Degree Bounds in the Nonmodular Case Invariant Theory

Moise Mouyebe
Advisor: Harm Derksen

Abstract

This paper is the sequel of the work done last year at the University of Michigan during the REU program and whose report can be found in [6]. First, We will present the degree bound problem and survey some relevant background results. Then, we discuss the geometry of subspace arrangements constructed via the regular representation of the underlying group as a possible solution to the problem, and we address some of the issues encountered along the way. Finally, we present our main result.

1 Intoduction

Given a field K and a group representation $\rho : G \longrightarrow \mathrm{GL}(V)$ of a group G on a finite dimensional vector space V, we can extend the linear action of G on V to a linear action on the K-algebra $K[V]$ of polynomial functions on V called the coordinate ring of V. Invariant theory is concerned with the following subalgebra of $K[V]$ called the *invariant ring* of G:

$$K[V]^G := \{f \in K[V] \mid gf = f \quad \forall g \in G\}$$

where, $gf(v) = f(\rho(g)^{-1}v), \forall g \in G, v \in V$, and $f \in K[V]$.

We say we are in the *nonmodular case* invariant theory when the order of the group G is invertible in the ground field K. For instance, such case arises when the ground field K is an extension of the field of rational numbers $\mathbb{Q}$. Of special interest in invariant theory research are the following three questions: First, does the ring $K[V]$ have a finite algebra generating set? Second, *can we find priori bounds on the degrees of a minimal algebra generating set of* $K[V]^G$? Finally, Can we design *"good"* algorithms to compute systems of algebra generators for the ring of invariants?

The first question is closely related to D. Hilbert's 14th problem (see [3]). Meanwhile, the second question is in essence the *Degree Bound Problem.*

One of the foundational work done to address this problem was by the prominent German mathematician E. Noether. For instance, in 1916 she showed [8] that if the group G is finite then the invariant ring $K[V]^G$ is finitely generated as an algebra over the field K. Meaning, we can always find finitely many invariants $f_1, ..., f_s$ such that $K[V]^G = K[f_1, ..., f_s]$.

We can now introduce the number $\beta(\rho) := \max\{\deg(f_i), 1 \leq i \leq s\}$, where $\{f_1, .., f_s\}$ is a minimal algebra generating set for $K[V]^G$. Hence, the *Degree Bound Problem* can simply be reformulated as: *Find bounds for* $\beta(\rho)$. Another important result in positive characteristic [8] by E. Noether known as the *Noether's Bound* stipulates that the ring of invariants $K[V]^G$ is generated by invariants of degree at most $|G|$. Meaning, we always have $\beta(\rho) \leq |G|$.

Noether's bound justifies the definition of the following number:

$$\beta(G) := \max\{\beta(\rho) \mid \rho \text{ finite dimensional representation of } G\}.$$

Example 1.1. *Let D_n be the group of symmetry of the regular polygon with n vertices, and let ρ be its two dimensional representation given by the matrices:*

$$\rho(r) = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \text{ and } \rho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The ring of invariants $\mathbb{R}[x, y]^{D_n}$ is generated as an $\mathbb{R}$-algebra by the homogeneous invariant polynomials $x^2 + y^2$ and $\prod_{i=0}^{n-1}(\cos(\frac{2\pi i}{n})x + \sin(\frac{2\pi i}{n})y)$. Hence, we have $\beta(\rho) = n$. However, we have:

$$\beta(D_n) = n + 1.$$

Example 1.2. *Let A_n be the alternating group on $n \geq 2$ symbols, and let $\rho : A_n \longrightarrow \mathrm{GL}(n, \mathbb{C})$ be its n-dimensional defining representation. One can verify that all the n symmetric functions $e_1, ...e_n$ are invariant under the action of the group A_n. Furthermore, the polynomial $\Delta_n = \prod_{1 \leq i \leq j}(x_i - x_j)$ of degree $\binom{n}{2}$ called the* Vandermonde determinant *is also invariant under the action of the group A_n. In fact, we have $\mathbb{C}[x_1, ...x_n]^{A_n} = \mathbb{C}[e_1, ..., e_n, \Delta_n]$. Hence, $\beta(\rho) = \binom{n}{2}$. This gives the following lower bound for $\beta(A_n)$:*

$$\beta(A_n) \geq \binom{n}{2}$$

2 Survey of Some Results

Noether's bound $\beta(\rho) \leq |G|$ is one of the fundamental results for the degree bound problem. In fact, it is now well established that the equality only holds when the group G is *cyclic*. The proof [11] of this statement is encoded in the following theorem:

