# SAGBI BASES FOR RINGS OF INVARIANT LAURENT POLYNOMIALS 

ALEXANDER DUNCAN AND ZINOVY REICHSTEIN

(Communicated by Martin Lorenz)


#### Abstract

Let $k$ be a field, let $L_{n}=k\left[x_{1}^{ \pm 1}, \ldots, x_{n}^{ \pm 1}\right]$ be the Laurent polynomial ring in $n$ variables and let $G$ be a finite group of $k$-algebra automorphisms of $L_{n}$. We give a necessary and sufficient condition for the ring of invariants $L_{n}^{G}$ to have a SAGBI basis. We show that if this condition is satisfied, then $L_{n}^{G}$ has a SAGBI basis relative to any choice of coordinates in $L_{n}$ and any term order.


## 1. Introduction

Let $k$ be a base field and let $P_{n}=k\left[x_{1}, \ldots, x_{n}\right]$ be the polynomial algebra in $n$ variables. Recall that the initial exponent $\mathbf{i n}(f)$ of $f \in P_{n} \backslash\{0\}$ is defined as the lexicographically largest $\left(a_{1}, \ldots, a_{n}\right) \in \mathbb{N}^{n}$ such that $x_{1}^{a_{1}} \ldots x_{n}^{a_{n}}$ occurs in $f$ with a non-zero coefficient. Note that $\mathbb{N}=\mathbb{Z}_{\geq 0}$. If $R$ is a $k$-subalgebra of $P_{n}$, then we define the semigroup of initial exponents of $R$ as

$$
\begin{equation*}
\operatorname{In}(R)=\{\operatorname{in}(f): 0 \neq f \in R\} \tag{1}
\end{equation*}
$$

A SAGBI basis for $R$ is a finite collection of non-zero elements $p_{1}, \ldots, p_{m} \in R$ such that $\operatorname{in}\left(p_{1}\right), \ldots, \operatorname{in}\left(p_{m}\right)$ generate $\operatorname{In}(R)$ as an additive semigroup. If $p_{1}, \ldots, p_{m}$ form a SAGBI basis for $R$, then these elements generate $R$ as a $k$-algebra. Moreover, an explicit representation of an element $f \in R$ as a polynomial in $p_{1}, \ldots, p_{m}$ can be found quickly and efficiently by using the subduction algorithm as follows. Choose a product $p_{1}^{a_{1}} \cdots p_{m}^{a_{m}}$, where each $a_{i} \in \mathbb{N}$ and $\operatorname{in}(f)=a_{1} \operatorname{in}\left(p_{1}\right)+\cdots+a_{m} \operatorname{in}\left(p_{m}\right)$. By selecting $\lambda \in k$ so as to cancel the leading term of $f$, we can ensure that $\operatorname{in}\left(f-\lambda p_{1}^{a_{1}} \cdots p_{m}^{a_{m}}\right)$ is strictly lexicographically smaller than $\operatorname{in}(f)$. We will write $\operatorname{in}(f) \succ \operatorname{in}\left(f_{1}\right)$, where $f_{1}=f-\lambda p_{1}^{a_{1}} \cdots p_{m}^{a_{m}}$. If $f_{1} \neq 0$, we can repeat this process on $f_{1}$ to get $f_{2}$ and so on. As a result we obtain a sequence $f=f_{0}, f_{1}, f_{2}, \ldots$, such that

$$
\begin{equation*}
\operatorname{in}\left(f_{0}\right) \succ \operatorname{in}\left(f_{1}\right) \succ \operatorname{in}\left(f_{2}\right) \succ \ldots \tag{2}
\end{equation*}
$$

[^0]Any lexicographically decreasing sequence in $\mathbb{N}^{n}$ has to terminate. Hence, $f_{i}=0$ for some $i \in \mathbb{N}$. In other words, the algorithm will terminate after $i$ steps and will yield a desired expression for $f$ as a polynomial in $p_{1}, \ldots, p_{m}$.

The reader will undoubtedly notice a strong resemblance between a SAGBI basis for a subalgebra of $P_{n}$ and a Gröbner basis for an ideal of $P_{n}$. In fact, the word "SAGBI", introduced by Robbiano and Sweedler in 9, is an acronym for "Subalgebra Analog to Gröbner Basis for Ideals". Note, however, that unlike Gröbner bases, SAGBI bases do not always exist. The question of finding necessary and sufficient conditions for a subalgebra $R \subset P_{n}$ to have a SAGBI basis is an important open problem; see, e.g., [10].

One reason this problem is so difficult is that the answer depends on the choice of the generators $x_{1}, \ldots, x_{n}$ for $P_{n}$, which is not intrinsic to the embedding $R \hookrightarrow P_{n}$. In other words, suppose $g: P_{n} \rightarrow P_{n}$ is a $k$-algebra automorphism and $y_{i}=g\left(x_{i}\right)$ for $i=1, \ldots, n$. We will refer to $y_{1}, \ldots, y_{n}$ as another choice of coordinates in $P_{n}$. Writing a non-zero element $f \in P_{n}$ as a polynomial in $y_{1}, \ldots, y_{n}$, we obtain a new initial exponent $\operatorname{in}_{y}(f)$ and a new semigroup of initial exponents $\operatorname{In}_{y}(R)=$ $\left\{\operatorname{in}_{y}(f) \mid 0 \neq f \in R\right\}$. In this situation it may happen that $\operatorname{In}(R)$ is a finitely generated semigroup and $\operatorname{In}_{y}(R)$ is not; see, e.g., 5. Equivalently, $g^{-1}(R)$ may have a SAGBI basis (relative to $x_{1}, \ldots, x_{n}$ ) even if $R$ does not.

