CONVEX CONES AND SAGBI BASES OF PERMUTATION INVARIANTS

NICOLAS M. THIÉRY AND STÉPHAN THOMASSÉ

Abstract. Let G be a permutation group acting on $\{1, \dots, n\}$, and $<$ be any admissible term order on the polynomial ring $\mathbb{K}[x_1, \dots, x_n]$. We prove that the invariant ring $\mathbb{K}[x_1, \dots, x_n]^G$ of G has a finite SAGBI basis if, and only if, G is generated by reflections.

1. Introduction

Let $\mathbb{K}$ be a field (or a ring). Let G be a permutation group on $\{1, \dots, n\}$. Let $V := \mathbb{K}^n$, and $x := (x_1, \dots, x_n)$ be the canonical basis of the dual of V. The invariant ring $\mathbb{K}[x]^G$ of G is the graded subalgebra of the polynomials of $\mathbb{K}[x] := \mathbb{K}[x_1, \dots, x_n]$ which are invariant for the natural action of G on the variables. Given a vector $u \in \mathbb{N}^n$, we denote by x^u the monomial $x_1^{u_1} \cdots x_n^{u_n}$. The *orbit sum* $\mathrm{o}(x^u)$ of a monomial x^u is the sum of all the monomials in the G-orbit of x^u. Given a subset S of $\{1, \dots, n\}$, we denote by $\mathfrak{S}(S)$ the symmetric group of all permutations of S and by $e_d(S)$ the d-th *elementary symmetric polynomial* in the corresponding variables $\sum_{(i_1 < \dots < i_d) \in S^d} x_{i_1} \cdots x_{i_d}$.

We recall the definition of a SAGBI basis (Subalgebra Analog of a Gröbner Basis for Ideals) [KM89, RS90], which provides a useful device in the computational study of invariant rings of permutation groups [Thi01]. Given an admissible term order $<$ on $\mathbb{K}[x]$, we denote by $\mathrm{in}_<(\mathbb{K}[x]^G)$ the monoid of all initial monomials of invariants in $\mathbb{K}[x]^G$. For a permutation group, this can also be defined as the monoid of all monomials x^u such that $x^u \geq g.x^u$ for all $g \in G$. By abuse of notations, we also denote by $\mathrm{in}_<(\mathbb{K}[x]^G)$ the initial algebra of $\mathbb{K}[x]^G$, which is the linear span of those monomials. A SAGBI basis of $\mathbb{K}[x]^G$ is a subset S of invariants in $\mathbb{K}[x]^G$ whose initial monomials generates $\mathrm{in}_<(\mathbb{K}[x]^G)$ as an algebra. It follows in particular that S generates $\mathbb{K}[x]^G$ as an algebra. A monomial $x^u \in \mathrm{in}_<(\mathbb{K}[x]^G)$ is *irreducible* if it cannot be decomposed as a product of two non-trivial monomials of $\mathrm{in}_<(\mathbb{K}[x]^G)$ (this definition generalizes for any monoid). If x^u is irreducible, then any SAGBI basis of $\mathrm{in}_<(\mathbb{K}[x]^G)$ must contain a polynomial having x^u as initial monomial. The set of all orbit sums of irreducible monomials is actually the minimal reduced SAGBI basis of $\mathrm{in}_<(\mathbb{K}[x]^G)$. We refer for example to [CLO97, Stu96] for further background on invariant rings, term orders, and SAGBI bases.

As opposed to Gröbner bases, SAGBI bases need not be finite, and it is an important problem to classify the algebras which have a finite SAGBI basis for some term order [Stu96]. In this article we complete this classification for invariant rings of permutation groups in their permutation basis.

Let $S_1, \dots, S_r$ be the orbits of G on the variables, and E be the set of the n elementary symmetric polynomials

$$(e_1(S_1), \dots, e_{|S_1|}(S_1), \dots, e_1(S_r), \dots, e_{|S_r|}(S_r)).$$

Date: $Id : main.tex, v1.142004/04/0507 : 33 : 02nthieryExp$.

This research was partially funded by Queen's University and the Royal Military College of Kingston (Ontario, Canada).