Theorem 2.1. *Let $\rho : G \longrightarrow \mathrm{GL}(V)$ be a finite dimensional representation of a finite and non-cyclic group G. Then, the ring of invariants $K[V]^G$ is generated by the homogeneous invariants of degree strictly less than $|G|$. That means we have $\beta(\rho) < |G|$.*

Using Weyl's theorem, B.Schmid [11] was able to establish that $\beta(G) = \beta(\rho_{reg})$, where ρ_{reg} represents the regular of the group G. It turns out that this result is very useful in practice when computing $\beta(G)$ explicitly. Furthermore, combining this result with Noether's bound we deduce that the regular representation ρ_{reg} of the group G realizes the worst case analysis in solving the degree bound problem. Meaning that if we can find bounds for the regular representation of G, we can be confident that we have found bounds for any representation of G; at least in the nonmodular case.

Definition 2.2. *Let $b_1, ..., b_s$ be nonzero elements of a group G (written additively). The equation $b_1 + ... + b_s = 0$ is said to be non-shortable if it has the property that for every nonempty strict subset $\{i_1, ..., i_s\} \subsetneq \{1, ...s\}$, we have $b_{i_1} + ... + b_{i_s} \neq 0$.*

Theorem 2.3 (B.Schmid)**.** *Let G be a finite abelian group, then $\beta(G)$ equals the maximal length of a non-shortable equation in G.*

Example 2.4. *In $\mathbb{Z}_3$ the equation $1+1+1=0$ is non-shortable. However, any equation $b_1+b_2+b_3+b_4=0$, where $b_i \in \{1,2\}$ is shortable.This is why: At least one of the b_i's, let's call it b_r must equal 1. Otherwise, the sum of b_i's will fail to be zero. Likewise, at least one of the b_i's, let's say b_s must equal 2. We then have $b_r+b_s=0$, and the result follows. A similar argument can be used to check that the maximal length of a non-shortable equation in $\mathbb{Z}_3$ is actually 3. Hence, by Theorem 2.4 we must have $\beta(\mathbb{Z}_3) = 3$. This result was predictable since $\mathbb{Z}_3$ is cyclic.*

In $\mathbb{Z}_3 \times \mathbb{Z}_3$, the equation $(0,1)+(0,1)+(1,0)+(1,0)+(1,1)=(0,0)$ is non-shortable. In fact, we have $\beta(\mathbb{Z}_3 \times \mathbb{Z}_3) = 5$. This is consistent with Theorem 2.1.

We want to conclude this paragraph with some of the classical results known. The proof of some of those can be found in [11].

Proposition 2.5. *We have the following:*

1. *If G is the dihedral group D_n of order $2n$ then $\beta(D_n) = n + 1$.*
2. *If $G = \mathbb{Z}_{p^{r_1}} \times ... \times \mathbb{Z}_{p^{r_s}}$, where p is a prime number then we have $\beta(G) = 1 + \sum_{i=1}^{s}(p^{r_i} - 1)$.*
3. *$\beta(S_2) = 2$, $\beta(A_3) = 3$, $\beta(S_3) = 4$ $\beta(A_4) = 6$, and $\beta(S_4) = 10$.*

3 Subspace Arrangements Explored

In [6] we introduced the geometric argument of subspace arrangements as a possible way to address the degree bound problem. More specifically, we focused on the variety

$$B := \bigcup_{g \in G} g\Delta(V)$$

where V is a finite dimensional K-vector space, and $\Delta : V \longrightarrow V \times V$ is the diagonal morphism. Moreover, the action of the group G on $V \times V$ is defined by $g(v, v) = (v, gv)$.

The following two theorems were the motivation to start thinking about the degree bound problem from a geometric stand point, because together they translate the degree bound problem from the ring of invariants $K[V]^G$ to a degree bound problem on the ideal $\mathcal{I}(B)$ of the variety B.