The dependence on the choice of coordinates is lessened (but not entirely eliminated) if we replace the polynomial ring $P_{n}=k\left[x_{1}, \ldots, x_{n}\right]$ by the ring $L_{n}=$ $k\left[x_{1}^{ \pm 1}, \ldots, x_{n}^{ \pm 1}\right]$ of Laurent polynomials for the simple reason that the automorphism group $\operatorname{Aut}\left(L_{n}\right)$ is much "smaller" and better understood than $\operatorname{Aut}\left(P_{n}\right)$. Let $R$ be a $k$-subalgebra of $L_{n}$. The initial exponent $\operatorname{in}(f)$ is now an element of $\mathbb{Z}^{n}$, and $\operatorname{In}(R)$ is a subsemigroup of $\mathbb{Z}^{n}$. The subduction algorithm is defined in the same way as before. The only difference is that the lexicographically decreasing sequence (2) in $\mathbb{Z}^{n}$ is no longer guaranteed to terminate. For this reason the definition of a SAGBI basis is modified in this setting to require the termination of the subduction algorithm; cf. [8. That is, $p_{1}, \ldots, p_{m} \in R \backslash\{0\}$ are said to form a SAGBI basis for a $k$-subalgebra $R \subset L_{n}$ if $\operatorname{in}\left(p_{1}\right), \ldots, \operatorname{in}\left(p_{m}\right)$ generate $\operatorname{In}(R)$ and the subduction algorithm terminates for all $f \in R$ regardless of the particular choice of product $p_{1}^{a_{1}} \cdots p_{m}^{a_{m}}$ used at each step.

Before proceeding to state our main result, we briefly recall that $\operatorname{Aut}\left(L_{n}\right)$ is the semidirect product $\mathbb{G}_{m}^{n} \rtimes \mathrm{GL}_{n}(\mathbb{Z})$; see, e.g., [7] p. 65]. Here we identify an element $\left(t_{1}, \ldots, t_{n}\right) \in \mathbb{G}_{m}^{n}$ with the scaling automorphism of $L_{n}$, taking each $x_{i}$ to $t_{i} x_{i}$, and an element $g \in \mathrm{GL}_{n}(\mathbb{Z})$ with the multiplicative automorphism taking each $x^{\mathbf{a}}=x_{1}^{a_{1}} \ldots x_{n}^{a_{n}}$ to $x^{g(\mathbf{a})}$. We will denote by $\pi$ the natural projection

$$
\begin{equation*}
\pi: \operatorname{Aut}\left(L_{n}\right) \rightarrow \operatorname{GL}_{n}(\mathbb{Z}) \tag{3}
\end{equation*}
$$

To define $\pi$ explicitly, note that every $g \in \operatorname{Aut}\left(L_{n}\right)$ preserves the set of invertible elements of $L_{n}$, which are of the form $\lambda x^{\mathbf{a}}$ for some $\lambda \in k^{*}$ and $\mathbf{a} \in \mathbb{Z}^{n}$. In particular, $g\left(x_{i}\right)=\lambda_{i} x_{1}^{a_{i 1}} \ldots x_{n}^{a_{i n}}$ for some $\lambda_{i} \in k^{*}$ and $a_{i j} \in \mathbb{Z}$. For such $g \in \operatorname{Aut}\left(L_{n}\right)$,

$$
\pi(g)=\left(\begin{array}{cccc}
a_{11} & a_{21} & \ldots & a_{n 1}  \tag{4}\\
\ldots & & & \\
a_{1 n} & a_{2 n} & \ldots & a_{n n}
\end{array}\right)
$$

Our main result can now be stated as follows.
Theorem 1.1. Let $k$ be a field, $L_{n}=k\left[x_{1}^{ \pm 1}, \ldots, x_{n}^{ \pm 1}\right]$ be the Laurent polynomial ring in $n$ variables and $G$ be a finite subgroup of $\operatorname{Aut}\left(L_{n}\right)$. Then
(1) $\operatorname{In}\left(L_{n}^{G}\right)$ is finitely generated,
(2) $L_{n}^{G}$ has a finite $S A G B I$ basis,
(3) $\pi(G)$ is generated by reflections.

Theorem 1.1 is a generalization of [8, Theorem 1.6], where $G$ is assumed to act on $L_{n}$ multiplicatively, i.e., $G \subset \mathrm{GL}_{n}(\mathbb{Z})$. Further results for multiplicative actions can be found in [11. A novel feature of Theorem 1.1 is that condition (3) is independent of the choice of coordinates in $L_{n}$. Indeed, as we mentioned above, a different choice of coordinates in $L_{n}$ corresponds to replacing $L_{n}^{G}$ by $g\left(L_{n}^{G}\right)$ for some $g \in \operatorname{Aut}\left(L_{n}\right)$ or, equivalently, to replacing $G$ by the conjugate subgroup $G^{\prime}=g G g^{-1}$ in $\operatorname{Aut}\left(L_{n}\right)$. Clearly, $\pi\left(G^{\prime}\right)$ is generated by reflections if and only if $\pi(G)$ is generated by reflections.

We also note that our proof of Theorem 1.1 below shows that Theorem 1.1 remains valid if the initial exponent $\operatorname{in}(f)$ is defined relative to any term order in $L_{n}$, not necessarily the lexicographic order. Recall that a term order in $L_{n}$ is a linear order on $\mathbb{Z}^{n}$, compatible with the group structure; cf. [8, Definition 1.2]. In view of these remarks, Theorem 1.1 can be restated as follows.

Theorem 1.2. Let $G$ be a finite subgroup of $\operatorname{Aut}\left(L_{n}\right)$.
(a) If $\pi(G)$ is generated by reflections, then $L_{n}^{G}$ has a $S A G B I$ basis relative to any choice of coordinates and term order in $L_{n}$.
(b) If $\pi(G)$ is not generated by reflections, then $\operatorname{In}\left(L_{n}^{G}\right)$ is not finitely generated (and, in particular, $L_{n}^{G}$ does not have a SAGBI basis) for any choice of coordinates and term order in $L_{n}$.

The rest of this paper is structured as follows. Sections 4 and 5 will be devoted to the proof of Theorem 1.1. The main new phenomenon we encounter, compared to the proof of [8, Theorem 1.6], is that the semigroup $\operatorname{In}\left(L_{n}^{G}\right)$ is no longer saturated in $\mathbb{Z}^{n}$. In order to deal with the resulting complications, we prove the Sandwich Lemma 3.1 in Section 3 In Section 6 we use a similar argument (also based on the Sandwich Lemma) to prove a generalized form of Göbel's conjecture. (For background material and references on Göbel's original conjecture, see the first paragraph of Section 6.) In the last section we work out an explicit example.

