Annales de l'institut Fourier

David Wehlau

Constructive invariant theory for tori

Annales de l'institut Fourier, tome 43, nº 4 (1993), p. 1055-1066

<http://www.numdam.org/item?id=AIF_1993__43_4_1055_0>

Ann. Inst. Fourier, Grenoble
43, 4 (1993), 1055-1066

CONSTRUCTIVE INVARIANT THEORY FOR TORI

by David L. WEHLAU

Introduction.

Let $\rho : G \to GL(V)$ be a rational representation of a reductive algebraic group over the algebraically closed field $\mathbf{k}$. The action of G on V induces an action of G on $\mathbf{k}[V]$, the algebra of polynomial functions on V, via $(g \cdot f)(v) = f(\rho(g^{-1})v)$ for $g \in G$, $f \in \mathbf{k}[V]$ and $v \in V$. The functions which are fixed by this action form a finitely generated subalgebra, $\mathbf{k}[V]^G$, the ring of invariants. The problem of constructive invariant theory is to give an algorithm which in a finite number of steps will explicitly construct a minimal set of homogeneous generators for the $\mathbf{k}$-algebra, $\mathbf{k}[V]^G$.

Now if $\{f_1, \ldots, f_p\}$ is such a set with $\deg f_1 \geq \deg f_2 \geq \ldots \geq \deg f_p$ then although the f_i are not uniquely determined the p-tuple of degrees $(\deg f_1, \ldots, \deg f_p)$ is unique. The number $N_{V,G} = \deg f_1$ is of special interest. It is the minimal integer N such that $\mathbf{k}[V]^G$ is generated by the subspace $\bigoplus_{m=0}^{N} \mathbf{k}[V]^G_m$ of invariants of degree at most N. Clearly an algorithm which constructs $\{f_1, \ldots, f_p\}$ also produces $N_{V,G} = \max\{\deg f_i \mid 1 \leq i \leq p\}$. For many groups, G, (e.g. if char $k = 0$ and G is reductive) the converse is also true : given $N_{V,G}$ there is a finite algorithm which constructs $\{f_1, \ldots, f_p\}$ (cf. [K], [P]).

If G is a finite group and the characteristic of $\mathbf{k}$ does not divide $|G|$, then by a celebrated theorem of Emmy Noether's, $N_{V,G} \leq |G|$ (see [N1]),

Research supported in part by NSERC Grant OGP0041784.
Key words : Torus invariants – Invariant theory – Torus representations.
A.M.S. Classification : 14D25 – 20M14.

[N2]). Recently Schmid has considered the question of whether this bound is sharp ([S]). She has shown that $N_{V,G} < |G|$ if G is not cyclic and has determined $N_{V,G}$ for various groups of small order including all abelian groups of order less than 30.

If G is semi-simple and the characteristic of $\mathbf{k}$ is zero and the representation ρ is almost faithful, then Popov has given in [P] an upper bound for $N_{V,G}$. Following the methods of Popov, Kempf ([K]) derived an upper bound for $N_{V,G}$ in the case that G is a torus and the characteristic of $\mathbf{k}$ is zero. Kempf also observed that these three bounds (for G finite, G semi-simple and G a torus) could be combined (by multiplying them) to obtain a bound for the general reductive group in characteristic zero.

The bounds for infinite groups are very large. In this paper we will consider the case $G = T$ is a torus and give better bounds for $N_{V,T}$. In addition we will construct certain distinguished elements of a minimal generating set for $\mathbf{k}[V]^T$.

I would like to thank John Harris for many helpful conversations.

Diagonalization.

Let $\mathbf{k}$ be an algebraically closed field of any characteristic. Let T be a torus, i.e., T is an algebraic group which is (abstractly) isomorphic to $(\mathbf{k}^*)^r$ and suppose that $\rho : T \to GL(V)$ is a rational representation of V. Let $X^*(T)$ denote the lattice of characters of T. Then $X^*(T)$ is (abstractly) isomorphic to $\mathbb{Z}^r$. From now on we will assume that we have chosen a fixed basis of V consisting of eigenvectors, $\{v_1, \ldots, v_n\}$, and that $\{x_1, \ldots, x_n\}$, is the corresponding dual basis of V^*. Furthermore we will denote the weight of v_i by ω_i. Then ρ induces an action of T on $V^* \subset \mathbf{k}[V]$ which in terms of weights is given by $t \cdot x_i = -\omega_i(t)x_i$. The action on all of $\mathbf{k}[V] \cong \mathbf{k}[x_1, \ldots, x_n]$ is obtained from the action on V^* by the two requirements $t \cdot (fg) = (t \cdot f)(t \cdot g)$ and $t \cdot (f + g) = t \cdot f + t \cdot g$ for $t \in T$ and $f, g \in \mathbf{k}[V]$.

