Rational invariants of scalings from Hermite normal forms.

Evelyne Hubert,
INRIA Méditerranée,
Sophia Antipolis, France,
Evelyne.Hubert@inria.fr,

George Labahn
Cheriton School of Computer Science
University of Waterloo, Canada,
glabahn@uwaterloo.ca

ABSTRACT

Scalings form a class of group actions that have both theoretical and practical importance. A scaling is accurately described by an integer matrix. Tools from linear algebra are exploited to compute a minimal generating set of rational invariants, trivial rewriting and rational sections for such a group action. The primary tools used are Hermite normal forms and their unimodular multipliers. With the same line of ideas, a complete solution to the scaling symmetry reduction of a polynomial system is also presented.
Keywords: Matrix normal form; Group actions; Rational invariants; Symmetry reduction.
AMS Classification: 08-04 12-04 14L30 15-04

1. INTRODUCTION

Scalings form a simple class of group actions: they are diagonal actions of a torus on an affine space. For example,

$$[(\mu,\nu),(z_1,z_2,z_3,z_4,z_5)] \to (\mu^6 z_1, \nu^3 z_2, \frac{\nu}{\mu^4} z_3, \frac{\mu}{\nu^4} z_4, \mu^3\nu^3 z_5)$$

describes the action of the group $(\mathbb{R}^*)^2$, with coordinates (μ,ν), on $\mathbb{R}^5$, with coordinates (z_1,z_2,z_3,z_4,z_5). The action simply rescales each individual coordinate. One can check that the three rational functions

$$g_1 = z_1 z_2^2 z_3^2 z_4^2, \quad g_2 = \frac{z_2^3 z_4^2}{z_1 z_3}, \quad g_3 = \frac{z_2 z_4 z_5}{z_1^2 z_3^2}$$

are left invariant by any of the above transformation determined by (μ,ν). They actually form a generating set of invariants of the scaling: they have the property that any other rational invariant f can be written as a rational function of them. In fact they have an even stronger property: the rewriting is given by a simple substitution. Indeed, if $f(z)$ is a rational invariant then

$$f(z_1,z_2,z_3,z_4,z_5) = f\left(g_1^{-1}, g_2, g_1, g_2^{-1}, g_3\right).$$

Providing a generating set of rational invariants along with an associated rewriting substitution for any given scaling is the first goal of the present article.

Though simple, scalings and their invariants have considerable practical importance. On the theoretical front scalings are known as torus actions and play a major role in algebraic geometry and combinatorics. In addition, they underlie what is known as dimensional analysis with the invariants giving the dimensionless quantities needed to derive physical laws [2, 3, 11]. Dimensional analysis has been automated in the works [12] and [13]. Central to this is the Buckingham-π-theorem. A reinterpretation of it states that a fundamental set of invariants is obtained from the basis of the nullspace of a matrix of exponents of the scaling [19, Section 3.4]. A second use of scalings is that they give mathematical sense to the rule of thumb used to reduce the number of parameters in biological models [15, 18]. This reduction by scaling symmetry of dynamical or polynomial systems was previously studied in [10, 14, 23].

In this paper we go further in this direction than handled in the previously cited works. In particular we produce invariants which are rational functions, that is, which do not involve any square roots or other fractional powers of the variables. In addition we provide trivial rewrite rules for our generating set of invariants. By this we mean that we give explicit substitution rules for rewriting any rational invariant (and actually any smooth invariant) in terms of the generating set. Again, this operation is performed without introducing any radicals.

Algorithmic tools for finding generating rational invariants and rewrite rules for the general class of rational actions of an algebraic group typically require Gröbner bases computations [7, 17]. A rewriting substitution can be achieved provided we allow algebraic functions [8].

In the case of scaling we show that a unimodular multiplier for the Hermite normal form of the integer matrix of exponents contains even more information. The unimodular multiplier provides a basis for the integer lattice of vectors in the kernel of the matrix of exponents. This basis actually describes rational invariants given as Laurent monomials (that is, monomials where we allow negative powers). We show that these invariants form a generating set for the field of rational invariants, and indeed forms a minimal generating set.

In fact we show more than the generation property. We also provide a simple method to rewrite any invariant in terms of these monomials via variable substitution. The substitution is read off from the inverse of the unimodular multiplier. The triviality of the rewrite rules actually reflects the existence of a rational section to the orbits of the action. The equation of the section can be read off the unimodular multiplier, something of independent theoretical interest in the area of group actions.

The unimodular multiplier for the Hermite form of the matrix of exponents is not unique. We give a construction for a canonical unimodular multipler which allows us to pinpoint the simplest rational sections. Our construction is also practical in terms of computation with the cost of determining both the Hermite form and the canonical unimodular multiplier being $O^{\sim}\left(n^{\omega+1}d\right)$. Here $O^{\sim}$ is the same as Big-O but without log factors, ω is the power of fast matrix multiplication and d is the maximal integer exponent of the scaling.

In order to show a practical application of our new tools we address and solve a specific symmetry reduction problem. The knowledge of a symmetry of the solution set of a polynomial system brings implies that the size of the problem can perhaps be reduced by factoring out the symmetry. The reduced system is given in terms of new variables which represent the generating invariants. Generally a more difficult task is then to retrieve the solution of the original system from the solution of the reduced system. In the case of scaling symmetries, the number of variables is reduced by the dimension of the group by a simple substitution. Here we provide a parameterization of the toric solutions of the original system from the toric solutions of the reduced system. Geometrically, the solution of the reduced sytem is the intersection of the solution set of the original system with the rational section. Yet, a unimodular multiplier for the Hermite normal form, and its inverse, are the only data required to spell out this symmetry reduction scheme.

2. INTEGER MATRIX NORMAL FORMS

In this section we provide the basic information about the Hermite normal form of a matrix of integers and its unimodular multiplier. We propose a canonical unimodular multiplier that is relevant in providing a simple rational section to the orbits of a scaling.

2.1 Hermite Normal Forms

Definition 2.1 *An $m \times n$ integer matrix $H = [h_{ij}]$ is in* column Hermite Normal Form *if there exists an integer r and a strictly increasing sequence $i_1 < i_2 < \cdots < i_r$ of pivot rows such that the last $n-r$ columns are zero and*

(i) $h_{k,j} = 0$ *for* $k > i_j$;

(ii) $0 \le h_{i_j,k} < h_{i_j,j}$ *when* $j < k$.

Thus a matrix is in column Hermite normal form if the submatrix formed by the pivot rows $i_1, \cdots, i_r$ and the first r columns is upper triangular and that all nonzero elements of the pivot rows are positive and less than the corresponding (positive) diagonal entry. The integer r is the rank of the matrix. By changing column to row and row to column indices in (i) and (ii) one obtains the *row Hermite Normal Form* of a matrix of integers.

Every integer matrix can be transformed via integer column operations to obtain a unique column Hermite form. The column operations are encoded in unimodular matrices, that is, invertible integer matrices whose inverses are also integer matrices. Thus for each A there exists a unimodular matrix V such that $A \cdot V$ is in Hermite normal form. Similar statements also hold for the row Hermite normal form. We refer the reader to [4, 22] for more information on such forms.