## 2. Notational conventions

The following symbols are used throughout this paper.

| $\mathbb{N}$ | the set of non-negative integers |
| :--- | :--- |
| $\Sigma_{n}$ | the symmetric group on $n$ letters |
| $k$ | base field |
| $P_{n}=k\left[x_{1}, \ldots, x_{n}\right]$ | polynomial ring in $n$ variables |
| $L_{n}=k\left[x_{1}^{ \pm 1}, \ldots, x_{n}^{ \pm 1}\right]$ | Laurent polynomial ring in $n$ variables |
| $\pi$ | projection Aut $\left(L_{n}\right) \rightarrow \mathrm{GL}_{n}(\mathbb{Z}) ;$ see (3) and (4) |
| $G$ | finite subgroup of $\operatorname{Aut}\left(L_{n}\right)$ |
| $\bar{G}$ | $=\pi(G)$ |
| $\succ$ | term order in $L_{n}$ or $P_{n}$ |
| in | the initial exponent relative to $\succ$ |
| In | the semigroup of initial exponents relative to $\succ$ |

We will write bold letters $\mathbf{a}, \mathbf{b}$, etc., for elements of $\mathbb{R}^{n}$. If $\mathbf{a}=\left(a_{1}, \ldots, a_{n}\right) \in \mathbb{Z}^{n}$, we will abbreviate $x_{1}^{a_{1}} \ldots x_{n}^{a_{n}}$ as $x^{\mathbf{a}}$.

All semigroups in this paper will be contained in $\mathbb{Z}^{n}$ and, in particular, will be abelian. We will use the words "semigroup" and "monoid" interchangeably; that is, all semigroups will be assumed to have an identity element. In particular, by the "semigroup generated by a set $S \subset \mathbb{Z}^{n}$ " we will mean

$$
\left\{a_{1} s_{1}+\cdots+a_{r} s_{r} \mid r, a_{1}, \ldots, s_{r} \in \mathbb{N} \text { and } s_{1}, \ldots, s_{r} \in S\right\}
$$

With the exception of Theorem 1.2 above, the term order $\succ$ will remain in the background; our arguments will work for any term order. The reader will lose little by assuming that $\succ$ is the lexicographic order from now on.

## 3. The sandwich lemma

The purpose of this section is to prove the following lemma, which will play a key role in the sequel. This lemma follows from standard results in semigroup theory; see, e.g., [1, Corollary 2.10]. We prove it here for the sake of completeness.

Lemma 3.1 (Sandwich Lemma). Suppose $A$ and $B$ are subsemigroups of $\mathbb{Z}^{n}$ such that $m A \subset B \subset A$ for some integer $m \geq 1$. Then $A$ is finitely generated if and only if $B$ is finitely generated.

Our proof will rely on the following classical result, which may be viewed as a variant of the Hilbert Basis Theorem; see [3, Lemma A] or [2, Section 2.4].

Lemma 3.2 (Dickson's Lemma). Suppose $A \subset \mathbb{N}^{n}$ has the property that for $\mathbf{a} \in A$ and any $\mathbf{n} \in \mathbb{N}^{n}$ we have $\mathbf{a}+\mathbf{n} \in A$. Then there exists a finite set $S \subset \mathbb{N}^{n}$ such that $A=\left\{\mathbf{s}+\mathbf{n} \mid \mathbf{s} \in S, \mathbf{n} \in \mathbb{N}^{n}\right\}$.
Proof of the Sandwich Lemma. Since $m A \simeq A$ and $m B \subset m A \subset B$, it suffices to prove only one direction. We will thus assume that $A$ is finitely generated and aim to prove that then $B$ is finitely generated as well.

In fact, we may assume without loss of generality that $A=\mathbb{N}^{n}$. Indeed, since $A$ is finitely generated there is a surjective semigroup homomorphism $\phi: \mathbb{N}^{n} \rightarrow A$ for some $n \geq 1$. Then $A^{\prime}=\mathbb{N}^{n}$ and $B^{\prime}=\phi^{-1}(B)$ satisfy $m A^{\prime} \subset B^{\prime} \subset A^{\prime}$. If we know that the theorem holds for $A^{\prime}$ and $B^{\prime}$, then $B^{\prime}$ is finitely generated and, hence, so is $B=\phi\left(B^{\prime}\right)$.

From now on we will assume that $A=\mathbb{N}^{n}$. Set

$$
R:=\left\{\left(r_{1}, \ldots, r_{n}\right) \in \mathbb{N}^{n} \mid 0 \leq r_{i}<m\right\}
$$

Then every element $\mathbb{N}^{n}$ can be written as $m \mathbf{q}+\mathbf{r}$ for some $\mathbf{q} \in \mathbb{N}^{n}$ and $\mathbf{r} \in R$. Given $\mathbf{r} \in R$, set

$$
Q_{\mathbf{r}}:=\left\{\mathbf{q} \in \mathbb{N}^{n} \mid m \mathbf{q}+\mathbf{r} \in B\right\} .
$$

(Our notation is meant to be suggestive: we think of elements of $R$ as "remainders" and elements of $Q_{\mathbf{r}}$ as "quotients".) Since we are assuming that $m \mathbb{N}^{n} \subset B$, each $Q_{\mathbf{r}}$ satisfies the requirements of Lemma 3.2. Thus for every $\mathbf{r} \in R$ there is a finite set $F_{\mathbf{r}} \subset \mathbb{N}^{n}$ such that

$$
Q_{\mathbf{r}}=\left\{\mathbf{s}+\mathbf{n} \mid \mathbf{s} \in F_{\mathbf{r}}, \mathbf{n} \in \mathbb{N}^{n}\right\} .
$$