We will consider monomials $X^A = x_1^{a_1} x_2^{a_2} \cdot \ldots \cdot x_n^{a_n}$ where $A = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Clearly T acts on X^A by $t \cdot X^A = \chi(t)X^A$ where χ is the character $\chi = -(a_1\omega_1 + \ldots + a_n\omega_n)$. We will denote χ by $\mathrm{wt}(X^A)$. The invariant monomials are in one-to-one correspondence with the semi-group, $S := \{A \in \mathbb{N}^n \mid X^A \in \mathbf{k}[V]^T\} = \{A \in \mathbb{N}^n \mid a_1\omega_1 + \ldots + a_n\omega_n = \mathbf{o}\}$ where $\mathbf{o}$ is the trivial character in $X^*(T)$. This semi-group was first studied by Gordan. He used it to show that $\mathbf{k}[V]^T$ is a finitely generated algebra by showing that S is finitely generated as a semi-group (see [Go]).

Recall that a representation $\rho : G \to GL(V)$ is called *stable* if the union of the closed G-orbits in V contains an open dense subset of V. It is sufficient to consider only faithful stable torus representations, (cf. [W], Lemma 2). From now on we will suppose that ρ is both faithful and stable.

Kempf's bound.

Choosing an explicit isomorphism $\psi : T \longrightarrow (k^*)^r$ induces an explicit isomorphism $\psi^* : X^*(T) \longrightarrow \mathbb{Z}^r$. The isomorphism ψ is determined only up to Aut $(T) \cong GL(r, \mathbb{Z})$. Having fixed a choice for ψ we may write out the weights of V as r-tuples: $\omega_i = (\omega_{i,1}, \ldots, \omega_{i,r}) \in \mathbb{Z}^r$ for $1 \le i \le n$. Then we may define $w := \max\{\,|\omega_{i,j}| : 1 \le i \le n,\ 1 \le j \le r\}$. Kempf showed in [K] that $N_{V,T} \le n\, C(n\, r!\, w^r)$ where $C(m)$ is the least common multiple of the integers $1, 2, \ldots, m$. This bound has the disadvantage of being dependent on w which depends on the choice of ψ.

Example 1. — Let $T \cong (\mathbf{k}^*)^2$ and let V be the 4 dimensional representation of T with weights $(2,2)$, $(-1,0)$, $(0,-5)$ and $(2,-1)$. It is fairly simple, for example using the iterative method of the next section, to compute a homogeneous minimal system of generators for $\mathbf{k}[V]^T$. We find that $\mathbf{k}[V]^T = \mathbf{k}[X^{R_1}, X^{R_2}, X^A]$ where $R_1 = (5, 10, 2, 0)$, $R_2 = (1, 6, 0, 2)$ and $A = (3, 8, 1, 1)$. Therefore $N_{V,T} = \deg R_1 = 17$. Here $r = 2$, $n = 4$ and $w = 5$. Hence for this example Kempf's bound gives $N_{V,T} \le 4\, C(4 \cdot 2! \cdot 5^2) = 4\, C(200) > 4(3 \times 10^{89}) > 10^{90}$.

An iterative method.

Consider first the case $r = 1$. Here the isomorphism of T with $\mathbf{k}^*$ is determined up to $GL(1, \mathbb{Z}) \cong \{\pm 1\}$ and thus w is completely determined in this case. Fixing one of the two choices $\psi : T \longrightarrow k^*$ we may write the weights of V as integers : $\omega_1, \omega_2, \ldots, \omega_n \in \mathbb{Z}$. Set $w_- := \min\{\omega_i | 1 \le i \le n\}$ and $w_+ := \max\{\omega_i | 1 \le i \le n\}$. Our assumptions that ρ is stable and faithful together imply that $w_- < 0$ and $w_+ > 0$.

THEOREM 1. — *Let V be a representation of $\mathbf{k}^*$ with weights $\omega_1 \ge \omega_2 \ge \ldots \ge \omega_n$ and set $B := \omega_1 - \omega_n$. Then $N_{V,\mathbf{k}^*} \le B$.*

Proof. — Suppose $X^A \in \mathbf{k}[V]^T$ has degree d. We will construct a sequence of d monomials: $h_1, h_2, \ldots, h_d$ with $\omega_n \leq \mathrm{wt}(h_i) \leq \omega_1 - 1$ for all $1 \leq i \leq d$ as follows. Choose j such that $\omega_j < 0$ and define $h_1 := x_j$. If $\mathrm{wt}(h_m) \geq 0$ then we choose j such that x_j divides X^A/h_m and $\omega_j \leq 0$. Similarly if $\mathrm{wt}(h_m) < 0$ then we choose j such that x_j divides X^A/h_m and $\omega_j > 0$. In either case we define $h_{m+1} := x_j\, h_m$. If $d > B$ then by the pigeon hole principle, two of the monomials have the same weight : $\mathrm{wt}(h_i) = \mathrm{wt}(h_j)$ where we may assume $i < j$. But then $h := h_j/h_i \in k[V]^T$ divides X^A and so we see that X^A is not irreducible. □

Remark 1. — If $\gcd(\omega_1, \omega_n) = 1$ then the invariant $x_1^{-\omega_n} x_n^{\omega_1}$ is irreducible and has degree $B = N_{V,\mathbf{k}^*}$.

