), multiply by $(1 - \lambda)^n$, and let $\lambda \to 1$ we obtain $1/|G| = \delta/d_1 \cdots d_n$.

**Example 1.** If $G$ is a finite unitary group generated by reflections then $R^G$ is a free ring and may be expressed in the form (1) with $\delta(G) = 1$ and $d_1d_2 \cdots d_n = |G|$ (Shephard and Todd [30]; see also [5]).

The next two examples are six-dimensional groups from Lindsey's list [22].

**Example 2.** Let $G$ be a six-dimensional representation of a nonsplitting
central extension of $\mathbb{Z}_3$ by the alternating group $\mathbb{A}_6$, of order $3 \cdot 360$. This group is of interest because it is generated by matrices with two eigenvalues $-1$ and the rest $1$. Such groups are a natural generalization of the class of groups given in Example 1, ([18], [41]). We shall see that $\delta(G) \geq 54$, which suggests that the invariants of these groups do not have such a simple description as those of Example 1.

The Molien series may be calculated from (2), and when written in simplest terms (with numerator and denominator relatively prime) is equal to

$$\Phi^{(1)}(\lambda) = \frac{f_1(\lambda)}{\phi_1 \phi_2 \phi_3 \phi_4 \phi_5 \phi_6 \phi_{12} \phi_{15}}$$

where

$$f_1(\lambda) = 1 - \lambda^3 + 3 \lambda^6 + \lambda^9 + 4 \lambda^{12} + 3 \lambda^{15} + 5 \lambda^{18} + 3 \lambda^{21} + 4 \lambda^{24} + \lambda^{27} + 3 \lambda^{30} - \lambda^{33} + \lambda^{36},$$

and $\phi_r(\lambda)$ is the $r$-th cyclotomic polynomial. The numerator of (5) (and of (6)-(10) below) is a symmetric polynomial: this is an easy consequence of the fact that all the group elements have determinant one. The Taylor series expansion of the Molien series is

$$1 + 2\lambda^3 + 7\lambda^6 + 16\lambda^9 + 38\lambda^{12} + 76\lambda^{15} + 146\lambda^{18} + \cdots$$

To obtain a lower bound on $\delta(G)$ we make use of Theorem 1. Let the Molien series be written in the form

$$\Phi^{(6)}(\lambda) = \frac{f_3(\lambda)}{(1 - \lambda D_1)(1 - \lambda D_2) \cdots (1 - \lambda D_6)}$$

where $f_3(\lambda)$ has nonnegative coefficients and the product $D_1D_2 \cdots D_6$ is a minimum. From Theorem 1,

$$\delta(G) \geq \delta_1(G) = \frac{D_1D_2 \cdots D_6}{|G|}.$$
such that the product of the \( j \)-th set divides \( 1 - \lambda^{D_j} \). (Thus the \( \phi_i \)'s in each set are distinct.) Let

\[ F_j = \text{l.c.m.}(t_{j1}, ..., t_{jr_j}). \]

Then the product of the \( j \)-th set of \( \phi_i \)'s divides \( 1 - \lambda^{F_j} \), \( F_j \) divides \( D_j \), and

\[ \delta_j(G) = \frac{D_1 \cdots D_6}{|G|} \geq \frac{F_1 \cdots F_6}{|G|}. \]

Consequently, if we multiply the numerator and denominator of \( \Phi^{(1)}(\lambda) \) by

\[ \rho_{12}(\lambda) = \frac{1 - \lambda^{F_1}}{\phi_{t_{11}} \cdots \phi_{t_{1r_1}}} \cdots \frac{1 - \lambda^{F_6}}{\phi_{t_{61}} \cdots \phi_{t_{6r_6}}}, \]

we obtain

\[ \Phi^{(2)}(\lambda) = \frac{f_2(\lambda)}{(1 - \lambda^{F_1}) \cdots (1 - \lambda^{F_6})}, \]

which is a form of the Molien series intermediate between \( \Phi^{(1)}(\lambda) \) and \( \Phi^{(3)}(\lambda) \). Then \( \Phi^{(3)}(\lambda) \) is obtained by multiplying the numerator and denominator of \( \Phi^{(2)}(\lambda) \) by

\[ \rho_{23}(\lambda) = \frac{1 - \lambda^{D_1}}{1 - \lambda^{F_1}} \cdots \frac{1 - \lambda^{D_6}}{1 - \lambda^{F_6}}. \]

In the present example it is not difficult to see that only three partitions of the \( \phi_i \)'s need be considered, namely:

(I) \[ \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_6 \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_4, \phi_6, \phi_{12} \}, \]
\[ \{ \phi_1, \phi_3, \phi_6, \phi_{15} \}, \]

with

\[ F_1 = F_2 = F_3 = 3, \quad F_4 = 6, \quad F_5 = 12, \quad F_6 = 15. \]

(II) \[ \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_4, \phi_6, \phi_{12} \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_6, \phi_{15} \}, \]

with

\[ F_1 = F_2 = F_3 = F_4 = 3, \quad F_5 = 12, \quad F_6 = 30. \]

(III) \[ \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \{ \phi_1, \phi_3 \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_6 \}, \]
\[ \{ \phi_1, \phi_2, \phi_3, \phi_4, \phi_6, \phi_{12}, \phi_{15} \}, \]

with

\[ F_1 = F_2 = F_3 = F_4 = 3, \quad F_5 = 6, \quad F_6 = 60. \]
Suppose partition (I) occurs. Then
\[ \Phi^{(2)}(\lambda) = \Phi^{(1)}(\lambda) \]
\[ = \frac{1 - \lambda^3 + 2\lambda^6 + \cdots + \lambda^{36}}{(1 - \lambda^3)(1 - \lambda^9)(1 - \lambda^{12})(1 - \lambda^{15})}, \]
and \( \rho_{12}(\lambda) = 1 \). Since the numerator of \( \Phi^{(2)}(\lambda) \) contains a negative coefficient, \( \rho_{21}(\lambda) \neq 1 \). If we take \( \rho_{23}(\lambda) = 1 + \lambda^3 \), we obtain
\[ \Phi^{(3)}(\lambda) = \frac{1 + 2\lambda^3 + 4\lambda^6 + 5\lambda^{12} + \cdots + \lambda^{20}}{(1 - \lambda^3)^2(1 - \lambda^6)(1 - \lambda^{12})(1 - \lambda^{15})}, \]
with nonnegative coefficients in the numerator, and \( D_1 \cdots D_6 = 3^3 \cdot 6^3 \cdot 12 \cdot 15 = 58320 \). Any other choice of \( \rho_{23}(\lambda) \) will give a larger value of \( D_1 \cdots D_6 \).

Suppose instead that partition (II) occurs. Now
\[ \rho_{12}(\lambda) = \phi_{10}\phi_{30} \]
and
\[ \Phi^{(2)}(\lambda) = \frac{1 - 2\lambda^3 + \cdots + \lambda^{48}}{(1 - \lambda^3)^4(1 - \lambda^{12})(1 - \lambda^{20})}. \]
Again \( \rho_{23}(\lambda) \neq 1 \), and so \( D_1 \cdots D_6 \geq 58320 \). Similarly for partition (III). We conclude that the minimum value of \( D_1 \cdots D_6 \) is 58320, and therefore
\[ \delta(G) \geq \delta_1(G) = \frac{58320}{3 \cdot 360} = 54. \]

**Example 3.** In this example we consider a member of another important class of groups, a six-dimensional representation of \( SL_2(13) \) of order 2184 \(([9], \text{Section 381})\). Using the method described in Example 2 (there are now 29 partitions to be considered) we find that the Molien series when written with minimum \( D_1 \cdots D_6 \) is
\[ \Phi^{(3)}(\lambda) = \frac{1 + \lambda^{10} + 5\lambda^{12} + 6\lambda^{14} + 12\lambda^{16} + 18\lambda^{18} + 25\lambda^{20} + \cdots + \lambda^{70}}{(1 - \lambda^4)(1 - \lambda^9)(1 - \lambda^{12})(1 - \lambda^{15})} = 1 + \lambda^4 + 2\lambda^8 + \lambda^{10} + 9\lambda^{12} + 8\lambda^{14} + 22\lambda^{16} + 27\lambda^{18} + 54\lambda^{20} + \cdots \]
Consequently
\[ \delta(G) \geq \delta_1(G) - 768. \]