We claim that

$$
\left(\bigcup_{\mathbf{r} \in R} \bigcup_{\mathbf{s} \in F_{\mathbf{r}}} m \mathbf{s}+\mathbf{r}\right) \cup\left\{m \mathbf{e}_{i} \mid i=1, \ldots, n\right\}
$$

is a (finite) set of generators for $B$. Here

$$
\mathbf{e}_{1}=(1,0, \ldots, 0), \ldots, \mathbf{e}_{n}=(0, \ldots, 0,1) ;
$$

note that $m \mathbf{e}_{i} \in m \mathbb{N}^{n} \subset B$.
To prove the claim, recall that every $\mathbf{b} \in B$ can be written as $\mathbf{b}=m \mathbf{q}+\mathbf{r}$ for some $\mathbf{r} \in R$ and some $\mathbf{q} \in Q_{\mathbf{r}}$. Writing $\mathbf{q}$ as $\mathbf{s}+\mathbf{n}$ for some $\mathbf{s} \in F_{\mathbf{r}}$ and some $\mathbf{n} \in \mathbb{N}^{n}$, we see that $\mathbf{b}=(m \mathbf{s}+\mathbf{r})+m \mathbf{n}$. Since $m \mathbf{n}$ is an $\mathbb{N}$-linear combination of $m \mathbf{e}_{1}, \ldots, m \mathbf{e}_{n}$, the claim follows.

## 4. Finite generation of the semigroup of initial exponents

In this section we will prove that conditions (1) and (3) of Theorem 1.1 are equivalent.

Let $\bar{G}=\pi(G) \subset \mathrm{GL}_{n}(\mathbb{Z})$. For $\mathbf{a} \in \mathbb{Z}^{n}$ let $S_{\mathbf{a}}$ be the subgroup of $G$ given by $S_{\mathbf{a}}=G \cap \pi^{-1}\left(\operatorname{Stab}_{\bar{G}}(\mathbf{a})\right)$. In other words, for every $s \in S_{\mathrm{a}}$ there exists a non-zero scalar $\eta_{\mathbf{a}}(s) \in k$ such that $s \cdot x^{\mathbf{a}}=\eta_{\mathbf{a}}(s) x^{\mathbf{a}}$. It is easy to see that $\eta_{\mathbf{a}}$ is, in fact, a multiplicative character $S_{\mathbf{a}} \rightarrow k^{*}$.

For a given set $D$ of distinct representatives for the left cosets of $S_{\mathbf{a}}$, we define

$$
\Omega_{D}(\mathbf{a}):=\sum_{d \in D} d\left(x^{\mathbf{a}}\right)
$$

Recall that the support $\operatorname{supp}(f) \subset \mathbb{Z}^{n}$ of $f \in L_{n}$ is defined as the set of exponents a such that $x^{\mathbf{a}}$ occurs in $f$ with a non-zero coefficient. For $S \subset L_{n}$ we define $\operatorname{Supp}(S)$ to be the union of $\operatorname{supp}(f)$, as $f$ ranges over $S$.

Lemma 4.1. For any $\mathbf{a} \in \mathbb{Z}^{n}$, the following are equivalent:
(a) $\mathbf{a} \in \operatorname{Supp}\left(L_{n}^{G}\right)$,
(b) $\eta_{\mathbf{a}}$ is the trivial character of $S_{\mathbf{a}}$,
(c) $\Omega_{D}(\mathbf{a})$ is independent of the choice of $D$,
(d) $\Omega_{D}(\mathbf{a}) \in L_{n}^{G}$ for any $D$,
(e) $\Omega_{D}(\mathbf{a}) \in L_{n}^{G}$ for some $D$.

If the equivalent conditions of Lemma 4.1 hold, then in view of (c) we will write $\Omega(\mathbf{a})$ in place of $\Omega_{D}(\mathbf{a})$.

Proof. (a) $\Rightarrow(\mathrm{b}):$ If $s \cdot x^{\mathbf{a}} \neq x^{\mathbf{a}}$ for some $s \in S_{\mathbf{a}}$, then no $f \in L_{n}$ containing $\mathbf{a}$ in its support can be invariant under the action of $s$.
$(\mathrm{b}) \Rightarrow(\mathrm{c})$ : Suppose $s \cdot x^{\mathbf{a}}=x^{\mathbf{a}}$ for any $s \in S_{\mathbf{a}}$. Then replacing $d \in D$ by another representative $d^{\prime}=d s$ in the same left coset of $S_{\mathbf{a}}$ does not change $d(\mathbf{a})$.
$(\mathrm{c}) \Rightarrow(\mathrm{d}):$ Let $h \in G$. It is easy to see that if $d_{1}, \ldots, d_{r}$ are representatives of distinct left cosets of $S_{\mathbf{a}}$ in $G$, then so are $h d_{1}, \ldots, h d_{r}$. Hence, $h\left(\Omega_{D}(\mathbf{a})\right)=\Omega_{D}(\mathbf{a})$.
$(\mathrm{d}) \Rightarrow(\mathrm{e})$ : Obvious.
(e) $\Rightarrow$ (a): If $\Omega_{D}(\mathbf{a}) \in L_{n}^{G}$, then clearly $\mathbf{a} \in \operatorname{Supp}\left(\Omega_{D}(\mathbf{a})\right) \subset \operatorname{Supp}\left(L_{n}^{G}\right)$.

If $H$ is a subgroup of $\mathrm{GL}_{n}(\mathbb{Z})$, then following [8, Definition 2.5] we set

$$
A(H)^{\succ}:=\left\{\mathbf{a} \in \mathbb{Z}^{n} \mid \mathbf{a} \succeq h(\mathbf{a}) \quad \forall h \in H\right\} .
$$

It is easy to see that $A(H)^{\succ}=\operatorname{In}\left(L_{n}^{H}\right)$; see [8, Lemma 2.6].
Corollary 4.2. $\operatorname{In}\left(L_{n}^{G}\right)=A(\bar{G})^{\succ} \cap\left\{\mathbf{a} \in \mathbb{Z}^{n} \mid \eta_{\mathbf{a}}=1\right\}$.