Remark 2. — Note that $w = \max\{\omega_1, -\omega_n\}$ and therefore $N_{V,\mathbf{k}^*} \leq 2w$.

THEOREM 2. — $N_{V,T} \leq (2w)^{2^r-1}$

Proof. — We proceed by induction on r. The theorem is true for the case $r = 1$ by Remark 2. For higher values of r we consider the coordinate decomposition of T induced by the isomorphism ψ, i.e., $T \cong T_1 \times \ldots \times T_r$ where $T_j \cong \mathbf{k}^*$ and the weight of x_i with respect to T_j is $\omega_{i,j}$. Set $T' = T_2 \times \ldots \times T_r$ so that $T = T_1 \times T'$. By induction, there exist monomial generators $h_1, \ldots, h_p$ of $\mathbf{k}[V]^{T'}$ with $\deg h_i \leq (2w)^{(2^{r-1}-1)}$ for all $1 \leq i \leq p$. Write $h_i = X^A$ and set $\nu_i := \mathrm{wt}(h_i) \in X^*(T_1) \cong \mathbb{Z}$. Then $\nu_i = a_1\omega_{1,1} + \ldots + a_n\omega_{n,1}$. Hence $|\nu_i| \leq a_1 w + \ldots + a_n w = (\deg h_i) w \leq (2w)^{(2^{r-1}-1)}\, w$.

Let V_1 be a p dimensional $\mathbf{k}$-vector space and suppose that T_1 acts on V_1 by the weights $-\nu_1, \ldots, -\nu_p$. Then we have a T_1-equivariant surjection $\mathbf{k}[V_1] \twoheadrightarrow \mathbf{k}[V]^{T'} = \mathbf{k}[h_1, \ldots, h_p]$. In particular we have the surjection $\mathbf{k}[V_1]^{T_1} \twoheadrightarrow (\mathbf{k}[V]^{T'})^{T_1} = \mathbf{k}[V]^T$. Hence $N_{V,T} \leq N_{V,T'} \cdot N_{V_1,T_1} \leq (2w)^{(2^{r-1}-1)} \cdot 2(2w)^{(2^{r-1}-1)}\, w = (2w)^{2^r-1}$. □

For the representation described in Example 1 (for which $N_{V,T} = 17$) this theorem gives the bound $N_{V,T} \leq 1000$. This is a better bound than Kempf's for this example but this is only because r is so small in the example. As a function of r the bound given in Theorem 2 grows much much faster than Kempf's bound. This new bound is, however, distinguished by the fact that it is independent of $n = \dim V$.

Geometric bounds.

In this section we will construct a set of distinguished monomials which is a subset of a minimal generating set for $\mathbf{k}[V]^T$. We begin with some notation and definitions. We will use $\mathbf{o}$ to denote the origin in $X^*(T) \otimes \mathbb{Q} \cong \mathbb{Q}^n$. If $Z = (z_1, \ldots, z_n) \in \mathbb{Q}^n$ define $\deg Z := z_1 + \ldots + z_n$. We also define $\operatorname{supp}(Z) := \{i \mid 1 \leq i \leq n,\, z_i \neq 0\}$ and the length of Z, $\ell(Z) := \#\operatorname{supp}(Z) - 1$. If $\{Z_1, \ldots, Z_d\} \subset \mathbb{Q}^n$ then $\mathcal{H}(Z_1, \ldots, Z_d)$ denotes the convex hull of the points $Z_1, \ldots, Z_d$ and $\mathcal{P}(Z_1, \ldots, Z_d)$ denotes the convex set $\left\{ \sum_{i=1}^{d} \alpha_i Z_i \mid \alpha_i \in [0,1] \text{ for } i = 1, \ldots, d \right\}$. Notice that if $\{Z_1, \ldots, Z_d\}$ is linearly independent then $\mathcal{P}(Z_1, \ldots, Z_d)$ is a d-dimensional parallelepiped.

By a polytope we will mean a compact convex set having finitely many vertices. The vertices of a polytope P are characterized by the property that Y is a vertex of P if and only if the set $P \setminus \{Y\}$ is a convex set. A d dimensional polytope having $d+1$ vertices is a simplex. We will often consider the case of a d dimensional polytope $P \subset \mathbb{Q}^m$ with $m \geq d$. In this case when we refer to the volume of P we mean the (positive) d dimensional volume of P obtained by considering P as a subset of the d dimensional affine space, $\mathbb{A}^d$, spanned by P. If we wish to consider the m dimensional volume of P (which is zero if $d < m$) we will write $\operatorname{vol}_m(P)$. Similarly the relative interior of P refers to the interior of P defined by the subspace topology induced by $P \subset \mathbb{A}^d$.