Assume that G is generated by reflections (i.e. by transpositions); otherwise said, assume that G is the direct product $\mathfrak{S}(S_1) \times \cdots \times \mathfrak{S}(S_r)$ of the symmetric groups on its transitive components. Then, it is well known that not only $\mathbb{K}[x]^G$ is the polynomial ring in E, but E is a *comprehensive* SAGBI basis of $\mathbb{K}[x]^G$, that is a SAGBI basis of E for any admissible term order.

In [Göb98], M. Göbel proved that these are the only permutation groups with a finite SAGBI basis with respect to the lexicographic term order.

Theorem 1.1. *Let G be a permutation group acting on $\{1, \ldots, n\}$, and $<_{\text{lex}}$ be the lexicographic term order on $\mathbb{K}[x]$. Then, the invariant ring $\mathbb{K}[x]^G$ has a finite SAGBI basis with respect to $<_{\text{lex}}$ if, and only if, G is generated by reflections.*

In [Göb99b, Göb99a, Göb00], M. Göbel further conjectures that this result extends to any admissible term order, and proves it for the alternating groups A_n, and a few other groups.

In this paper, we confirm this conjecture by proving the following theorem.

Theorem 1.2. *Let G be a permutation group acting on $\{1, \ldots, n\}$, and $<$ be any admissible term order on $\mathbb{K}[x]$. Then, the invariant ring $\mathbb{K}[x]^G$ has a finite SAGBI basis with respect to $<$ if, and only if, G is generated by reflections.*

This result was also obtained independently by Z. Reichstein [Rei02], as a corollary of a more general theorem on multiplicative invariants, as well as by Shigeru Kuroda [Kur02], with some further generalizations. The techniques used in each cases are essentially the same, our proof being by far the shortest.

Note that theorem 1.2 does not preclude the existence of a finite SAGBI basis for $\mathbb{K}[x]^G = \mathbb{K}[V]^G$ when the dual basis of V is not one of its permutation basis. Consider, for example, the cyclic group $C_3 = A_3$ acting by permutation on the variables x_1, x_2, x_3 in characteristic 3. In the basis $y_1 := x_1, y_2 := x_2 - x_1, y_3 := x_3 - 2x_2 + x_1$, the invariant ring $\mathbb{F}_3[x]^{C_3} = \mathbb{F}_3[V]^{C_3} = \mathbb{F}_3[y_1, y_2, y_3]^{C_3}$ has a finite SAGBI basis w.r.t. the degree reverse lexicographic order with $y_1 < y_2 < y_3$ [SW02]. Thus, classifying the invariants rings of permutation groups which have a finite SAGBI basis for some term order in some basis remains an open problem.

The paper is organized as follows. In section 2, we show that, if a convex cone C of ${\mathbb{R}^+}^n$ is not closed for the usual topology, then its monoid of *integer vectors* (vectors with nonnegative integer coordinates) contains infinitely many irreducible elements. In section 3, we describe the monoid $\operatorname{in}_<(\mathbb{K}[x]^G)$ as the monoid of integer vectors of a suitable convex cone $C_<(G)$ of ${\mathbb{R}^+}^n$, and prove theorem 1.2 by showing that this convex cone is not closed when G is not generated by reflections. This last step relies on an explicit and fairly simple construction of a line segment in C with an extremity not in C.

2. CONVEX CONES

Let $\mathbb{R}^+$ be the set of non-negative real numbers. We call *convex cone* a subset C of ${\mathbb{R}^+}^n$ such that $\lambda u + \mu v \in C$ for all u, v in C and λ, μ in $\mathbb{R}^+$. In particular, C is a monoid for $+$. Its *integral cone* $M(C) := C \cap \mathbb{N}^n$ is the submonoid of the integer vectors of C. An element of $M(C)$ is *irreducible* if it cannot be decomposed as the sum of two non-trivial elements of $M(C)$. Obviously, the set of irreducible elements of $M(C)$ is a minimal generating set for $M(C)$.