When $A \in \mathbb{Z}^{r\times n}$, with $r \le n$, has full row rank r then the column Hermite normal form satisfies:

$$A \cdot V = [H, 0] \text{ with } H \in \mathbb{Z}^{r\times r} \text{ triangular of full rank.} \quad (1)$$

If $W \in \mathbb{Z}^{n\times n}$ is the inverse of V then we can partition V and W as

$$V = [V_{\mathfrak{i}}, V_{\mathfrak{n}}] \text{ with } V_{\mathfrak{i}} \in \mathbb{Z}^{n\times r} \text{ and } V_{\mathfrak{n}} \in \mathbb{Z}^{n\times(n-r)} \quad (2)$$

and

$$W = \left[\begin{array}{c} W_{\mathfrak{u}} \\ W_{\mathfrak{d}} \end{array}\right] \text{ with } W_{\mathfrak{u}} \in \mathbb{Z}^{r\times n} \text{ and } W_{\mathfrak{d}} \in \mathbb{Z}^{(n-r)\times n}. \quad (3)$$

We then have

$$I_n = WV = \left[\begin{array}{cc} W_{\mathfrak{u}}V_{\mathfrak{i}} & W_{\mathfrak{u}}V_{\mathfrak{n}} \\ W_{\mathfrak{d}}V_{\mathfrak{i}} & W_{\mathfrak{d}}V_{\mathfrak{n}} \end{array}\right] \quad (4)$$

$$I_n = VW = V_{\mathfrak{i}}W_{\mathfrak{u}} + V_{\mathfrak{n}}W_{\mathfrak{d}} \ . \quad (5)$$

Note that the blocks of V provide the Hermite normalization of the blocks of W since from (4) we have

$$W_{\mathfrak{u}}[V_{\mathfrak{i}}, V_{\mathfrak{n}}] = [I_r, 0] \quad \text{and} \quad W_{\mathfrak{d}}[V_{\mathfrak{n}}, V_{\mathfrak{i}}] = [I_{n-r}, 0].$$

We state some well known properties of Hermite normal forms [4, 22] in a way that will be needed later in the paper.

Lemma 2.2 *Let $A \in \mathbb{Z}^{r\times n}$ be a full row rank matrix and $V \in \mathbb{Z}^{n\times n}$ a unimodular matrix such that $AV = [\ H,\ 0]$ with $H \in \mathbb{Z}^{r\times r}$. If V is partitioned as in (2), then the columns of $V_{\mathfrak{n}}$ form a basis for the integer lattice defined by the kernel of A.*

2.2 Normal unimodular multiplier

For the problem of interest in this paper the number of columns is larger than the rank. In this case the unimodular multiplier is not unique. Indeed, with the partition $V = [V_{\mathfrak{i}}, V_{\mathfrak{n}}]$ as in (2), column operations using the columns of $V_{\mathfrak{n}}$ do not affect the Hermite form H for the initial matrix A and hence results in a different unimodular multiplier V. In this subsection we describe a normalization of the multiplier V which is both simple and unique. Previous work on determining unique unimodular multipliers includes that of [6] for integer matrices where the unimodular multiplier is reduced via lattice reduction. We favor the component $V_{\mathfrak{n}}$ to be in Hermite normal form, as in [1], which deals with polynomial matrices. The resulting triangular form exhibits the simplest rational sections (Proposition 4.7) and allows for a rational parameter reduction scheme for dynamical systems [9].

Proposition 2.3 *Suppose $A \in \mathbb{Z}^{r\times n}$ has full row rank. Then there exists a* unique *unimodular matrix V (called the* normal unimodular multiplier*) such that* *(a)* $A \cdot V = [H, 0]$ *with* $H \in \mathbb{Z}^{r\times r}$ *in column Hermite normal form,*

(b) $V = [V_{\mathfrak{i}}, V_{\mathfrak{n}}]$ *with* $V_{\mathfrak{n}} \in \mathbb{Z}^{n\times(n-r)}$ *in column Hermite normal form,*

(c) If $i_1 < i_2 < \cdots < i_{n-r}$ *are the pivot rows for* $V_{\mathfrak{n}}$ *then for each* $1 \le j \le n-r$ *:*

$$0 \le [V_{\mathfrak{i}}]_{i_j,k} < [V_{\mathfrak{n}}]_{i_j,j} \text{ for all } 1 \le k \le r.$$

Thus $V_{\mathfrak{i}}$ *is reduced with respect to the pivot rows of* $V_{\mathfrak{n}}$*.*

Proof. While it is possible to prove the result directly, the following gives a proof which also hints at a simple method for computing both the Hermite form and its normal unimodular multiplier.

Let $V^* \in \mathbb{Z}^{n\times n}$ be a unimodular matrix such that

$$H^* = \begin{bmatrix} I_n \\ A \end{bmatrix} \cdot V^*$$

is in column Hermite form. Partition $V^* = [V_1^*, V_2^*]$ with V_2^* having r columns and set $V = [V_2^*, V_1^*]$. We claim that V is our normal unimodular multiplier, that is, $V_1^* = V_{\mathfrak{n}}$ and $V_2^* = V_{\mathfrak{i}}$.

Notice first that V is unimodular since this matrix is simply a reordering of the columns of the unimodular matrix V^*. In addition, since $A\cdot V^*$ is equal to the last r rows of H^*, which is in column Hermite form, and A has full row rank, says that $A \cdot V^* = [0, H^+]$ with H^+ in Hermite form. Therefore $A \cdot V = [H^+, 0]$ is in column Hermite form with V unimodular and so by uniqueness we have $H^+ = H$. This gives part (a). Parts (b) and (c) follow from the fact that V^* is also equal to the first n rows of H^*, which is in column Hermite form. Finally, the uniqueness of V follows from the uniqueness of Hermite forms. □

The proof of Proposition 2.3 provides a computational method for determining both the Hermite form H and the normal unimodular multiplier $V = [V_{\mathfrak{i}}, V_{\mathfrak{n}}]$. Indeed one has

$$\begin{bmatrix} I_n \\ A \end{bmatrix} \cdot [V_{\mathfrak{n}}, V_{\mathfrak{i}}] = \begin{bmatrix} V_n & V_i \\ 0 & H \end{bmatrix},$$

with the right side in column Hermite form. The complexity of such a computation is therefore the cost of finding a column Hermite form of an $(r+n)\times n$ integer matrix. This can be done using the methods of [24, 25] with a cost of $O^{\sim}\left(n^{\omega+1}d\right)$ bit operations, with d being the size of the largest entry in A.

Example 2.4 *Let*

$$A = \begin{bmatrix} 8 & 2 & 15 & 9 & 11 \\ 6 & 0 & 6 & 2 & 3 \end{bmatrix}$$

which has Hermite normal form $[I_2, 0]$*. The reduction performed by Maple results in the unimodular multiplier*

$$V' = \left[\begin{array}{rr|rrr} -49 & -1 & -57 & -13 & -28 \\ -36 & -1 & -42 & -10 & -21 \\ 79 & 2 & 92 & 21 & 45 \\ -36 & -1 & -42 & -9 & -21 \\ -36 & -1 & -42 & -10 & -20 \end{array}\right].$$

while the normalized unimodular multiplier is

$$V = \left[\begin{array}{rr|rrr} -1 & -2 & -2 & -2 & -1 \\ -3 & -14 & -7 & -13 & -7 \\ 1 & 1 & 2 & 1 & 0 \\ 0 & 2 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 2 \end{array}\right].$$

3. SCALINGS

Scalings can be described through the matrix of exponents of the group parameters as they act on each component. In this section we describe the matrix forms and properties that are useful when representing scalings and computing their invariants.