The monomial generators of $\mathbf{k}[V]^T$ correspond to generators of the semi-group S. Gordan showed how to find the generators of S (see for example [O], Proposition 1.1 (ii)). Consider the pointed (half) cone $\Gamma \subset (\mathbb{Q}^+)^n$ generated by S: $\Gamma := (\mathbb{Q}^+ \cdot S)$ where $\mathbb{Q}^+ = \{ q \in \mathbb{Q} \mid q \geq 0 \}$. This cone, Γ, is just the set of solutions $(z_1, \ldots, z_n) \in (\mathbb{Q}^+)^n$ of the system of equations :

$$(*) \qquad z_1\omega_1 + \ldots + z_n\omega_n = \mathbf{o}.$$

If $\mathcal{L}$ is an extremal ray of Γ then $\mathcal{L} \cap S$ is a semigroup isomorphic to $\mathbb{N}$. Let $R_{\mathcal{L}}$ denote the unique generator of this semigroup. Write $\{R_1, \ldots, R_s\} = \{R_{\mathcal{L}} \mid \mathcal{L} \text{ an extremal ray of } C\}$. The intersection $\mathcal{P}(R_1, \ldots, R_s) \cap S$ is a finite generating set for S. Following Stanley ([St]), we call these R_j *completely fundamental generators* of S. These are characterized by the fact that if $mR_j = A+B$ for some $m \in \mathbb{N}$ and some $A, B \in S$ then $A = kR_j$ and $B = (m-k)R_j$ for some integer $k \leq m$ ([St], p. 36). The elements

$X^{R_1}, \ldots, X^{R_s}$ are the distinguished monomial generators we referred to earlier.

Now we are ready to begin our construction of the completely fundamental generators.

LEMMA 1. — *There exists $A \in S$ with* $\operatorname{supp}(A) = \Omega$ *if and only if* $\mathbf{o}$ *lies in the relative interior of* $\mathcal{H}(\omega_i \mid i \in \Omega)$.

Proof. — Suppose $0 \neq A \in S$ and $\operatorname{supp}(A) = \Omega$. Then we have $\mathbf{o} = \sum_{i=1}^{n} a_i\omega_i = \sum_{i\in\Omega} a_i\omega_i = \sum_{i\in\Omega} (a_i/\deg A)\,\omega_i$. Since $a_i \geq 0$ for all i and $\sum_{i\in\Omega} a_i = \deg A$ we see that $\mathbf{o} \in \mathcal{H}(\omega_i \mid i \in \Omega)$. Furthermore, since the coefficient $a_i/\deg A$ is non-zero for each $i \in \Omega$, $\mathbf{o}$ is an interior point of $\mathcal{H}(\omega_i \mid i \in \Omega)$.

Conversely, suppose that $\mathbf{o}$ lies in the relative interior of $\mathcal{H}(\omega_i \mid i \in \Omega)$. Then there exist rational numbers p_i/q where $p_i, q \in \mathbb{N}$ with $1 \leq p_i \leq q$ such that $\sum_{i\in\Omega} (p_i/q)\,\omega_i = \mathbf{o}$ and $\sum_{i\in\Omega} p_i/q = 1$. Hence if we define $p_i = 0$ if $i \notin \Omega$ we have $\sum_{i=1}^{n} p_i\omega_i = \mathbf{o}$ and $A := (p_1, \ldots, p_n) \in S$ with $\operatorname{supp}(A) = \Omega$.

□

Define a partial order on $\Gamma \setminus \{\mathbf{o}\}$ by inclusion of supports, i.e., if $Y_1, Y_2 \in \Gamma \setminus \{\mathbf{o}\}$ with $\operatorname{supp}(Y_1) \subseteq \operatorname{supp}(Y_2)$ then $Y_1 \preceq Y_2$. Also given $Y \in \Gamma$, define $\sigma(Y) := \mathcal{H}(\omega_i \mid i \in \operatorname{supp}(Y))$.

PROPOSITION 1. — *Let $\mathbf{o} \neq Y \in S$ with $Y/m \notin S$ for all $m \geq 2$. Then the following are all equivalent :*

(1) *Y is minimal in Γ.*

(2) *$\sigma(Y)$ is an $\ell(Y)$ dimensional simplex with $\mathbf{o}$ in its relative interior.*

(3) *Y is a completely fundamental generator of S.*

Proof. — The proof that (1) $\Longrightarrow$ (2) follows from Lemma 1. Let Y be an element of S which is minimal with respect to the partial order. Then by Lemma 1, $\mathbf{o}$ lies in the relative interior of $\sigma(Y)$. Therefore $\sigma(Y)$ is an $\ell(Y)$ dimensional simplex with $\mathbf{o}$ in its relative interior. For if this were not true, by Carathéodory's theorem (see for example [B], Corollary 2.4 or [O], Theorem A.3), we could find a proper subset $\Omega \subsetneq \operatorname{supp}(Y)$ such that $\mathbf{o} \in \mathcal{H}(\omega_i \mid i \in \Omega)$. But this would contradict the minimality of Y.