Proof. The inclusion $\operatorname{In}\left(L_{n}^{G}\right) \subset A(\bar{G})^{\succ}$ is clear from the definition. On the other hand, by Lemma 4.1

$$
\operatorname{In}\left(L_{n}^{G}\right) \subset \operatorname{Supp}\left(L_{n}^{G}\right) \subset\left\{\mathbf{a} \in \mathbb{Z}^{n} \mid \eta_{\mathbf{a}}=1\right\}
$$

This shows that $\operatorname{In}\left(L_{n}^{G}\right) \subset A(\bar{G})^{\succ} \cap\left\{\mathbf{a} \in \mathbb{Z}^{n} \mid \eta_{\mathbf{a}}=1\right\}$.
To prove the opposite inclusion, note that by Lemma4.1, if $\eta_{\mathbf{a}}=1$, then $\Omega(\mathbf{a}) \in$ $L_{n}^{G}$. If moreover $\mathbf{a} \in A(\bar{G})^{\succ}$, then $\mathbf{a}=\operatorname{in}(\Omega(\mathbf{a})) \in \operatorname{In}\left(L_{n}^{G}\right)$.

We are now ready to show that conditions (1) and (3) of Theorem 1.1 are equivalent. Let $\mathbf{a} \in \mathbb{Z}^{n}$. Clearly $S_{r \mathbf{a}}=S_{\mathbf{a}}$ and $\eta_{r \mathbf{a}}=\eta_{\mathbf{a}}^{r}$ for any non-zero integer $r$. This implies that $\eta_{r \mathbf{a}}=1$ for any $r$ divisible by the order of $S_{\mathbf{a}}$. Taking $r=|G|$ we see that $\eta_{r \mathbf{a}}=1$ for every $\mathbf{a} \in \mathbb{Z}^{n}$. Thus by Corollary $4.2,|G| \cdot A(\bar{G})^{\succ} \subset \operatorname{In}\left(L_{n}^{G}\right) \subset A(\bar{G})^{\succ}$. Equivalently,

$$
|G| \cdot \operatorname{In}\left(L_{n}^{\bar{G}}\right) \subset \operatorname{In}\left(L_{n}^{G}\right) \subset \operatorname{In}\left(L_{n}^{\bar{G}}\right)
$$

By [8, Theorem 1.6], $\operatorname{In}\left(L_{n}^{\bar{G}}\right)$ is finitely generated if and only if $\bar{G}$ is generated by reflections. Lemma 3.1now tells us that the same is true of $\operatorname{In}\left(L_{n}^{G}\right)$. In other words, conditions (1) and (3) of Theorem 1.1 are equivalent.

## 5. Termination of the subduction algorithm

In this section we will finish the proof of Theorem 1.1. We have shown that conditions (1) and (3) are equivalent. Moreover, by definition, (2) $\Rightarrow$ (1). Thus it remains to show that $(3) \Rightarrow(2)$. This implication is a consequence of the following proposition.

Proposition 5.1. Let $G$ be a finite subgroup of $\operatorname{Aut}\left(L_{n}\right)$. Assume that $\pi(G) \subset$ $\mathrm{GL}_{n}(\mathbb{Z})$ is generated by reflections. If $\mathbf{a}_{1}, \ldots, \mathbf{a}_{m}$ generate the semigroup $\operatorname{In}\left(L_{n}^{G}\right)$, then $p_{1}=\Omega\left(\mathbf{a}_{1}\right), \ldots, p_{m}=\Omega\left(\mathbf{a}_{m}\right)$ form a SAGBI basis in $L_{n}^{G}$.

The proof of this proposition is essentially the same as the proof of [8, Proposition 5.8]; for the sake of completeness we outline the argument below.

Proof. Suppose we apply the subduction algorithm to express $f \in L_{n}^{G}$ as a polynomial in $p_{1}, \ldots, p_{m}$. The algorithm produces a sequence of elements $f_{0}=f, f_{1}, f_{2}, \ldots$ in $L_{n}^{G}$ with initial terms

$$
\begin{equation*}
\operatorname{in}\left(f_{0}\right) \succ \operatorname{in}\left(f_{1}\right) \succ \operatorname{in}\left(f_{2}\right) \succ \ldots \tag{5}
\end{equation*}
$$

We need to show that this sequence will terminate, regardless of the choice of $f$ or the choices we made in carrying out the subduction algorithm. We will argue by contradiction: assume that the above sequence does not terminate for some $f \in L_{n}^{G}$.

Let us embed $\bar{G} \subset \mathrm{GL}_{n}(\mathbb{Z})$ into $\mathrm{GL}_{n}(\mathbb{R})$ in the natural way, lifting the $\bar{G}$-action from $\mathbb{Z}^{n}$ to $\mathbb{R}^{n}$. An easy exercise in linear algebra shows that $\mathbb{R}^{n}$ is the direct sum of two $\bar{G}$-invariant subspaces,

$$
\left(\mathbb{R}^{n}\right)^{\bar{G}}=\left\{\mathbf{v} \in \mathbb{R}^{n} \mid g(\mathbf{v})=\mathbf{v} \quad \forall g \in \bar{G}\right\}
$$

and

$$
\left(\mathbb{R}^{n}\right)_{0}=\left\{\mathbf{v} \in \mathbb{R}^{n} \mid \sum_{g \in \bar{G}} g(\mathbf{v})=\mathbf{0}\right\}
$$

and that $\left(\mathbb{R}^{n}\right)_{0}$ is the orthogonal complement of $\left(\mathbb{R}^{n}\right)^{\bar{G}}$ relative to any $\bar{G}$-invariant scalar product on $\mathbb{R}^{n}$. We also have $\bar{G}$-invariant linear maps $\pi_{1}: \mathbb{R}^{n} \rightarrow\left(\mathbb{R}^{n}\right)^{\bar{G}}$ and $\pi_{2}: \mathbb{R}^{n} \rightarrow\left(\mathbb{R}^{n}\right)_{0}$ given by

$$
\pi_{1}(\mathbf{v})=\sum_{g \in \bar{G}} g(\mathbf{v}) \quad \text { and } \quad \pi_{2}(\mathbf{v})=|\bar{G}| \mathbf{v}-\pi_{1}(\mathbf{v})
$$

which are simply the orthogonal projections of $|\bar{G}| \mathbf{v}$ onto $\left(\mathbb{R}^{n}\right)^{G}$ and $\left(\mathbb{R}^{n}\right)_{0}$ respectively. Note that both $\pi_{1}$ and $\pi_{2}$ are defined over the integers (i.e., carry $\mathbb{Z}^{n}$ into itself); this is the reason we did not divide by $|\bar{G}|$ in the formulas.