We consider an algebraically closed field $\mathbb{K}$, the multiplicative group of which is $\mathbb{K}^*$.

3.1 Matrix notations for monomial maps

If $a = [a_1, \ldots, a_r]^T$ is a column vector of integers and $\lambda = [\lambda_1, \ldots, \lambda_r]$ is a row vector with entries in $\mathbb{K}^*$ then λ^a denotes the scalar

$$\lambda^a = \lambda_1^{a_1} \cdots \lambda_r^{a_r}.$$

If $\lambda = [\lambda_1, \ldots, \lambda_r]$ is a row vector of r indeterminates, then λ^a can be understood as a monomial in the Laurent polynomial ring $\mathbb{K}[\lambda, \lambda^{-1}]$, a domain isomorphic to $\mathbb{K}[\lambda, \mu]/(\lambda_1\mu_1 - 1, \ldots, \lambda_r\mu_r - 1)$. We extend this notation to matrices: If A is an $r \times n$ matrix then λ^A is the row vector

$$\lambda^A = [\lambda^{A_{\cdot,1}}, \cdots, \lambda^{A_{\cdot,n}}]$$

where $A_{\cdot,1}, \ldots, A_{\cdot,n}$ are the n columns of A.

If $x = [x_1, \ldots, x_n]$ and $y = [y_1, \ldots, y_n]$ are two row vectors, we write $x \star y$ for the row vector obtained by component wise multiplication:

$$x \star y = [x_1y_1, \ldots, x_ny_n]$$

Proposition 3.1 *Suppose* A *and* B *are matrices of size* $r \times n$ *and* $n \times n$*, respectively, and that* λ *is a row vector with* r *components. Then*

(a) If $A = [A_{\mathfrak{i}}, A_{\mathfrak{n}}]$ *is a partition of the columns of* A*, then* $\lambda^A = [\lambda^{A_{\mathfrak{i}}}, \lambda^{A_{\mathfrak{n}}}]$,

(b) $\lambda^{AB} = (\lambda^A)^B$,

(c) $(y \star z)^A = y^A \star z^A$.

(d) $\lambda^{A+B} = \lambda^A \star \lambda^B$

Proof. Part (a) follows directly from the definition of λ^A. For part (b) we have for each component j, $1 \le j \le t$:

$$\begin{aligned} [(\lambda^A)^B]_j &= \textstyle\prod_{i=1}^n [\lambda^A]_i^{b_{ij}} = \prod_{i=1}^n \left(\prod_{\ell=1}^r \lambda_\ell^{a_{\ell i}} \right)^{b_{ij}} \\ &= \textstyle\prod_{\ell=1}^r \left(\prod_{i=1}^n \lambda_\ell^{a_{\ell i} b_{ij}}\right) \\ &= \textstyle\prod_{\ell=1}^r \left(\lambda_\ell^{\sum_{i=1}^n a_{\ell i} b_{ij}} \right) = [\lambda^{AB}]_j \,. \end{aligned}$$

For part (c) one simply notices that for each j we have

$$\begin{aligned} [(y\star z)^A]_j &= \textstyle\prod_i^r [y \star z]_i^{a_{i,j}} = \prod_i^r y_i^{a_{i,j}} \cdot z_i^{a_{i,j}} \\ &= [y^A]_j [z^A]_j = [y^A \star z^A]_j. \end{aligned}$$

The proof of (d) follows along the same lines. □

3.2 Scalings in matrix notation

The r-dimensional torus is the Abelian group $(\mathbb{K}^*)^r$. Its identity is $1_r = (1, \ldots, 1)$ and the group operation is componentwise multiplication, which we denoted $\star$.

Definition 3.2 *Let A be a $r \times n$ integer matrix: $A \in \mathbb{Z}^{r\times n}$. The associated* scaling *is the linear action of $T = (\mathbb{K}^*)^r$ on the affine space $\mathbb{K}^n$ given by*

$$\begin{array}{rcl} (\mathbb{K}^*)^r \times \mathbb{K}^n & \rightarrow & \mathbb{K}^n \\ (\lambda \;\;,\;\; z) & \rightarrow & \lambda^A \star z. \end{array} \qquad (6)$$

With the notations introduced above we have that

$$\lambda^A \star z = [\lambda^{A_{\cdot,1}} z_1, \ldots, \lambda^{A_{\cdot,n}} z_n]$$

with $A_{\cdot,1}, \ldots, A_{\cdot,n}$ being the n columns of A. Thus for each $j = 1, \ldots, n$ the action scales the j^{th} component z_j by the power product $\lambda_1^{a_{1,j}} \cdots \lambda_r^{a_{r,j}}$. The axioms for a group action are satisfied thanks to Proposition 3.1: $1_r \star z = z$ and $(\lambda \star \mu)^A \star z = \lambda^A \star (\mu^A \star z)$.

There is no loss of generality in assuming that A has full row rank. Indeed, we can view the scaling defined by A as a diagonal representation of $(\mathbb{K}^*)^r$ on the n dimensional space $\mathbb{K}^n$:

$$\begin{array}{rcl} (\mathbb{K}^*)^r & \rightarrow & \mathrm{D}_n \\ (\lambda_1, \ldots, \lambda_r) & \mapsto & \mathrm{diag}(\lambda^A) \end{array}$$

where D_n is the group of invertible diagonal matrices. This in turn can be factored by the group morphism from $(\mathbb{K}^*)^r$ to $(\mathbb{K}^*)^n$ defined by A. This is given explicitly by:

$$\rho(A): \begin{array}{rcl} (\mathbb{K}^*)^r & \rightarrow & (\mathbb{K}^*)^n \\ (\lambda_1, \ldots, \lambda_r) & \mapsto & \lambda^A \end{array}$$

Suppose now that $UA = \begin{bmatrix} B \\ 0 \end{bmatrix}$ is a *row* Hermite form for A with unimodular row multiplier U. Writing $U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}$ where $U_1 A = B$ is of row dimension d we have that $U_2 A = 0$. Then

$$\begin{array}{ccccc} (\mathbb{K}^*)^d \times (\mathbb{K}^*)^{r-d} & \xrightarrow{U} & (\mathbb{K}^*)^r & \xrightarrow{A} & (\mathbb{K}^*)^n \\ (\mu_1, \mu_2) & \mapsto & \mu_1^{U_1} \star \mu_2^{U_2} & \mapsto & (\mu_1^{U_1} \star \mu_2^{U_2})^A = \mu_1^B. \end{array}$$

Since U is unimodular, $\rho(U)$ is an isomorphism of groups and the image of $(\mathbb{K}^*)^r$ by $\rho(A)$ is equal to the image of $(\mathbb{K}^*)^d$ by $\rho(B)$.