In particular, this implies that any proper subset of $\{\omega_i \mid i \in \operatorname{supp}(Y)\}$ is linearly independent.

Now to see that (2) $\Longrightarrow$ (3), suppose (2) holds and that there exists $n \in \mathbb{N}$ and $A, B \in S$ with $nY = A + B$. Since $\sigma(Y)$ is a simplex, $\mathbf{o}$ can be expressed *uniquely* as a convex linear combination of $\{\, \omega_i \mid i \in \operatorname{supp}(Y)\,\}$: $\sum_{i \in \operatorname{supp}(Y)} \alpha_i \omega_i = \mathbf{o}$ where $\alpha_i \in [0,1]$ and $\sum_{i \in \operatorname{supp}(Y)} \alpha_i = 1$. Now $\sum_i a_i \omega_i = \mathbf{o}$ and $a_i = 0$ if $i \notin \operatorname{supp}(Y)$. Hence, by the uniqueness, we have $a_i / \deg(A) = \alpha_i = y_i / \deg(Y)$. Therefore $A = (\deg A / \deg Y) Y$ from which it follows that Y is completely fundamental.

Finally, we prove that (3) $\Longrightarrow$ (1). Suppose Y is a completely fundamental generator of S and $Z \in \Gamma$ with $Z \preceq Y$. Clearly, clearing denominators, we may suppose that $Z \in S$. Since $Z \preceq Y$, for $m \in \mathbb{N}$ sufficiently large we have $my_i \geq z_i$ for all $1 \leq i \leq n$. Hence mY decomposes within S as $mY = Z + (mY - Z)$. Since Y is completely fundamental, this implies that $Z = kY$ for some $k \leq m$. Hence $\operatorname{supp}(Y) = \operatorname{supp}(Z)$ and $Y \preceq Z$. □

Thus to each minimal element Y of Γ we have an associated $\ell(Y)$ dimensional simplex, $\sigma(Y) := \mathcal{H}(\omega_i \mid i \in \operatorname{supp}(Y))$. Given $\operatorname{supp}(Y)$ we can recover Y since every point in a simplex can be written *uniquely* as a convex linear combination of the vertices of the simplex. Therefore the map $Y \mapsto \operatorname{supp}(Y)$ is one-to-one. Moreover, if $Y \in \Gamma$ is minimal then $\{\omega_i \mid i \in \operatorname{supp}(Y)\}$ is a minimal linearly dependent subset of $\{\omega_1, \ldots, \omega_n\}$.

Note that the map $Y \mapsto \sigma(Y)$ is not necessarily one-to-one. More precisely, $\operatorname{supp}(Y) \mapsto \sigma(Y)$ is one-to-one if and only if the weights of V are distinct. If V_1 and V_2 are two representations of T having the same weights (except for multiplicities) then clearly, $N_{V_1,T} = N_{V_2,T}$ and thus it would suffice to consider only representations whose weights were distinct.

THEOREM 3. — *If the R_j are ordered so that* $\deg R_1 \geq \deg R_2 \geq \ldots \geq \deg R_s$ *then* $N_{V,T} \leq \sum_{j=1}^{n-r} \deg R_j \leq (n-r) \deg R_1$.

Proof. — Suppose $\mathbf{o} \neq A \in S$. By Carathéodory's theorem we may write

$$A = \alpha_1 R_{j_1} + \ldots + \alpha_{n-r} R_{j_{n-r}}$$

where each $\alpha_j \geq 0$. If $\alpha_j > 1$ then we may decompose A within S as $A = (A - R_{j_i}) + R_{j_i}$. Hence if A is a generator of S then each $\alpha_i \leq 1$. But then $\deg A = \alpha_1 \deg R_{j_1} + \ldots + \alpha_{n-r} \deg R_{j_{n-r}} \leq \deg R_{j_1} + \ldots + \deg R_{j_{n-r}} \leq \deg R_1 + \ldots + \deg R_{n-r}$. □

Remark 3. — Applying these two bounds to the representation of Example 1 we get $N_{V,T} \leq 17 + 9 = 26$ and $N_{V,T} \leq 2 \cdot 17 = 34$.

A theorem of Ewald and Wessels ([EW], Theorem 2) allows us to improve the preceding theorem. Specifically, (using the notation of Theorem 3) they show that if $\alpha_1 + \ldots + \alpha_{n-r} > n - r - 1 \geq 1$ then A is decomposable within S. Thus we have the following corollary.

COROLLARY 1. — *If* $n - r \geq 2$ *then* $N_{V,T} \leq (n - r - 1) \deg R_1$.

Remark 4. — If we apply this result to Example 1 we find that $N_{V,T} \leq (4 - 2 - 1) \cdot 17 = 17$.

The following proposition shows how the completely fundamental solutions are distinguished among the elements of a monomial minimal generating set.