Arguing as in the proof of [8, Proposition 5.8], we see that the sequence

$$
\pi_{1}\left(\operatorname{in}\left(f_{0}\right)\right), \pi_{1}\left(\operatorname{in}\left(f_{1}\right)\right), \pi_{1}\left(\operatorname{in}\left(f_{2}\right)\right), \ldots
$$

assumes only finitely many values Thus, we can choose an infinite subsequence $\mathbf{w}_{1} \succ \mathbf{w}_{2} \succ \mathbf{w}_{3} \succ$ of the sequence (5) such that $\pi_{1}\left(\mathbf{w}_{i}\right)=\mathbf{c}$ is the same for every $i \geq 1$. The argument in the proof of [8, Proposition 5.8] then shows that

$$
\pi_{2}\left(\mathbf{w}_{1}\right) \succ \pi_{2}\left(\mathbf{w}_{2}\right) \succ \ldots
$$

is an infinite strictly decreasing sequence in $A^{\succ}(\bar{G}) \cap\left(\mathbb{R}^{n}\right)_{0}$. On the other hand, by [8, Lemma 5.3(a) and Proposition 5.5] this sequence has to terminate. This contradiction shows that the sequence (5) always terminates. This completes the proof of Proposition 5.1 and thus of Theorem 1.1 .

## 6. The generalized GöBel's conjecture

We now return to the setting we introduced at the beginning of Section where we asked which $k$-subalgebras $R$ of the polynomial algebra $P_{n}=k\left[x_{1}, \ldots, x_{n}\right]$ have a SAGBI basis. Suppose $G \subset \Sigma_{n}$ acts on $P_{n}$ by permuting the variables. Here, $\Sigma_{n}$ denotes the permutation group on $n$ letters. Göbel [4, p. 65] conjectured that $R=P_{n}^{G}$ has a SAGBI basis if and only if $G$ is conjugate to $\Sigma_{n_{1}} \times \cdots \times \Sigma_{n_{k}}$ for some partition $\left(n_{1}, \ldots, n_{r}\right)$ of $n$. This conjecture was proved independently by Kuroda [6], Thiéry-Thomassé [12] and the second author [8].

Now, in the spirit of Theorem 1.1, we replace $\Sigma_{n}$ with $N=\mathbb{G}_{m}^{n} \rtimes \Sigma_{n}$, where $\Sigma_{n}$ acts on $\mathbb{G}_{m}^{n}$ by permuting the factors. Note that $N$ is naturally embedded into the group $\operatorname{Aut}\left(L_{n}\right)=\mathbb{G}_{m}^{n} \rtimes \mathrm{GL}_{n}(\mathbb{Z})$. Moreover, every element of $N \subset \operatorname{Aut}\left(L_{n}\right)$ preserves the polynomial ring $P_{n}$ and restricts to an automorphism of $P_{n}$. That is, $\mathbb{G}_{m}^{n}$ acts by rescaling and $\Sigma_{n}$ by permuting the variables $x_{1}, \ldots, x_{n}$. We will denote the natural projection $N \rightarrow N /\left(\mathbb{G}_{m}^{n}\right)=\Sigma_{n}$ by $\pi$, as before.

Theorem 6.1 (Generalized Göbel's conjecture). Suppose $G$ is a finite subgroup of $\mathbb{G}_{m}^{n} \rtimes \Sigma_{n}$, acting naturally on $P_{n}=k\left[x_{1}, \ldots, x_{n}\right]$. Then $P_{n}^{G}$ has a finite SAGBI basis if and only if $\pi(G) \simeq \Sigma_{n_{1}} \times \cdots \times \Sigma_{n_{k}}$ for some partition $\left(n_{1}, \ldots, n_{r}\right)$ of $n$.

Proof. Recall from the introduction that we only need to show that $\operatorname{In}\left(P_{n}^{G}\right)$ is finitely generated; termination of the subduction algorithm is automatic in $P_{n}$.

We will use the notations of Section 4. except that we always take a in $\mathbb{N}^{n}$, rather than in all of $\mathbb{Z}^{n}$. In particular, we will denote $\pi(G)$ by $\bar{G}$ and view it

[^1]as a subgroup of $\Sigma_{n}$. Note that if $\eta_{\mathbf{a}}=1$ for some $\mathbf{a} \in \mathbb{N}^{n}$, then, by definition, $\Omega(\mathbf{a}) \in P_{n}^{G}$. Arguing exactly as in Section 4 we show that
$$
\operatorname{In}\left(P_{n}^{G}\right)=A(\bar{G})^{\succ} \cap\left\{\mathbf{a} \in \mathbb{N}^{n} \mid \eta_{\mathbf{a}}=1\right\}
$$
and thus
$$
|G| \cdot\left(A(\bar{G})^{\succ} \cap \mathbb{N}^{n}\right) \subset \operatorname{In}\left(P_{n}^{G}\right) \subset A(\bar{G})^{\succ} \cap \mathbb{N}^{n}
$$

We know that $\operatorname{In}\left(P_{n}^{\bar{G}}\right)=A(\bar{G})^{\succ} \cap \mathbb{N}^{n}$ is a finitely generated semigroup if and only if $\bar{G} \simeq \Sigma_{n_{1}} \times \cdots \times \Sigma_{n_{k}}$ for some partition $\left(n_{1}, \ldots, n_{r}\right)$ of $n$ (this is Göbel's original conjecture). The desired conclusion now follows from the Sandwich Lemma 3.1 ,

## 7. An example

Consider the cyclic subgroup $G=\langle h\rangle$ of $N=\mathbb{G}_{m}^{n} \rtimes \Sigma_{n} \subset \operatorname{Aut}\left(L_{n}\right)$, where

$$
h: \begin{aligned}
& x_{1} \mapsto \lambda_{1} x_{2} \\
& x_{2} \mapsto \lambda_{2} x_{3} \\
& \ldots \\
& x_{n} \mapsto \lambda_{n} x_{1}
\end{aligned}
$$

for some $\lambda_{1}, \ldots, \lambda_{n} \in k$. To ensure that $h$ has finite order, we will assume that the product $\lambda_{1} \lambda_{2} \cdots \lambda_{n}$ is a root of unity, say a primitive $d$ th root of unity. We will denote this product by $\zeta$.