4. RATIONAL INVARIANTS

Consider a full row rank matrix $A \in \mathbb{Z}^{r\times n}$ which defines an action of the torus $(\mathbb{K}^*)^r$ on $\mathbb{K}^n$. A rational invariant is an element f of $\mathbb{K}(z)$ such that $f(\lambda^A \star z) = f(z)$. Rational invariants form the subfield $\mathbb{K}(z)^A$ of $\mathbb{K}(z)$. In this section we show how a unimodular multiplier V, where $A \cdot V$ is the Hermite normal form, provides us with a complete description of the subfield of rational invariants. From V we shall extract

- $n-r$ generating rational invariants that are algebraically (and functionally) independent
- a simple rewriting of any (rational) invariant in terms of this generating set,
- a rational section to the orbits of the scaling.

We thus go much further than the group action transcription of the Buckingham π-theorem of dimensional analysis [2, 19]. This latter takes any basis of the nullspace of the matrix A and provides a set of *functionally* generating invariants, some of which could involve fractional powers. In the present approach, only integer powers are involved. This spares us the determination of proper domains of definition. Furthermore, the Buckingham π-theorem gives no indication on how to rewrite an invariant in terms of the generators produced. The rewriting we propose is a simple substitution. This is reminiscent of the *normalized invariants* appearing in [5, 8, 16] (or *replacement invariants* in [7]). We are also in a position to exhibit a rational section to the orbits of the scaling. The substitution is again rational: we do not introduce any algebraic functions as would generally be the case when choosing a (local) cross-section arbitrarily.

4.1 Generating and replacement invariants

A Laurent monomial z^v is a rational invariant if $(\lambda^A \star z)^v = z^v$ and therefore if and only if $Av = 0$. The following lemma shows that rational invariants of a scaling can be written as a rational function of invariant Laurent monomials.

Lemma 4.1 *Suppose $\frac{p}{q} \in \mathbb{K}(z)^A$, with $p, q \in \mathbb{K}[z]$ relatively prime. Then there exists $u \in \mathbb{Z}^n$ such that*

$$p(z) = \sum_{v \,\in\, \ker A \,\cap\, \mathbb{Z}^n} a_v\, z^{u+v} \quad \textit{and} \quad q(z) = \sum_{v \,\in\, \ker A \,\cap\, \mathbb{Z}^n} b_v\, z^{u+v}$$

where the families of coefficients, $(a_v)_v$ and $(b_v)_v$, have finite support.[1]

Proof. We take advantage of the more general fact that rational invariants of a linear action on $\mathbb{K}^n$ are quotients of semi-invariants (see for instance [21, Theorem 3.3]). Indeed, if p/q is a rational invariant, then we have

$$p(z)\, q(\lambda^A \star z) = p(\lambda^A \star z)\, q(z)$$

in $\mathbb{K}(\lambda)[z]$. As p and q are relatively prime, $p(z)$ divides $p(\lambda^A \star z)$ and, since these two polynomials have the same degree, there exists $\chi(\lambda) \in \mathbb{K}(\lambda)$ such that $p(\lambda^A \star z) = \chi(\lambda)\, p(z)$. It then also follows that $q(\lambda^A \star z) = \chi(\lambda)\, q(z)$.

Let us now look at the specific case of a scaling. Then

$$p(z) = \sum_{w \,\in\, \mathbb{Z}^n} a_w\, z^w \quad \Rightarrow \quad p(\lambda^A \star z) = \sum_{w \,\in\, \mathbb{Z}^n} a_w \lambda^{Aw}\, z^w.$$

For $p(\lambda^A \star z)$ to factor as $\chi(\lambda) p(z)$ we must have $Aw = Au$ for any two vectors $u, w \in \mathbb{Z}^n$ with a_v and a_u in the support of p. Let us fix u. Then $w - u \in \ker A$ and $\chi(\lambda) = \lambda^{Au}$. From the previous paragraph we have $\sum_{w\,\in\,\mathbb{Z}^n} b_w \lambda^{Aw}\, z^w = q(\lambda^A \star z) = \lambda^{Au} q(z) = \lambda^{Au} \sum_{w\,\in\,\mathbb{Z}^n} b_w\, z^w$. Thus $Au = Aw$ and therefore there exists $v \in \ker A \cap \mathbb{Z}^n$ such that $w = u + v$ for all w with b_w in the support of q. □

[1] In particular $a_v = 0$ (respectively $b_v = 0$) when $u + v \notin \mathbb{N}^n$.

We remark that one can prove Lemma 4.1 by specializing more general results on generating sets of rational invariants and the multiplicative group of invariant monomials [21]. Our proof has the advantage of being both simple and direct.

The set of rational functions on $\mathbb{K}^n$ that are invariant under a group action form a subfield of $\mathbb{K}(z)$ and, as such, it is a finitely generated field. In the case of a scaling the generators of this field can be constructed making use only of linear algebra and the representation of rational invariants given in Lemma 4.1.

Theorem 4.2 *Let $V = [\ V_{\mathfrak{i}},\ V_{\mathfrak{n}}\ ]$ and $W = \begin{bmatrix} W_{\mathfrak{u}} \\ W_{\mathfrak{d}} \end{bmatrix}$ be unimodular matrices of integers such that $AV = [\ H,\ 0\ ]$ is in column Hermite normal form and W is the inverse of V. Then the scaling defined by A has the following properties:*

- *(a) The $n-r$ components of $g = [z_1, \ldots, z_n]^{V_{\mathfrak{n}}}$ form a generating set of rational invariants;*
- *(b) Any rational invariant can be written in terms of the components of g by substituting $z = [z_1, \ldots, z_n]$ by the respective components of $g^{W_{\mathfrak{d}}}$.*

PROOF. Observe first that the components of g are invariants. Indeed the columns of $V_{\mathfrak{n}}$ span $\ker A$ and so $\left(\lambda^A \star z\right)^{V_{\mathfrak{n}}} = \lambda^{AV_{\mathfrak{n}}} \star z^{V_{\mathfrak{n}}} = z^{V_{\mathfrak{n}}}$. We shall prove that any rational invariant can be rewritten in terms of these components.

Since V and W are inverses of each other we have $I_n = V_{\mathfrak{i}}W_{\mathfrak{u}} + V_{\mathfrak{n}}W_{\mathfrak{d}}$. Thus $z = z^{V_{\mathfrak{i}}W_{\mathfrak{u}}+V_{\mathfrak{n}}W_{\mathfrak{d}}}$, where $z = [z_1, \ldots, z_n]$, the vector of degree 1 monomials. More generally, for any $v \in \mathbb{Z}^n$, $z^v = z^{(V_{\mathfrak{i}}W_{\mathfrak{u}}+V_{\mathfrak{n}}W_{\mathfrak{d}})v}$. If now $v \in \ker A \cap \mathbb{Z}^n$ then $z^v = z^{V_n W_{\mathfrak{d}} v} = g^{W_d v}$ since $\ker A \subset \ker W_{\mathfrak{u}}$.