Theorem 3.1 (H. Derksen)**.** *Let I be the ideal of $K[V]$ generated by all homogeneous invariants of positive degree. We can further reasonably assume that $I = (h_1, ..., h_s)$ where all the h_i, $1 \leq i \leq s$ are homogeneous, then $K[V]^G = K[\mathcal{R}(h_1), ..., \mathcal{R}(h_s)]$, where $\mathcal{R}$ is the averaging Reynolds operator defined by:*

$$\begin{aligned} \mathcal{R} \colon K[V] &\longrightarrow K[V]^G \\ h &\longmapsto \frac{1}{|G|} \sum_{g \in G} gh. \end{aligned}$$

Theorem 3.2. *Suppose the ideal $\mathcal{I}(B) \subset K[V \oplus V]$ of the variety B is generated by the homogeneous polynomials $f_1(x, y), ..., f_r(x, y)$, then the ideal I in Derksen's theorem is given by $I = (f_1(x, 0), ..., f_r(x, 0))$.*

We presented a simple geometric intuition that lead us to define the following alpha number:

$$\alpha(\rho_{reg}) := \max \{\sharp(\mathcal{L} \cap B_{reg}) \mid \mathcal{L} \text{ affine line in } V \oplus V \text{ such that } \mathcal{L} \nsubseteq B_{reg}\}$$

where ρ_{reg} is the regular representation of G, B_{reg} is the subspace arrangement associated with ρ_{reg}, and $\sharp(\mathcal{L} \cap B_{reg})$ stands for the number of point of intersection between $\mathcal{L}$ and B_{reg}. We had the following proposition that we hoped would give us a lower bound for $\beta(G)$:

Proposition 3.3. $\beta(\rho_{reg}) \geq \alpha(\rho_{reg})$.

One of our goals this year was to examine how *good* of a lower bound $\alpha(\rho_{reg})$ could be. So, we decided to investigate this question through explicit examples whose $\beta(\rho_{reg})$ are known.

For instance, it turns out that the argument works well for $\mathbb{Z}_2 \times \mathbb{Z}_2$ as the computation carry in [6] show. In this case we got a lower bound of 3 which is very good considering that $\beta(\mathbb{Z}_2 \times \mathbb{Z}_2) = 3$. However, the argument doesn't work that well for $\mathbb{Z}_3 \times \mathbb{Z}_3$ where we failed to even get a lower bound of 4 considering that $\beta(\mathbb{Z}_3 \times \mathbb{Z}_3) = 5$.

It is important to mention that the computation involved to calculate the lower bound given by the alpha number can quickly become intractable as the group order increases. For example, in the $\mathbb{Z}_3 \times \mathbb{Z}_3$ case we worked with the following representation which is equivalent to its regular representation and is afforded by the matrices:

$$\rho(\sigma) = [e_1\ e_2\ e_3\ \zeta e_4\ \zeta e_5\ \zeta e_6\ \zeta^2 e_7\ \zeta^2 e_8\ \zeta^2 e_9] \in GL(9, \mathbb{C})$$

and

$$\rho(\tau) = [e_1\ \zeta e_2\ \zeta^2 e_3\ e_4\ \zeta e_5\ \zeta^2 e_6\ e_7\ \zeta e_8\ \zeta^2 e_9] \in GL(9, \mathbb{C})$$

where e_k represents the k-th standard vector of $\mathbb{C}^9$ for $1 \leq k \leq 9$, σ and τ are the group generators, and ζ represents the primitive 3^{rd} root of unity. That is ζ satisfies the equation: $\zeta^2 + \zeta + 1 = 0$.

Aiming for a lower of 4 simply means intersecting the affine line in $\mathbb{C}^{18}$ given by $\mathcal{L}(t) = (a_1 + tb_1, ..., a_{18} + tb_{18})$ with 4 distinct subspaces in the variety B. This amounts to solving $\binom{9}{4} = 126$ systems of $9 \cdot 4 = 36$ non-linear equations in $18 + 18 + 4 + 1 = 41$ unknowns. The equations can be made linear by *fixing* a value for ζ. In that case the number of unknowns decreases by 1. In either case, we were not successful in finding *non-trivial solutions*!

4 The Symmetric Group S_n

After wresting for some time with the computation outlined at the end of the preceding paragraph, we decided to try something different. So, we shifted

our attention to the symmetric group in n symbols S_n. Before we can state the main result, let us recall some background in representation theory.

1. If V and W are two representations of a group G, then we have
$$Hom(V,W)^G \cong (V^* \otimes W)^G$$
.

2. If V is irreducible, and $W = V_1^{d_1} \oplus ... \oplus V_r^{d_r}$, where V_i is irreducible for $1 \leq i \leq r$, then a corollary of Schur's lemma implies that $Hom(V,W)^G \neq 0$ if and only if $V \cong V_i$, for some i.