Since $\pi(h)$ is the $n$-cycle $(12 \ldots n)$ in $\Sigma_{n}$, Theorem 1.1 tells us that $L_{n}^{G}$ has a SAGBI basis if and only if $n=2$. Similarly, Theorem 6.1 tells us that $P_{n}^{G}$ has a SAGBI basis if and only if $n=2$.

We will now set $n=2$ and find explicit SAGBI bases for these rings, relative to the lexicographic term order where $x_{1} \succ x_{2}$. To reduce the number of subscripts, we will write $x$ and $y$ instead of $x_{1}$ and $x_{2}$, respectively. We begin by computing the groups $S_{\mathbf{a}}$ and the characters $\eta_{\mathbf{a}}: S_{\mathbf{a}} \rightarrow k^{*}$. If $\mathbf{a}=(s, s)$ for some integer $s$, then $S_{\mathbf{a}}$ is the whole group $G$. Moreover, $h \cdot x^{s} y^{s}=\zeta^{s} x^{s} y^{s}$, so $\eta_{(s, s)}(h)=\zeta^{s}$. The character $\eta_{(s, s)}$ is trivial if and only if $s$ is divisible by $d$.

Now let $\mathbf{a}=(s, t)$, where $s>t$. Here $S_{\mathbf{a}}$ is the subgroup $\left\langle h^{2}\right\rangle$ of $G$ of index 2 . Since $h^{2} \cdot x^{s} y^{t}=\zeta^{s+t} x^{s} y^{t}$, the character $\eta_{\mathbf{a}}: S_{\mathbf{a}} \rightarrow k^{*}$ is given by $\eta_{(s, t)}\left(h^{2}\right)=\zeta^{s+t}$. This character is trivial if and only if $s+t$ is divisible by $d$. Using Corollary 4.2, we conclude that

$$
\begin{aligned}
\operatorname{In}\left(L_{2}^{G}\right) & =A(\bar{G})^{\succ} \cap\left\{\mathbf{a} \in \mathbb{Z}^{n} \mid \eta_{\mathbf{a}}=1\right\} \\
& =\{(s, s) \mid s \in d \mathbb{Z}\} \cup\{(s, t) \mid s>t \text { and } s+t \in d \mathbb{Z}\} \subset \mathbb{Z}^{2}
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
\operatorname{In}\left(P_{2}^{G}\right) & =A(\bar{G})^{\succ} \cap\left\{\mathbf{a} \in \mathbb{N}^{n} \mid \eta_{\mathbf{a}}=1\right\} \\
& =\{(s, s) \mid s \in d \mathbb{N}\} \cup\{(s, t) \mid s>t \text { and } s+t \in d \mathbb{N}\} \subset \mathbb{N}^{2}
\end{aligned}
$$

Lemma 7.1. (a) If $d=2 r+1$ is odd, then the semigroup $\operatorname{In}\left(L_{2}^{G}\right)$ is generated by

$$
\mathbf{a}_{1}=(d, d), \mathbf{a}_{2}=(-d,-d) \text { and } \mathbf{a}_{3}^{\text {odd }}=(r+1, r)
$$

Moreover, $\Omega\left(\mathbf{a}_{1}\right)=x^{d} y^{d}, \Omega\left(\mathbf{a}_{2}\right)=x^{-d} y^{-d}$, and $\Omega\left(\mathbf{a}_{3}^{o d d}\right)=x^{r+1} y^{r}+\zeta^{r} \lambda_{1} x^{r} y^{r+1}$ form a SAGBI basis of $\operatorname{In}\left(L_{2}^{G}\right)$.
(b) If $d=2 r$ is even, then the semigroup $\operatorname{In}\left(L_{2}^{G}\right)$ is generated by
$\mathbf{a}_{1}=(d, d), \mathbf{a}_{2}=(-d,-d), \mathbf{a}_{3}^{\text {even }}=(r+1, r-1)$ and $\mathbf{a}_{4}^{\text {even }}=(d+1, d-1)$.

Moreover, $\Omega\left(\mathbf{a}_{1}\right)=x^{d} y^{d}, \Omega\left(\mathbf{a}_{2}\right)=x^{-d} y^{-d}, \Omega\left(\mathbf{a}_{3}^{\text {even }}\right)=x^{r+1} y^{r-1}-\lambda_{1} \lambda_{2}^{-1} x^{r-1} y^{r+1}$ and $\Omega\left(\mathbf{a}_{4}^{\text {even }}\right)=x^{d+1} y^{d-1}+\lambda_{1} \lambda_{2}^{-1} x^{d-1} y^{d+1}$ form a SAGBI basis of $\operatorname{In}\left(L_{2}^{G}\right)$.

Proof. In view of Proposition 5.1, we only need to prove that the given set of initial exponents generates $\operatorname{In}\left(L_{2}^{G}\right)$ in parts (a) and (b). That is, we want to show that any given $(s, t) \in \operatorname{In}\left(L_{2}^{G}\right)$ can be expressed as a $\mathbb{N}$-linear combination of our generators. Choose $k \in \mathbb{Z}$ so that $s+t=k d$.
(a) If $d=2 r+1$ is odd, then

$$
(s, t)=((r+1) k-s)(d, d)+(s-t)(r+1, r)
$$

(b) Suppose $d=2 r$ is even. We may assume without loss of generality that $s>t$; otherwise $(s, t)=(s, s)$ is a non-negative integer multiple of $\mathbf{a}_{1}$ or $\mathbf{a}_{2}$. Since $s+t$ is divisible by $d$, it is even, and hence so is $s-t$. Let $m=(s-t) / 2$. Now

$$
(s, t)=\frac{k-m}{2}(d, d)+m(r+1, r-1)
$$

if $k-m$ is even, and

$$
(s, t)=\frac{k-m-1}{2}(d, d)+(m-1)(r+1, r-1)+(d+1, d-1)
$$

if $k-m$ is odd.
We now turn to the problem of constructing a SAGBI basis for $P_{2}^{G}$.
Lemma 7.2. (a) The semigroup $\operatorname{In}\left(P_{2}^{G}\right)$ is generated by