Lemma 2.1. *Let C be a convex cone which spans $\mathbb{R}^n$ as a vector space, and is not closed for the usual topology of $\mathbb{R}^n$. Then, its integral cone $M(C)$ has infinitely many irreducible elements.*

Proof. Let $v_1, \ldots, v_n$ be a subset of $M(C)$ which spans $\mathbb{R}^n$ as a vector space. Assume $M(C)$ is generated by a finite set S of integer vectors, and let $\langle S \rangle$ be the convex subcone of C spanned by S. This subcone is a closed subset of $\mathbb{R}^n$. Hence, $C\backslash\langle S\rangle$ is non-empty. Let v_0 be a vector of $C\backslash\langle S\rangle$, and consider the convex hull $O := \{\lambda_0 v_0 + \lambda_1 v_1 + \cdots + \lambda_n v_n, 0 < \lambda_i < 1\}$, which is both open and contained in C. Since v_0 is in the closure of O, and $\langle S\rangle$ is closed, $O\backslash\langle S\rangle$ is non-empty, open and included in C. Hence, $C\backslash\langle S\rangle$ has a non-empty interior.

Now, we can take an open ball $B(u, \epsilon)$ of center u and radius $\epsilon > 0$ in $C\backslash\langle S\rangle$. The open ball $B(\frac{\sqrt{n}}{\epsilon}u, \sqrt{n})$ still lies in $C\backslash\langle S\rangle$, but also contains an integer vector p. This vector p cannot be generated by S, which is the desired contradiction. ☐

As a first application, we verify one of the very first results on SAGBI basis, namely that the invariant ring $\mathbb{K}[x]^{A_3}$ of the alternating group A_3 on 3 elements has no finite SAGBI basis with respect to the lexicographic term order with $x_1 > x_2 > x_3$. Let $x^u := x_1^{u_1} x_2^{u_2} x_3^{u_3}$ be a monomial. Then, x^u is initial if, and only if,

$$(u_1, u_2, u_3) \geq_{\text{lex}} (u_2, u_3, u_1) \text{ and } (u_1, u_2, u_3) \geq_{\text{lex}} (u_3, u_1, u_2),$$

which we can rewrite as

$$(u_1 - u_2, u_2 - u_3, u_3 - u_1) \geq_{\text{lex}} (0, 0, 0) \text{ and } (u_1 - u_3, u_2 - u_1, u_3 - u_2) \geq_{\text{lex}} (0, 0, 0).$$

We define the *initial cone* C to be the convex cone of all vectors of ${\mathbb{R}^+}^3$ satisfying those inequations, so that $\text{in}_{\text{lex}}(\mathbb{K}[x]^{A_3})$ is the integral cone of C. Note that C spans $\mathbb{R}^n$, since it contains the independent vectors $(1, 0, 0)$, $(1, 1, 0)$, and $(1, 1, 1)$.

Now, proving that $\mathbb{K}[x]^{A_3}$ has no finite SAGBI basis for lex is immediate: $(1, 0, 1)$ is not in C, whereas $(1, 0, 1) + \epsilon(1, 0, 0)$ is in C for any $\epsilon > 0$; hence, C is not closed, and by lemma 2.1 $\text{in}_{\text{lex}}(\mathbb{K}[x]^{A_3})$ has infinitely many irreducible elements.

The general proof will follow exactly the same line.

3. Infiniteness of SAGBI basis of permutation invariants

Let $<$ be an admissible term order on $\mathbb{K}[x]$; without loss of generality, we may assume that $x_1 > x_2 > \cdots > x_n$. By the classical characterization of admissible term orders (see [CLO97]), there exists n linearly independent linear forms $l_1, \ldots, l_n$ in $\mathbb{R}^n \mapsto \mathbb{R}$ such that $x^u > x^v$ if, and only if,

$$(l_1(u), \ldots, l_n(u)) >_{\text{lex}} (l_1(v), \ldots, l_n(v)).$$

Then, a monomial x^u is in the initial algebra $\text{in}_<(\mathbb{K}[x]^G)$ if, and only if, $x^u \geq g.x^u$, for all $g \in G$, that is

$$(l_1(u), \ldots, l_n(u)) \geq_{\text{lex}} (l_1(g.u), \ldots, l_n(g.u)), \qquad \text{for all } g \in G$$