**Example 4.** Let \( G \) be the 24-dimensional representation of the Conway group .0, of order 8315553613086720000 \(([6])\). The Molien series is
\[ \Phi_{.0}(\lambda) = \rho(\lambda)/q(\lambda), \]
MOST PRIMITIVE GROUPS HAVE MESSY INVARIANTS

\[ p(\lambda) = 1 + \lambda^{12} + \lambda^{26} + 2\lambda^{38} + \lambda^{50} + \lambda^{52} + 3\lambda^{34} + \cdots + 401078\lambda^{100} + \cdots + \lambda^{916} \]

and

\[ q(\lambda) = (1 - \lambda^2)(1 - \lambda^{16})(1 - \lambda^{18})(1 - \lambda^{20})(1 - \lambda^{22})(1 - \lambda^{24})(1 - \lambda^{30})^2 \\
\cdot (1 - \lambda^{32})^2(1 - \lambda^{36})^2(1 - \lambda^{40})(1 - \lambda^{42})(1 - \lambda^{48})(1 - \lambda^{52})(1 - \lambda^{56}) \\
\cdot (1 - \lambda^{60})(1 - \lambda^{62})(1 - \lambda^{70})(1 - \lambda^{78})(1 - \lambda^{84}), \text{ of degree } 940. \]

Thus

\[ \Phi_{\ast}(\lambda) = \frac{1}{1 - \lambda^2} (1 + \lambda^{12} + \lambda^{16} + \lambda^{18} + \lambda^{30} + \lambda^{32} + 3\lambda^{34} + \lambda^{26} + 3\lambda^{28} + 4\lambda^{30} + 5\lambda^{32} + 5\lambda^{34} + 10\lambda^{36} + 8\lambda^{38} + 14\lambda^{40} + 17\lambda^{42} + 22\lambda^{44} + 27\lambda^{46} + 44\lambda^{48} + 45\lambda^{50} + \cdots) \]

We have not attempted to minimize \( D_1 \cdots D_{24} \) in this example. However, if (10) is the minimum—and our experience suggests it should be close to the minimum then \( \delta(G) \geq \delta_1(G) = D_1 \cdots D_{24}/|G| \approx 205679393714995200. \)

**Example 5.** The direct product \( \mathcal{P}_2 \times Z_m \) of the symmetric group of order 6 with a cyclic group of order \( m \), where \( m \) is prime to 6, has a two-dimensional representation \([43, II, p. 394]\) for which \( S(G) = m \).

These examples illustrate the fact that in general \( S(G) \) is large. We now give our bounds on \( S(G) \). The upper bound is a consequence of the following (unpublished) theorem of Dade, which we include with his permission.

Let \( R = \mathbb{Q}[x_1, \ldots, x_n] \). A sequence \( \theta_1, \ldots, \theta_n \) in \( R \) is called an \( R \)-sequence ([20, p. 84], [43, II, p. 394]) if the image of \( \theta_{k+1} \) is neither a unit nor a zero-divisor in \( R/(R\theta_1 + \cdots + R\theta_k) \), for \( 0 \leq k < n \).

**Theorem 2** (Dade [7]). With \( G \) as above, there exists an \( R \)-sequence \( \theta_1, \ldots, \theta_n \) such that each \( \theta_i \) is a homogeneous invariant in \( R^G \) of degree dividing \( |G| \).

**Remark.** Once such an \( R \)-sequence has been found it is straightforward to show that there are further invariants \( \eta_1, \ldots, \eta_n \) such that (1) holds (see for example [35]).

**Proof.** Let \( R_1 \) consist of the homogeneous linear polynomials in \( R \). Choose any non-zero \( f_1 \in R_1 \), and let \( f_{11} = f_1, f_{12}, \ldots, f_{1v_1} \) be the distinct images of \( f_1 \) under \( G \). Set

\[ \theta_i = \prod_{j=1}^{v_1} f_{ij}, \]
Suppose \( \theta_1, \ldots, \theta_i \ (1 \leq i < n) \) have been found. Choose \( f_{i+1} \in R_i \) such that
\[
f_{i+1} \text{ is not in the prime ideal } (f_{i+1}, f_{i+2}, \ldots, f_{i+i}) \tag{11}
\]
for all \( 1 \leq c_1 \leq a_1, \ldots, 1 \leq c_i \leq a_i \). (Since there are only finitely many of these ideals, and each intersects \( R_i \) in a vector space of dimension \( i < n \), such an \( f_{i+1} \) can always be found.) Let \( f_{i+1,1} = f_{i+1}, f_{i+1,2}, \ldots, f_{i+1,a_{i+1}} \) be the distinct images of \( f_{i+1} \) under \( G \), and set
\[
\theta_{i+1} = \prod_{j=1}^{a_{i+1}} f_{i+1,j}.
\]
The construction implies that \( f_{i+1,j} \) is not in the ideal (11) for all \( 1 \leq c_1 \leq a_1, \ldots, 1 \leq c_i \leq a_i \). Repeat until \( \theta_1, \ldots, \theta_n \) have been obtained. Clearly the \( \theta_j \) are homogeneous invariants of degrees dividing \( |G| \).