Combining the two points above, we deduce that:

$$\mathbb{C}[V \oplus W]^G_{d,1} \neq \{0\} \text{ if and only if } W \subset \mathbb{C}[V]_d$$

where $\mathbb{C}[V \oplus W]_{d,1}$ is the subspace of homogeneous polynomials of multidegree $(d,1)$ in the bigraded ring $\mathbb{C}[V \oplus W]$.

Lemma 4.1. *Let V be the standard representation of the symmetric group S_n, and let W be its sign representation. The following holds:*

$$W \subset \mathbb{C}[V]_d \text{ implies } d \geq \binom{n}{2}.$$

Proof. Suppose $0 \neq f \in W \subset \mathbb{C}[V]_d$, and let σ be the transposition (i,j) with $i < j$. Then we have $\sigma f = f(X_1, ..., X_j, ...X_i, ..., X_n) = -f(X_1, ..., X_i, ...X_j, ..., X_n)$. This implies that $X_i - X_j$ divides f. Since the polynomial $X_i - X_i$ is irreducible, and the pair (i,j) was chosen arbitrarily, we can therefore conclude that $\prod_{i<j}(X_i - X_j)$ divides f. Hence, $deg(f) = d \geq \binom{n}{2}$.

□

Proposition 4.2. $\beta(S_n) \geq 1 + \binom{n}{2}$.

Proof. Consider the polynomial $f = \prod_{i<j}(X_i - X_j)Y \in \mathbb{C}[V \oplus W]^{S_n}_{\binom{n}{2},1}$, and suppose that there exists a polynomial P and invariants f_i, $1 \leq i \leq r$ such that $f = P(f_1, ...f_r)$, where multideg$(f_i) < 1 + \binom{n}{2}$ for all i. We can write $f = \sum_{i=1}^r (g_i h_i)$, where g_i and h_i are non-constant polynomials and multideg(g_i) + multideg$(h_i) = (\binom{n}{2}, 1)$. It is clear that one of the g_i's or h_i's must have multidegree $(e,1)$ for some integer $e < \binom{n}{2}$. Let's call it g_s. We then have: multideg$(g_s) = (e,1)$ and multideg$(h_s) = (\binom{n}{2} - e, 0)$. However, since $0 \neq g_s \in \mathbb{C}[V \oplus W]^{S_n}_{e,1}$, Schur's lemma implies that $W \subset \mathbb{C}[\mathbb{V}]$. Thus, we must have $e \geq \binom{n}{2}$ by Lemma 4.1. Hence the contradiction. □

Acknowledgements

I want to express my gratitude to my advisor professor Harm Derksen whose patience and willingness to explain difficult concepts have kept me motivated throughout this work. I also want to extend my thanks the department of Mathematics at the University of Michigan for allowing me to come back this year around to further the research started last year. Finally, I want to thank the NSF whose grant number 1302032 has funded this research.

References

[1] D. Cox, J. Little, D. O'Shea. (1992): Ideals, varieties and algorithms. Springer, Berlin Heidelberg New York Tokyo (Undergraduate texts in mathematics).

[2] H. Derksen, G. Kemper, Computational Invariant Theory, Encyclopaedia of Mathematical Sciences 130, Springer-Verlag, Berlin, Heidelberg, New York 2002.

[3] H. Derksen, H. Kraft. Constructive Invariant Theory, Universitat Basel, October 15, 1995.

[4] P. Fleischmann, The Noether Bound in Invariant Theory of Finite Groups, Adv. in Math. 156 (2000), 23-32.

[5] J. Fogarty, On Noether's Bound for Polynomial Invariants of Finite Groups, Electronic Research Announcements of the AMS 7 (2001), 5-7.

[6] M. Mouyebe, H. Derksen. Degree Bounds on the Ring of Invariants, Math REU University of Michigan Ann-Arbor (2015) .

[7] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, Math. Annalen 77 (1916), 89-92.

[8] E. Noether, Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Characteristik p, Nachr. v. d Ges. Wiss. zu Gottingen (1926), 89-92.

[9] M.D. Neusel, Degree bounds - An invitation to postmodern invariant theory, Topology and its Applications 154 (2007) 792-814.

[10] M.D. Neusel, L. Smith, Invariant Theory of Finite Groups, Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI 2002.

[11] B.J. Schmid. Finite Groups and Invariant Theory. Mathematishes Institut Universitat Basel. April 1990.