The representation given in Lemma 4.1 implies that any $\frac{p}{q} \in \mathbb{K}(z)^T$, with $p, q \in \mathbb{K}[z]$ relatively prime, has the form

$$p(z) = \sum_{v\,\in\,\ker A\,\cap\,\mathbb{Z}^n} a_v\, z^{u+v} \quad \text{and} \quad q(z) = \sum_{v\,\in\,\ker A\,\cap\,\mathbb{Z}^n} b_v\, z^{u+v}$$

for some $u \in \mathbb{Z}^n$. As elements of $\mathbb{K}(z)$, we can rewrite these as

$$\begin{array}{rcl} p(z) & = & z^u \sum_{v\in\ker A\,\cap\,\mathbb{Z}^n} a_v \left(z^{V_{\mathfrak{n}}W_{\mathfrak{d}}}\right)^v \\ q(z) & = & z^u \sum_{v\,\in\,\ker A\,\cap\,\mathbb{Z}^n} b_v \left(z^{V_{\mathfrak{n}}W_{\mathfrak{d}}}\right)^v \end{array}$$

and so

$$\frac{p(z)}{q(z)} = \frac{p\left(z^{V_{\mathfrak{n}}W_{\mathfrak{d}}}\right)}{q\left(z^{V_{\mathfrak{n}}W_{\mathfrak{d}}}\right)} = \frac{p\left(g^{W_{\mathfrak{d}}}\right)}{q\left(g^{W_{\mathfrak{d}}}\right)}.$$

□

Both V and W are needed for computing invariants and rewrite rules. Since a matrix V is produced from column operations converting A to Hermite normal form, the W matrix can be computed simultaneously with minimal cost by the inverse column operations.

Example 4.3 *Consider the scaling defined by $A = \begin{bmatrix} 2 & 3 \end{bmatrix}$. A unimodular multiplier for its Hermite normal form is*

$$V = \begin{bmatrix} -1 & 3 \\ 1 & -2 \end{bmatrix} \quad \textit{with inverse} \quad W = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}.$$

It follows that $g = \frac{x^3}{y^2}$ is a generating invariant. Any other rational invariant can be written in terms of g with the substitution $x \mapsto g$, $y \mapsto g$.

Example 4.4 *Consider the 2×5 matrix A given by*

$$A = \begin{bmatrix} 6 & 0 & -4 & 1 & 3 \\ 0 & 3 & 1 & -4 & 3 \end{bmatrix}.$$

If $z = (z_1, z_2, z_3, z_4, z_5)$ and $\lambda = (\mu, \nu)$ then the group action defined by A is given by

$$\lambda^A \star z = (\ \mu^6 z_1,\ \nu^3 z_2,\ \frac{\nu}{\mu^4} z_3,\ \frac{\mu}{\nu^4} z_4,\ \mu^3\nu^3 z_5).$$

The column Hermite normal form for A is given by

$$[H, 0] = \begin{bmatrix} 3 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

and the normal unimodular multiplier and its inverse are

$$V = \left[\begin{array}{cc|ccc} 1 & 1 & 2 & 1 & 0 \\ 1 & 0 & -1 & 2 & 0 \\ 1 & 1 & 3 & 2 & 1 \\ 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right],\quad W = \left[\begin{array}{ccccc} 2 & -2 & -2 & 3 & -1 \\ 0 & 3 & 1 & -4 & 3 \\ \hline 0 & -1 & 0 & 1 & -1 \\ -1 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

A generating set of invariants is given by the components

$$(g_1, g_2, g_3) = z^{V_{\mathfrak{n}}} = \left(\frac{z_1^2 z_3^3}{z_2},\ z_1 z_2^2 z_3^2 z_4^2,\ z_3 z_4 z_5 \right)$$

while the rewrite rules are given by

$$(z_1, z_2, z_3, z_4, z_5) \to g^{W_{\mathfrak{d}}} = \left(\frac{1}{g_2},\ \frac{g_2}{g_1},\ g_2,\ \frac{g_1}{g_2},\ \frac{g_3}{g_1} \right).$$

4.2 Rational section to the orbits

The fact that we can rewrite any invariant in terms of the generating set by a simple substitution actually reflects the existence and intrinsic use of a rational section [7, 8]. And indeed, any unimodular multiplier for the Hermite normal form provides a rational section. The simplest rational sections are uncovered by the normal unimodular multipliers of Proposition 2.3.

An irreducible variety $\mathcal{P} \subset \mathbb{K}^n$ is a *rational section* for the rational action of an affine algebraic group if there exists a nonempty Zariski open subset $\mathcal{Z} \subset \mathbb{K}^n$ such that any orbit of the induced action on $\mathcal{Z}$ intersects $\mathcal{P}$ at exactly one point [21, Section 2.5].

Every vector $a \in \mathbb{Z}^r$ can be uniquely written as $a = a^+ - a^-$ where a^+ and a^- are nonnegative and have disjoint support. Their components are:

$$[a^+]_i = \begin{cases} a_i & \text{if } a_i \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad [a^-]_i = \begin{cases} a_i & \text{if } a_i \leq 0 \\ 0 & \text{otherwise.} \end{cases}$$

This can be extended to $r \times n$ matrices by

$$A^+ = [(A_{.,1})^+, \cdots, (A_{.,n})^+] \text{ and } A^- = [(A_{.,1})^-, \cdots, (A_{.,n})^-].$$

Theorem 4.5 *With the hypotheses of Theorem 4.2, the variety $\mathcal{P}$ of $(z^{V_{\mathfrak{i}}^+} - z^{V_{\mathfrak{i}}^-}) : z^\infty$ is a rational section for the scaling defined by A. The intersection of the orbit of a point $z \in (\mathbb{K}^*)^n$ with this section is the point $z^{V_{\mathfrak{n}}W_{\mathfrak{d}}}$.*

PROOF. The matrix $W_\mathfrak{d}$ is full row rank and $W_\mathfrak{d}\cdot[V_\mathfrak{n}, V_\mathfrak{i}] = [I_{n-r}, 0]$. By Lemma 2.2 the columns of $V_\mathfrak{i}$ span the lattice kernel of $W_\mathfrak{d}$. Thus the kernel of

$$\begin{array}{ccc} \mathbb{K}[z] & \rightarrow & \mathbb{K}[x, x^{-1}] \\ z & \mapsto & x^{W_\mathfrak{d}}. \end{array}$$

is the prime (toric) ideal $P = \left(z^{V_\mathfrak{i}^+} - z^{V_\mathfrak{i}^-}\right) : (z_1 \dots z_n)^\infty$ of dimension r [26, Lemma 4.1, 4.2 and 12.2].