PROPOSITION 2 (Stanley [St], Theorem 3.7). — *Suppose* $\{X^{A_1}, \ldots, X^{A_q}\}$ *is any minimal set of monomials such that* $\mathbf{k}[V]^T$ *is integral over* $\mathbf{k}[X^{A_1}, \ldots, X^{A_q}]$. *Then* $q = s$ *and there exists a permutation* π *of* $\{1, \ldots, s\}$ *such that* $\operatorname{supp}(R_j) = \operatorname{supp}(A_{\pi(j)})$. *In fact, there exist positive integers* $m_1, \ldots, m_s$ *such that* $A_{\pi(j)} = m_j \cdot R_j$.

Remark 5. — Kempf ([K]) also constructed the elements $R_1, \ldots, R_s$. His method of construction is somewhat less direct than that which we will give in the next section and consequently the bound he gave for $\deg R_j$ is larger than the one we will give.

Computing the completely fundamental generators.

In this section we will give an algorithm for finding the completely fundamental generators. Suppose Ω is a minimal linearly dependent subset of $\{\omega_1, \ldots, \omega_n\}$ with $\mathbf{o} \in \mathcal{H}(\omega \in \Omega)$. Then $\Omega = \{\,\omega_i \mid i \in \operatorname{supp}(R_j)\,\}$ for some j. We want to compute R_j. Set $d := \ell(R_j) \leq r$. Then without loss of generality we may suppose that $\operatorname{supp}(R_j) = \{1, 2, \ldots, d+1\}$. Consider the system of r linear equations in d unknowns :

$$(\dagger) \qquad y_1\omega_1 + \ldots + y_d\omega_d = -\omega_{d+1}.$$

These r equations impose only d conditions and so in order to solve this system we take the $r \times d$ matrix of rank d, $M := (\omega_1\ \omega_2\ \dots\ \omega_d)$ and choose a $d \times d$ non-singular submatrix M'. If M' consists of the rows $j_1, \dots, j_d$ of M then the ith column of M' is $\omega'_i := (\omega_{i,j_1}, \dots, \omega_{i,j_d})$ for $1 \leq i \leq d$. Also define $\omega'_{d+1} := (\omega_{d+1,j_1}, \dots, \omega_{d+1,j_d})$. Then solving (†) is equivalent to solving

$$(\dagger\dagger) \qquad y_1\omega'_1 + \dots + y_d\omega'_d = -\omega'_{d+1}.$$

But we may solve (††) by Cramer's rule :

$$y_1 = \frac{|\omega'_{d+1}, \omega'_2, \dots, \omega'_d|}{|\omega'_1, \omega'_2, \dots, \omega'_d|}, \quad \dots, \quad y_d = \frac{|\omega'_1, \dots, \omega'_{d-1}, \omega'_{d+1}|}{|\omega'_1, \omega'_2, \dots, \omega'_d|}.$$

Then if we define

$$\begin{aligned} q_i &= y_i|\omega'_1, \dots, \omega'_d| \\ &= |\omega'_1, \dots, \omega'_{i-1}, \omega'_{d+1}, \omega'_{i+1}, \dots, \omega'_d| \text{ for } 1 \leq i \leq d \\ \text{and } q_{d+1} &= -|\omega'_1, \omega'_2, \dots, \omega'_d| \end{aligned}$$

we have

$$q_1\omega_1 + \dots + q_{d+1}\omega_{d+1} = \mathbf{o}$$

where each $q_i \in \mathbb{Z}$. This solution is unique up to scalar multiplication by an element of $\mathbb{Q}$. Since $\mathbf{o} \in \mathcal{H}(\omega_1, \dots, \omega_{d+1})$ all the q_i must have the same sign and, multiplying by -1 if necessary, we get each $q_i \in \mathbb{N}$. If we define $q_i = 0$ for all $i \notin \{1, \dots, d+1\} (= \operatorname{supp}(R_j))$ and $Q_j := (q_1, \dots, q_n)$ then $R_j = Q_j/m$ where m is the greatest common divisor of the integers $q_1, \dots, q_{d+1}$.

Thus to construct $\{R_1, \dots, R_s\}$ we consider each minimal linearly dependent subset, Ω, of the weights $\{\omega_1, \dots, \omega_n\}$. For each such Ω we compute the determinants $q_1, \dots, q_{d+1}$. If any two of these determinants have opposite signs then Ω does not correspond to any invariant. If however, all the q_i have the same sign then $(q_1/m, \dots, q_n/m)$ is one of the completely fundamental generators.

Degrees as volumes.

In this section we will continue to study the fixed R_j of the previous section. We will obtain bounds on $\deg R_j$ and thus on $N_{V,T}$ in terms of volumes of certain polytopes.

THEOREM 4. — *Let σ_j be the simplex $\sigma_j = \mathcal{H}(\omega_i \mid i \in \operatorname{supp}(R_j))$. Then* $\deg R_j \le d!\operatorname{vol}(\sigma_j)$.