$$
\mathbf{b}_{i}=(d-i, i) \text { and } \mathbf{c}_{j}=(2 d-j, j)
$$

as $i$ ranges from 0 to $\left[\frac{d-1}{2}\right]$ and $j$ ranges from 1 to $d$.
(b) The elements $\Omega\left(\mathbf{b}_{i}\right)=x^{d-i} y^{i}+\zeta^{i} \lambda_{1}^{d-2 i} x^{i} y^{d-i}$ and $\Omega\left(\mathbf{c}_{j}\right)=x^{2 d-j} y^{j}+$ $\zeta^{j} \lambda_{1}^{2 d-2 j} x^{j} y^{2 d-j}$ form a SAGBI basis for $\operatorname{In}\left(P_{n}^{G}\right)$ as $i$ ranges from 0 to $\left[\frac{d-1}{2}\right]$ and $j$ ranges from 1 to $d$.

Proof. By the definition of a SAGBI basis in a subalgebra of $P_{n},(\mathrm{~b})$ is an immediate consequence of (a). Thus we only need to show that every $(s, t) \in \operatorname{In}\left(P_{2}^{G}\right)$ lies in $\Lambda$, where $\Lambda$ is the semigroup generated by all $\mathbf{b}_{i}$ and $\mathbf{c}_{j}$. If $s=t$ this is obvious, since in this case $(s, t)=(s, s)$ is a non-negative integer multiple of $\mathbf{c}_{d}=(d, d)$. We may thus assume that $s>t$. After subtracting a suitable non-negative integer multiple of $\mathbf{c}_{d}$, we may assume that $0 \leq t \leq d-1$. Moreover, after subtracting a suitable multiple of $\mathbf{b}_{0}=(d, 0)$, we may assume that $0<s-t \leq d$. Thus $s+t=(s-t)+2 t \leq 3 d-2$, i.e., $s+t=d$ or $2 d$. In other words, $(s, t)=\mathbf{b}_{t}$ or $\mathbf{c}_{t}$. In particular, $(s, t) \in \Lambda$, as claimed.

The set of generators given in Lemma 7.2 is not minimal. In fact, if $d=2 r$ is even, we only need $\mathbf{b}_{0}, \ldots, \mathbf{b}_{r-1}, \mathbf{c}_{d-1}$ and $\mathbf{c}_{d}$, and if $d$ is odd, only $\mathbf{b}_{0}, \ldots, \mathbf{b}_{r}$ and $\mathbf{c}_{d}$. We leave a proof of these assertions as an exercise for the reader.

## Acknowledgement

We would like to thank the referee for helpful comments and in particular for pointing us to [1, Corollary 2.10].

## References

1. Winfried Bruns and Joseph Gubeladze, Polytopes, rings and k-theory, http://math.sfsu.edu/gubeladze/publications/kripo/kripo.pdf.
2. David Cox, John Little, and Donal O'Shea, Ideals, varieties, and algorithms, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992, An introduction to computational algebraic geometry and commutative algebra. MR1189133 (93j:13031)
3. Leonard Eugene Dickson, Finiteness of the odd perfect and primitive abundant numbers with $n$ distinct prime factors, American Journal of Mathematics 35 (1913), no. 4, 413-422. MR1506194
4. Manfred Göbel, The optimal lower bound for generators of invariant rings without finite SAGBI bases with respect to any admissible order, Discrete Math. Theor. Comput. Sci. 3 (1999), no. 2, 65-70 (electronic). MR1695195 (2001b:13008)
5. Manfred Göbel, Finite SAGBI bases for polynomial invariants of conjugates of alternating groups, Math. Comp. 71 (2002), no. 238, 761-765 (electronic). MR1885626 (2002m:13009)
6. Shigeru Kuroda, The infiniteness of the SAGBI bases for certain invariant rings, Osaka J. Math. 39 (2002), no. 3, 665-680. MR1932287 (2003k:13033)
7. Martin Lorenz, Multiplicative invariant theory, Encyclopaedia of Mathematical Sciences, vol. 135, Springer-Verlag, Berlin, 2005, Invariant Theory and Algebraic Transformation Groups, VI. MR2131760 (2005m:13012)
8. Zinovy Reichstein, SAGBI bases in rings of multiplicative invariants, Comment. Math. Helv. 78 (2003), no. 1, 185-202. MR1966757 (2004c:13005)
9. Lorenzo Robbiano and Moss Sweedler, Subalgebra bases, Commutative algebra (Salvador, 1988), Lecture Notes in Math., vol. 1430, Springer, Berlin, 1990, pp. 61-87. MR 1068324 (91f:13027)
10. Bernd Sturmfels, Gröbner bases and convex polytopes, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996. MR1363949 (97b:13034)
11. Mohammed Tesemma, On multiplicative invariants of finite reflection groups, Comm. Algebra 35 (2007), no. 7, 2258-2274. MR2331844
12. N. M. Thiéry and S. Thomassé, Convex cones and SAGBI bases of permutation invariants, Invariant theory in all characteristics, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 259-263. MR2066473 (2005e:13006)

Department of Mathematics, University of British Columbia, Vancouver, British Columbia V6T 1Z2, Canada

E-mail address: duncan@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver, British Columbia V6T 1Z2, Canada

E-mail address: reichst@math.ubc.ca


[^0]:    Received by the editors February 6, 2008, and, in revised form, February 28, 2008.
    2000 Mathematics Subject Classification. Primary 13A50, 13 P99.
    Key words and phrases. SAGBI basis, subduction algorithm, Göbel's conjecture, group action, algebra of invariants, reflection group, abelian semigroup.

    The first author was partially supported by an NSERC Canada Graduate Scholarship.
    The second author was partially supported by NSERC Discovery and Accelerator Supplement grants.

[^1]:    ${ }^{1}$ We would like to use this opportunity to correct a misprint in the proof of 8 Proposition 5.8]: in the sentence after the formula $p(v)=\sum_{g \in G} g(v)$ the roles of the variables $\alpha$ and $\alpha_{1}$ should be interchanged.