Assume $z \in (\mathbb{K}^*)^n$. For $\tilde{z} = \lambda^A \star z$ to be on the variety $\mathcal{P}$ of P the components of $\tilde{z}^{V_\mathfrak{i}}$ need to all be equal to 1. Thus $\lambda^{AV_\mathfrak{i}} = z^{-V_\mathfrak{i}}$, that is, $\lambda^H = z^{-V_\mathfrak{i}}$. Because of the triangular structure of H we can always find $\lambda \in (\mathbb{K}^*)^r$ satisfying this equation. For any such λ we then have $\tilde{z} = \left(\lambda^A \star z\right)^{V_\mathfrak{i} W_\mathfrak{u} + V_\mathfrak{n} W_\mathfrak{d}}$ since $V_\mathfrak{i} W_\mathfrak{u} + V_\mathfrak{n} W_\mathfrak{d} = I_n$ and so $\tilde{z} = \lambda^{HW_\mathfrak{u}} \star z^{V_\mathfrak{i} W_\mathfrak{u} + V_\mathfrak{n} W_\mathfrak{d}} = z^{-V_\mathfrak{i} W_\mathfrak{u}} \star z^{V_\mathfrak{i} W_\mathfrak{u} + V_\mathfrak{n} W_\mathfrak{d}} = z^{V_\mathfrak{n} W_\mathfrak{d}}$ by Proposition 3.1. Thus the intersection of the orbit of z with the variety of P exists, is unique and equal to $z^{V_\mathfrak{n} W_\mathfrak{d}}$. □

From this description we deduce that the invariants $z^{V_\mathfrak{n} W_\mathfrak{d}}$ are actually the *normalized invariants* as defined in [8]. As such the rewriting of Theorem 4.2 applies to the more general class of smooth invariants. Furthermore, if the Hermite form of A is I_r there is a global *moving frame* for the group action and $z^{V_\mathfrak{n} W_\mathfrak{d}}$ correspond to the normalized invariants as originally defined in [5]. This moving frame is the equivariant map $(\mathbb{K}^*)^n \rightarrow (\mathbb{K}^*)^r$ given by $z \mapsto z^{-V_\mathfrak{i}}$.

Example 4.6 *Consider the scaling given by*

$$(z_1, z_2, z_3, z_4, z_5) \rightarrow \left(\frac{\eta}{\nu^3} z_1, \frac{\eta}{\mu} z_2, \eta z_3, \frac{\nu}{\eta\mu} z_4, \frac{\eta\nu}{\mu} z_5\right)$$

an example used to illustrate dimensional analysis in [19]. In this case the matrix of exponents is

$$A = \left[\begin{array}{ccccc} -3 & 1 & 1 & -1 & 1 \\ 0 & -1 & 0 & -1 & -2 \\ 1 & 0 & 0 & 1 & 1 \end{array}\right].$$

The normal unimodular multiplier and its inverse are

$$V = \left[\begin{array}{ccc|cc} 0 & 0 & 1 & -1 & -1 \\ 0 & -1 & 0 & -1 & -2 \\ 1 & 1 & 3 & -1 & -2 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right], W = \left[\begin{array}{ccccc} -3 & 1 & 1 & -1 & 1 \\ 0 & -1 & 0 & -1 & -2 \\ 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

Thus the rewrite rules are simply $z \rightarrow g^{W_\mathfrak{d}} = (1, 1, 1, g_1, g_2)$. By Theorem 4.5 the associated rational section is the variety $(z_3 - 1, z_3 - z_2, z_1 z_3^3 - 1) : z^\infty$. Simple combinations of the ideal generators show that this ideal is equal to $(z_1 - 1, z_2 - 1, z_3 - 1)$.

Example 4.3 illustrates a case where things are particularly simple: The r first components of the rewrite tuple $g^{W_\mathfrak{d}}$ are equal to 1. This comes from the lower left $(n - r) \times r$ block of V, and therefore of W, being zero. When such a situation is possible the normal unimodular multiplier and its inverse are

$$V = \left[\begin{array}{cc} V_\mathfrak{i}^* & V_\mathfrak{n}^* \\ 0 & I_{n-r} \end{array}\right] \text{ and } W = \left[\begin{array}{cc} V_\mathfrak{i}^{*-1} & -V_\mathfrak{i}^{*-1} V_\mathfrak{n}^* \\ 0 & I_{n-r} \end{array}\right].$$

Indeed, the diagonal blocks of V are then unimodular. The Hermite normal form of $V_\mathfrak{n}$ has the identity matrix as bottom $n - r$ rows.

Proposition 4.7 *If the canonical unimodular multiplier V of A for its Hermite normal form is*

$$V = \left[\begin{array}{cc} V_\mathfrak{i}^* & V_\mathfrak{n}^* \\ 0 & I_{n-r} \end{array}\right] \quad (7)$$

then the variety of $(z_1 - 1, \dots, z_r - 1)$ is a rational section to the scaling defined by A. There are then $n - r$ generating invariants $g_{r+1}^*, \dots, g_n^*$ such that any other rational invariants can be written in terms of these invariants using the substitution $(z_1, \dots, z_n) \mapsto (1, \dots, 1, g_{r+1}^*, \dots, g_n^*)$.

The proof proceeds by first noting that $V_\mathfrak{i}^*$ is unimodular and so one can take the power $(V_\mathfrak{i}^*)^{-1}$ of $(z^{V_\mathfrak{i}^+} - z^{V_\mathfrak{i}^-})$. The components then belong to the ideal generated by the components of $(z^{V_\mathfrak{i}^+} - z^{V_\mathfrak{i}^-})$ which factors as a product of $(z_1 - 1, \dots, z_r - 1)$ with a monomial in z. This then implies that $(1, \dots, 1, g_{r+1}^*, \dots, g_n^*) = z^{V_\mathfrak{n} \cdot W_\mathfrak{d}} = (1_r, z^{V_\mathfrak{n}}) = (1_r, g)$.

An equally simple section can be chosen when the pivot rows of $V_\mathfrak{n}$ are the rows of an $(n-r)$-identity matrix. In this case we can recover the above situation by permuting the columns of A and therefore the order of the original variables.

5. REDUCING POLYNOMIAL SYSTEMS

If the solution set of a polynomial system of equations is invariant under a group action, then there is an equivalent system given in terms of invariants of this group action [19]. The equivalent system written in terms of a generating set of invariants is the *reduced system*. A further problem is to recover the solutions of the original system from the solutions of the reduced system.

In this section we show how to fully work out a symmetry reduction for a scaling symmetry. If the scaling symmetry is r-dimensional, then the reduced system has r fewer variables. In addition, we show how to retrieve all *toric* solutions of the original system from the toric solutions of the reduced system. We shall indeed discount the solutions for which there is a zero component. This is a relevant case. For instance, in a chemical reaction or a population dynamics model we look for the equilibria where no species disappears.

We consider a set of equations $p_1(z) = 0, \quad \dots, \quad p_m(z) = 0$ where $p_1, \dots, p_m$ are in $\mathbb{K}[z] = \mathbb{K}[z_1, \dots, z_n]$ or even in the Laurent polynomial ring $\mathbb{K}[z, z^{-1}]$ since we are concerned with solutions in $(\mathbb{K}^*)^n$. For convenience we introduce the map $p = (p_1, \dots, p_m)$ and write the system of equations as $p(z) = 0$.