Proof. — Let Δ denote the perpendicular (coordinate) projection :

$$\Delta : X^*(T) \otimes \mathbb{Q} \cong \mathbb{Q}^r \to \mathbb{Q}^d \text{ given by } \Delta(u_1, \ldots, u_r) = (u_{j_1}, \ldots, u_{j_d}).$$

Then $\Delta(\omega_i) = \omega_i'$. Define $\sigma_j(i) := \mathcal{H}(\mathbf{o}, \omega_1, \ldots, \omega_{i-1}, \omega_{i+1}, \ldots, \omega_{d+1})$, $\sigma_j' := \Delta(\sigma_j)$ and $\sigma_j'(i) := \Delta(\sigma_j(i))$. Notice that q_i is the d dimensional volume of the parallelepiped $\mathcal{P}(\omega_1', \ldots, \omega_{i-1}', \omega_{i+1}', \ldots, \omega_{d+1}')$. Hence $q_i = d!\operatorname{vol}(\sigma_j'(i))$.

Now $\sigma_j' = \sigma_j'(1) \cup \ldots \cup \sigma'(d+1)$ is a triangulation of σ_j' by d-simplices since $\mathbf{o}$ lies in the relative interior of σ_j'. Thus $\deg Q_j = q_1 + \ldots + q_{d+1} = d!\operatorname{vol}(\sigma_j')$. Therefore $\deg R_j \le \deg Q_j = d!\operatorname{vol}(\sigma_j') \le d!\operatorname{vol}(\sigma_j)$ where the last inequality follows for example from [Ga], (30) p. 253. □

Let $\mathcal{W} := \mathcal{H}(\omega_1, \ldots, \omega_n)$, the convex hull of the weights in $X^*(T) \otimes \mathbb{Q} \cong \mathbb{Q}^r$.

THEOREM 5. — $\deg R_j \le r!\operatorname{vol}(\mathcal{W})$.

Proof. — It is not true in general that $d!\operatorname{vol}(\sigma_j') \le r!\operatorname{vol}(\mathcal{W})$ when $d < r$. Hence to prove this theorem we consider a slightly different construction of R_j (when $d < r$). Recall that we have assumed that $\operatorname{supp}(R_j) = \{1, \ldots, d+1\}$. Without loss of generality we may assume that $\Sigma := \mathcal{H}(\omega_1, \ldots, \omega_{d+1}, \ldots, \omega_{r+1})$ is an r dimensional simplex. To construct R_j we solve the system of r linearly independent equations in r unknowns :

$$y_2\omega_2 + \ldots + y_{r+1}\omega_{r+1} = -\omega_1.$$

As before we apply Cramer's rule to solve this system and so find $(a_1, \ldots, a_{r+1}) \in \mathbb{N}^{r+1}$ with

$$a_1\omega_1 + \ldots + a_{r+1}\omega_{r+1} = \mathbf{o}$$
$$\text{and } a_i = r!\operatorname{vol}_r(\mathcal{H}(\mathbf{o}, \omega_1, \ldots, \omega_{i-1}, \omega_{i+1}, \ldots, \omega_{r+1})).$$

Again we set $a_{r+2} = \ldots = a_n = 0$ and $A = (a_1, \ldots, a_n)$. Notice that $a_{d+2} = \ldots = a_{r+1} = 0$ and that A is a multiple of R_j. Hence $\deg R_j \le \deg A = a_1 + \ldots + a_n = r!\operatorname{vol}(\Sigma) \le r!\operatorname{vol}(\mathcal{W})$. □

COROLLARY 2. — *If $n - r \ge 2$ then $N_{V,T} \le (n-r-1)\,r!\operatorname{vol}(\mathcal{W})$. If $1 \le n - r \le 2$ then $N_{V,T} \le r!\operatorname{vol}(\mathcal{W})$.*

Remark 6. — This bound is invariant under the action of $\operatorname{Aut}(T) \cong GL(r, \mathbb{Z})$ and thus is independent of the choice of ψ.

Remark 7. — For the representation of Example 1, $\mathcal{W}$ is a quadrilateral of area 23/2. Hence we get the bound $N_{V,T} \leq 2! \cdot (23/2) = 23$.

It seems likely that the factor $n - r - 1$ is unnecessary in the first statement of Corollary 2. I know of no examples of representations where $N_{V,T} > r!\,\mathrm{vol}(\mathcal{W})$. Conversely for all values of n and r there exist faithful stable n dimensional representations, V, of $T \cong (\mathbf{k}^*)^r$ such that $N_{V,T} = r!\,\mathrm{vol}(\mathcal{W})$ – for example this often occurs when $\mathcal{W}$ is itself a simplex.

CONJECTURE. — *There is a (small) constant $c \in \mathbb{R}$ such that $N_{V,T} \leq c\,r!\,\mathrm{vol}\,(\mathcal{W})$.*

Bounds in terms of w.

Next we bound $\deg R_j$ in terms of $w := \max\{|\omega_{i,m}| : 1 \leq i \leq n, 1 \leq m \leq r\}$.