**Corollary**

\[
\delta(G) \leq |G|^{-1}. 
\]

**Proof.** Immediate from Theorems 1 and 2.

**Theorem 3.** Let \( n \) be fixed, and let \( \mathcal{C} \) be an infinite family of finite, inequivalent, \( n \times n \) complex groups that satisfies

- (A1) every element of \( \mathcal{C} \) is irreducible, and
- (A2) there are finitely many abstract groups \( H_1, \ldots, H_n \) such that if \( G \in \mathcal{C} \) then \( G/Z(G) \cong H_k \) for some \( k \), where \( Z(G) \) is the center of \( G \).

Then for any fixed \( \varepsilon > 0 \),
\[
\begin{align*}
\frac{\delta(G)}{|G|^{n-1-\varepsilon}} &\to \infty \quad \text{as} \quad |G| \to \infty \\
\end{align*}
\]
and so \( \delta(G) \geq |G|^{n-1-\varepsilon} \) for almost all \( G \in \mathcal{C} \).

**Proof.** For \( G \in \mathcal{C} \) let \( Z(G) \) have order \( m \). Then by [11, Theorem 1.4], \( Z(G) = \{\omega^j : 0 \leq j < m\} \), where \( \omega = e^{2\pi i/m} \). Suppose \( G/Z(G) \cong H_k \). Then \( |G| = m \cdot |H_k| \leq mh \), where \( h = \max|H_1, \ldots, |H_n|\). The degree of any homogeneous invariant of \( G \) must be divisible by \( m \), so in (4) each \( d_j \geq m \). Then
\[
\begin{align*}
\frac{\delta(G)}{|G|^{n-1-\varepsilon}} &= \frac{d_1 \cdots d_n}{|G|^{n-\varepsilon}} \geq \frac{m^n}{(mh)^{n-\varepsilon}} = \frac{m^n}{h^{n-\varepsilon}}.
\end{align*}
\]
As \( |G| \to \infty \) we must have \( |Z(G)| = m \to \infty \) (since there are only finitely many \( H_k \)'s), which proves (8) and the theorem.

Let \( G \) be an irreducible finite group of \( n \times n \) matrices acting on a complex \( n \)-dimensional vector space \( V \). Then \( G \) is \textit{imprimitive} if \( V \) is a direct sum of vector spaces:

\[
V = V_1 \oplus \cdots \oplus V_m
\]

where \( m \geq 2 \), each \( V_i \neq 0 \), and for all \( A \in G \) and all \( i \), \( A(V_i) = V_j \) for some \( j = j(A, i) \). Otherwise \( G \) is \textit{primitive}. \( G \) is \textit{quasiprimitive} if for any normal subgroup \( N \) of \( G \), \( V \) is a direct sum (14) where the \( V_i \) are invariant under \( N \) and afford equivalent representations of \( N \). By Clifford's theorem ([8], [9], [14]) a primitive group is quasiprimitive. In the classification of linear groups it is customary to restrict attention to primitive or quasiprimitive groups ([1], [2], [12], [16], [18], [27], [40]) since imprimitive groups are induced from a representation of smaller degree of a proper subgroup (cf. [9, Th. 14.1 (4)]).

**Theorem 4.** The conclusion of Theorem 3 applies to the family of inequivalent \( n \times n \) primitive groups or quasiprimitive groups.

**Proof.** Suppose \( G \) is quasiprimitive, and let \( H \) be any abelian normal subgroup of \( G \). By hypothesis \( V \) is the direct sum of one-dimensional subspaces that are invariant under \( H \), and the elements of \( H \) can be taken to be scalar matrices. Hence \( H \subset Z(G) \). Therefore by Jordan's theorem ([1], [9]), \( |G/Z(G)| \) is bounded, and so (A2) holds, proving the theorem.

**Remark.** It seems likely that a similar result will hold for the class of all \( n \times n \) groups, or all \( n \times n \) irreducible groups. The conclusion will not be as strong, however, since for any \( n \geq 2 \) there is an infinite family of irreducible imprimitive unitary groups generated by reflections with \( \delta(G) = 1 \) (the groups \( G(m, p, n) \) in [30]).

**Acknowledgments**

We thank J. H. Conway for providing the data used to calculate the Molien series of his group, E. C. Dade for permission to include his theorem, and R. L. Graham, C. L. Mallows and R. P. Stanley for helpful discussions. Some of the computations were carried out on the ALTRAN and MACSYMA systems ([3], [26]).

**References**