Definition 5.1 *The matrix $A \in \mathbb{Z}^{r \times n}$ defines a scaling symmetry for the polynomial system $p(z) = 0$ if, for a given $z \in (\mathbb{K}^*)^n$, we have*

$$p(z) = 0 \ \Rightarrow \ p(\lambda^A \star z) = 0, \quad \forall \lambda \in (\mathbb{K}^*)^r. \quad (8)$$

In the following we suppose that $A \in \mathbb{Z}^{r \times n}$ defines a scaling symmetry for the polynomial system $p(z) = 0$. A sufficient, but not necessary, condition for that is that the p_i are invariants or semi-invariants[2]. Then V is a unimodular multiplier such that $A \cdot V$ is the Hermite normal form of A, and W is the inverse of V. The *reduction* of $p \in \mathbb{K}[z, z^{-1}]$ associated to a choice of V is a Laurent polynomial q in $n-r$ variables $(y_1, \ldots, y_{n-r})$ defined by $q(y) = f\left(y^{W\mathfrak{d}}\right)$. From Theorem 4.2 we know that if p is invariant then $p(z) = q(g)$ where $g = z^{V_\mathfrak{n}}$. However we do not restrict reduction to invariants.

Proposition 5.2 *Let $q_1, \ldots, q_m$ in $\mathbb{K}[y, y^{-1}]$ be defined as $q_i(y) = p_i\left(y^{W\mathfrak{d}}\right)$. If $y \in (\mathbb{K}^*)^{n-r}$ is a solution of $q(y) = 0$, then for all $\lambda \in (\mathbb{K}^*)^r$, $\lambda^A \star y^{W_\mathfrak{d}}$ is a solution of $p(z) = 0$.*

The Laurent polynomials $q_1, \ldots, q_m$ form the *reduced system*. This reduced system has r fewer variables than the original system. As described in the above proposition, any point on its solution set provides a parameterized r-dimensional set of solutions for the original system. Proposition 5.2 is an immediate result of the symmetry condition (8). The following result is a stronger assertion: any toric solution of the original system can be obtained that way.

Theorem 5.3 *Assume that $A \in \mathbb{Z}^{r \times n}$ defines a scaling symmetry for the polynomial system $p(z) = 0$ and that $q(y) = 0$ is the reduced system. Then for any $z \in (\mathbb{K}^*)^n$ satisfying $p(z) = 0$ there exists $\lambda \in (\mathbb{K}^*)^r$ and $y \in (\mathbb{K}^*)^{n-r}$ such that $q(y) = 0$ and $z = \lambda^A \star y^{W_\mathfrak{d}}$.*

Proof. Assume $z \in (\mathbb{K}^*)^n$ satisfies $p(z) = 0$. Since H is triangular and nonsingular, there exists $\lambda \in (\mathbb{K}^*)^r$ such that $\lambda^H = z^{-V_\mathfrak{i}}$. Set $y = z^{V_\mathfrak{n}}$. Since $\lambda^{[H,0]} = \left(z^{-V_\mathfrak{i}}, 1_{n-r}\right)$ we have

$$\left(\lambda^A \star z\right)^{[V_\mathfrak{i}, V_\mathfrak{n}]} = \lambda^{[H,0]} \star \left(z^{V_\mathfrak{i}}, z^{V_\mathfrak{n}}\right) = (1_r, y).$$

Taking both sides of the above equality to the power W gives

$$\lambda^A \star z = \left(\lambda^A \star z\right)^{V \cdot W} = (1_r, y)^{\left[\begin{array}{c} W_\mathfrak{u} \\ W_\mathfrak{d} \end{array}\right]} = y^{W_\mathfrak{d}}.$$

By the symmetry hypothesis $p\left(y^{W_\mathfrak{d}}\right) = p(\lambda^A \star z) = 0$. Thus $q(y) = 0$. □

There is a geometric interpretation for the above approach that stems out of the work of [5, 7, 8]. Namely, the solution set of the reduced system describes the projection, along the orbits, of the original solution set on the section $z^{V_\mathfrak{i}} = 1$. From the above proof it is clear that the group element $\lambda \in (\mathbb{K}^*)^r$ providing the link between the solution of the original system and the solution of the reduced system is unique if and only if the Hermite normal form is the identity.

Example 5.4 *Consider the system of polynomial equations*

$$\begin{array}{rcl} z_2 {z_4}^2 - z_1 & = & 0 \\ z_1 z_3 - z_2 & = & 0. \end{array}$$

presented in [14, Example 3.14]. On one hand we can look for the solutions that have a zero component. They are part of the two-parameter family of solutions given by $(0, 0, \alpha, \beta)$. The scaling symmetry for this system determined by [9, Section 5] is

$$A = \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 \end{array}\right].$$

A unimodular multiplier V, and its inverse W, to obtain the Hermite normal form of A are

$$V = \left[\begin{array}{cc|cc} 1 & -1 & 1 & -1 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{array}\right], \quad W = \left[\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 \\ \hline 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \end{array}\right].$$

The reduced system is thus obtained by substituting (z_1, z_2, z_3, z_4) by $(y_1, y_2)^{W_\mathfrak{d}} = (1, \frac{1}{y_2}, \frac{y_1}{y_2}, y_2)$:

$$\left.\begin{array}{rcl} \frac{1}{y_2} y_2^2 - 1 & = & 0 \\ \frac{y_1}{y_2} - \frac{1}{y_2} & = & 0 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcl} y_1 & = & 1 \\ y_2 & = & 1. \end{array}\right.$$

The latter system has a solution set consisting of a single point. It provides a two parameter solution to the original system: $\lambda^A \star (1,1)^{W_\mathfrak{d}} = (\lambda_1, \lambda_1\lambda_2^2, \lambda_2^2, \lambda_2^{-1})$. By Theorem 5.3, any solution, without zero component, of the original system is obtained in this way. Since $A \cdot V = \left[\begin{array}{cc} I_2 & 0 \end{array}\right]$, the pair (λ_1, λ_2) providing the given solution is unique. It can be read from the columns of $V_\mathfrak{i}$: $(\lambda_1, \lambda_2) = \left(\frac{1}{z_1}, \frac{z_1}{z_2 z_4}\right)$.

For the geometric interpretation note that the underlying rational section is the variety of $(z_1 - 1, z_2 z_4 - z_1)$. One can check that the intersection of the solution set of the original system with this section is $(1,1)^{W_\mathfrak{d}} = (1,1,1,1)$. Any element in the orbit of this point solves the original system.

The semi-rectified *system obtained in [14] is different than our reduced system. The process described there introduces square roots and the semi-rectified system has two solutions. This owes to the row-echelon form used. In our approach we get a clear connection between the toric solutions of the reduced system and of the original system. As we are free of fractional powers, we avoid having to pay attention to the sign of the components in the solution set.*

Example 5.5 *Consider the polynomial system of 3 equations in 5 variables given by*

$$\begin{array}{rcl} z_1^4 z_3^6 - 5 z_1^2 z_2 z_3^3 + 6 z_2^2 & = & 0 \\ z_1^2 z_2^5 z_3^4 z_4^4 - 2 z_1^3 z_2^2 z_3^5 z_4^2 - z_1^2 z_3^3 + z_2 & = & 0 \\ z_1 z_2^3 z_3^4 z_4^3 z_5 - z_1^2 z_3^3 - z_2 & = & 0. \end{array}$$

On one hand there is a three-parameter family of solutions given by $(0, 0, \alpha, \beta, \gamma)$. On the other hand, a symmetry of this system is given by the 2×5 matrix A of Example 4.4. The reduced system

$$\begin{array}{rcl} y_1^2 - 5 y_1 + 6 & = & 0 \\ y_2^2 - 2 y_1 y_2 + y_1 + 1 & = & 0 \\ y_2 y_3 - y_1 - 1 & = & 0. \end{array}$$

is obtained with the substitution:

$$(z_1, z_2, z_3, z_4, z_5) \mapsto \left(\frac{1}{y_2}, \frac{y_2}{y_1}, y_2, \frac{y_1}{y_2}, \frac{y_3}{y_1}\right).$$

[2]Given p, [9, Section 5] provides an algorithm to determine a maximal scaling such that the p_i are semi-invariants.