THEOREM 6. — $\deg R_j \leq \lfloor w^d\,(d+1)^{(d+1)/2} \rfloor$.

Proof. — We have $\deg R_j \leq d!\,\mathrm{vol}(\sigma'_j)$ where $\sigma'_j = \mathcal{H}(\omega'_1, \ldots, \omega'_{d+1}) \subset [-w, w]^d \subset \mathbb{Q}^d$. Define $\widetilde{\sigma'_j} := \mathcal{H}(\omega'_1/2w, \ldots, \omega'_{d+1}/2w) + (1/2, \ldots, 1/2)$. Then $\widetilde{\sigma'_j}$ is a d dimensional simplex contained in $[0,1]^d$ with $\mathrm{vol}(\sigma'_j) = (2w)^d \mathrm{vol}(\widetilde{\sigma'_j})$.

Thus we now seek to bound the value $B := \max\{\mathrm{vol}(\tau) \mid \tau \subset [0,1]^d$ is a d dimensional simplex$\}$. By linear programming it is clear that the value B is attained by a simplex μ all of whose vertices are also vertices of the cube $[0,1]^d$. Without loss of generality we may assume that $(0, \ldots, 0)$ is one of the vertices of μ. Let $\nu_1, \ldots, \nu_d$ be the other vertices of μ. Then $\mathrm{vol}(\mu) = |\det(M)|/d!$ where $M = (\nu_1\ \ldots\ \nu_d)$ is a $d \times d$ matrix all of whose entries are either 0 or 1. But then by a theorem of Ryser (see [R], Equation (11)) we have

$$|\det(M)| \leq 2\left(\frac{\sqrt{d+1}}{2}\right)^{d+1}.$$

Thus we get the bound $\deg R_j \leq w^d (d+1)^{(d+1)/2} \leq w^r (r+1)^{(r+1)/2}$. □

COROLLARY 3. — *If $n - r \geq 2$ then $N_{V,T} \leq (n-r-1)\lfloor w^r (r+1)^{(r+1)/2} \rfloor$. If $1 \leq n-r \leq 2$ then $N_{V,T} \leq \lfloor w^r (r+1)^{(r+1)/2} \rfloor$.*

Remark 8. — In Example 1 we had $n = 4$, $r = 2$ and $w = 5$. Thus Corollary 3 gives $N_{V,T} \leq \lfloor 5^2 \cdot (2+1)^{(2+1)/2} \rfloor = \lfloor 25 \cdot 3^{3/2} \rfloor = 129$.

BIBLIOGRAPHY

[B] A. BRONDSTED, An Introduction to Convex Polytopes, Springer-Verlag, Berlin–Heidelberg–New York, 1983.

[EW] G. EWALD, U. WESSELS, On the ampleness of invertible sheaves in complete projective toric varieties, Results in Math., (1991), 275–278.

[Ga] F.R. GANTMACHER, The Theory of Matrices, Vol. 1, Chelsea Publishing Company, New York, 1959.

[Go] P. GORDAN, Invariantentheorie, Chelsea Publishing Company, New York, 1987.

[K] G. KEMPF, Computing Invariants, S. S. Koh (Ed.) Invariant Theory, Lect. Notes Math., 1278, 81–94, Springer-Verlag, Berlin–Heidelberg–New York, 1987.

[N1] E.NOETHER, Der endlichkeitssatz der Invarianten endlicher Gruppen, Math. Ann., 77 (1916), 89–92.

[N2] E. NOETHER, Der endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p., Nachr. v. d. Ges. Wiss. zu Göttingen, (1926), 485–491.

[O] T. ODA, Convex Bodies and Algebraic Geometry, Ergeb. Math. und Grenzgeb., Bd. 15 , Springer-Verlag, Berlin–Heidelberg–New York, 1988.

[P] V.L. POPOV, Constructive Invariant Theory, Astérisque, 87/88 (1981), 303–334.

[R] H.J. RYSER, Maximal Determinants in Combinatorial Investigations, Can. Jour. Math., 8 (1956), 245–249.

[S] B. SCHMID, Finite Groups and Invariant Theory, M.-P. Malliavin(Ed.) Topics in Invariant Theory (Lect. Notes Math. 1478), 35–66, Springer-Verlag, Berlin–Heidelberg–New York, 1991 .

[St] R.P. STANLEY, Combinatorics and Commutative Algebra, Progress in Mathematics, 41, Birkhäuser, Boston–Basel–Stuttgart, 1983.

[W] D. WEHLAU, The Popov Conjecture for Tori, Proc. Amer. Math. Soc., 114 (1992), 839–845.

Note added in proof: The construction of the completely fundamental generators given here was also pointed out by B. Sturmfels in "Gröbner bases of toric varieties", Tôhoku Math. J., second series, vol. 43, no. 2 (1991).

Manuscrit reçu le 27 novembre 1992.

David L. WEHLAU,
The Royal Military College of Canada
Dept of Mathematics & Computer Science
Kingston K7K 5LO (Canada).