The solution set of the above reduced system consists of the 4 *points* $(2, 1, 3)$, $(2, 3, 1)$, $(3, 3+\sqrt{5}, 3-\sqrt{5})$ *and* $(3, 3-\sqrt{5}, 3+\sqrt{5})$. *In this case the underlying rational section is the variety of* $(z_1z_2z_3z_4-1, z_2z_4-1)$. *The intersection of the solution set of the original system are the four points* $(2, 1, 3)^{W_\mathfrak{d}} = (1, \frac{1}{2}, 1, 2, \frac{3}{2})$, $(2, 3, 1)^{W_\mathfrak{d}} = (\frac{1}{3}, 3, 3, \frac{1}{3}, \frac{1}{2})$, $(3, 3+\sqrt{5}, 3-\sqrt{5})^{W_\mathfrak{d}}$ *and* $(3, 3-\sqrt{5}, 3+\sqrt{5})^{W_\mathfrak{d}}$. *Any element in the orbits of these points is a solution of the original system. We thus have four parameterized two dimensional solution subsets. For example,* $\lambda^A \star (2, 1, 3)^{W_\mathfrak{d}} = (\mu^6, \frac{\nu^3}{2}, \frac{\nu}{\mu^4}, \frac{2\nu}{\mu^4}, \frac{3\mu^3\nu^3}{2})$ *is a parameterized two-dimensional subset of solutions. By Theorem 5.3, all solutions, without zero component, of the original system are obtained in this way.*

6. CONCLUSION

In this paper we have made use of the Hermite Normal Form of the matrix of exponents of a scaling symmetry. Invariants, rewrite rules and rational section for a scaling are all determined from an associated unimodular multiplier and its inverse. We have also illustrated how scaling can be used to reduce polynomial systems of equations. All the algorithms in this paper have been implemented in the computer algebra system Maple.

There are a number of research topics that follow from our work. The Hermite Normal Form is not the only rank-revealing or normalizing transformation of an integer matrix. Other possibilities include using the Smith Normal Form of the scaling matrix or lattice reduction basis (i.e. LLL) for the normal unimodular multiplier. We are interested in the invariants, rewrite rules and sections that result from using these alternate forms, in particular seeing when these are simpler than those that result from the use of the Hermite form.

We have shown how to reduce polynomial systems of equations by scaling symmetries. A complete scheme for scaling symmetry reduction of dynamical systems is also available in [9]. This has applications to parameter reduction in biological and physical modeling. We expect to report on the reduction of other significant classes of differential systems in future publications.

7. REFERENCES

[1] B. Beckermann, G. Labahn, and G. Villard. Normal forms for general polynomial matrices. *Journal of Symbolic Computation*, 41(6):708–737, 2006.

[2] G. Birkhoff. *Hydrodynamics: A study in logic, fact and similitude.* Princeton Univ. Press, 1960.

[3] P. Bridgman. *Dimensional Analysis.* Yale Univ. Press, 1931.

[4] H. Cohen. *A course in computational algebraic number theory.* Springer-Verlag, 1993.

[5] M. Fels and P. Olver. Moving coframes. ii. Regularization and theoretical foundations. *Acta Appl. Math.*, 55(2):127–208, 1999.

[6] G. Havas, B. Majewski, and K. Matthews. Extended gcd and Hermite normal form algorithms via lattice basis reduction. *Experimental Mathematics*, 7(2), 1998.

[7] E. Hubert and I. Kogan. Rational invariants of a group action. Construction and rewriting. *Journal of Symbolic Computation*, 42(1-2):203–217, 2007.

[8] E. Hubert and I. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4):345–383, 2007.

[9] E. Hubert and G. Labahn. Scaling invariants and symmetry reduction of dynamical systems. `http://hal.inria.fr/hal-00668882`, 2012.

[10] E. Hubert and A. Sedoglavic. Polynomial Time Nondimensionalisation of Ordinary Differential Equations via their Lie Point Symmetries, 2006.

[11] H. E. Huntley. *Dimensional Analysis.* Dover Publications, New York, 1967.

[12] Y. Ishida. Formula processing on physical systems. *Complex Systems*, 11(2):141–160, 1997.

[13] R. Khanin. Dimensional Analysis in Computer Algebra. In *Proceedings of ISSAC'01*, pages 201–208. ACM press, 2001.

[14] F. Lemaire and A. Ürgüplü. A method for semi-rectifying algebraic and differential systems using scaling type Lie point symmetries with linear algebra. In *Proceedings of ISSAC'10*, pages 85–92. ACM press, 2010.

[15] C. Lin and L. Segel. *Mathematics applied to deterministic problems in the natural sciences.* Society for Industrial and Applied Mathematics, 1988.

[16] E. Mansfield. *A Practical Guide to the Invariant Calculus.* Cambridge University Press, 2010.

[17] J. Müller-Quade and T. Beth. Calculating generators for invariant fields of linear algebraic groups. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 1719 of *LNCS.* Springer, 1999.

[18] J. D. Murray. *Mathematical Biology*, volume 17 of *Interdisciplinary Applied Mathematics.* Springer, 2002.

[19] P. J. Olver. *Applications of Lie Groups to Differential Equations.* Number 107 in Graduate texts in Mathematics. Springer-Verlag, New York, 1986.

[20] A. Parshin and I. Shafarevich, editors. *Algebraic Geometry. IV*, volume 55 of *Encyclopaedia of Mathematical Sciences.* Springer-Verlag, 1994.

[21] V. L. Popov and E. B. Vinberg. Invariant Theory. In *Algebraic geometry. IV*, Encyclopaedia of Mathematical Sciences. Springer-Verlag, 1994.

[22] A. Schrijver. *Theory of Linear and Integer Programming.* Wiley, 1986.

[23] A. Sedoglavic. Reduction of algebraic parametric systems by rectification of their affine expanded lie symmetries. In *Algebraic Biology*, volume 4545 of *LNCS.* Springer, 2007.

[24] A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Department of Computer Science, Swiss Federal Institute of Technology—ETH, 2000.

[25] A. Storjohann and G. Labahn. Asymptotically fast computation of Hermite Normal Forms of integer matrices. In *Proceedings of ISSAC'96*, pages 259–266. ACM press, 1996.

[26] B. Sturmfels. *Gröbner bases and convex polytopes.* American Mathematical Society, Providence, RI, 1996.