We define the *initial convex cone* $C := C_<(\mathbb{K}[x]^G)$ to be the convex cone of ${\mathbb{R}^+}^n$ defined by those inequations:

$$(l_1(u - g.u), \ldots, l_n(u - g.u)) \geq_{\text{lex}} (0, \ldots, 0), \qquad \text{for all } g \in G,$$

so that $\text{in}_{\text{lex}}(\mathbb{K}[x]^G)$ is the integral cone of C. It is well known that any *non-increasing* monomial (monomial x^u such that $u_1 \geq u_2 \geq \cdots \geq u_n$) is in C; it is the initial monomial of the corresponding symmetric function. Hence, $(1, 0, \ldots, 0)$, $(1, 1, 0, \ldots, 0)$, $(1, \ldots, 1)$ are in C, and C spans $\mathbb{R}^n$ as a vector space.

We now turn to the proof of theorem 1.2.

Proof. Let G be a permutation group. Assume that C is closed, while G is not generated by reflections. Then, there exists $a < b$ such that the transposition (a, b) is not in G, while a is in the G-orbit of b. Choose such a pair $a < b$ with b minimal. We claim that there is no transposition (a', b) in G with $a' < b$. Otherwise, a and a' are in the same G-orbit, and by minimality of b, $(a, a') \in G$; thus, $(a, b) = (a, a')(a', b)(a, a') \in G$. Pick $g \in G$ such that $g.b = a$, and define

$$u_t := ((n-1)t,\ (n-2)t,\ \ldots,\ (n-b+1)t,\ n-b,\ (n-b-1)t,\ \ldots,\ t,\ 0).$$

Note that $u_0 < g.u_0$, so $u_0 \notin C$, whereas $u_1 \in C$. Furthermore, the entries of u_t are all distinct, except when $t = \frac{n-b}{n-a'}$ for some $a' < b$, in which case the a'-th and b-th entries are equal. Since $(a', b) \notin G$, for any t, $0 < t \leq 1$, the orbit of u_t is of size $|G|$, and there exists a unique permutation $\sigma_t \in G$ such that $\sigma_t.u_t$ is in C.

Let $t_0 = \inf\{t \geq 0, u_t \in C\}$. If $u_{t_0} \notin C$, then u_{t_0} is in the closure of C, but not in C, a contradiction. Otherwise, $u_{t_0} \in C$, and $t_0 > 0$ because $u_0 \notin C$. For any permutation σ, $\{\sigma.u_t, t \geq 0\}$ is a half-line; so, C being convex and closed, $I_\sigma := \{t, \sigma.u_t \in C\}$ is a closed interval $[x_\sigma, y_\sigma]$. For example, $I_{\mathrm{id}} = [t_0, 1] \subsetneq [0, 1]$. Since the interval $[0, 1]$ is the union of all the I_σ, there exists $\sigma \neq \mathrm{id}$ such that $t_0 \in I_\sigma$. This contradicts the uniqueness of σ_{t_0}. □

4. Conclusion

Let a be a real number. The convex cone in ${\mathbb{R}^+}^2$ of all (x, y) such that $y > ax$ is a very simple geometrical object; yet, its integer monoid has a very rich structure, the irreducible elements being essentially the famous Sturm words. The very same phenomenon appears for SAGBI basis of permutation groups, and explains the tediousness of the ad hoc constructions of infinite sequences of irreducible elements in [Göb99b, Göb99a, Göb00]. Thus, the proof of theorem 1.2 suggests that looking at the geometry of the initial convex cone is the proper tool to obtain further information on SAGBI basis of permutation groups.

References

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[Göb98] Manfred Göbel. A constructive description of SAGBI bases for polynomial invariants of permutation groups. *J. Symbolic Comput.*, 26(3):261–272, 1998.

[Göb99a] 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(2):65–70 (electronic), 1999.

[Göb99b] Manfred Göbel. The "smallest" ring of polynomial invariants of a permutation group which has no finite SAGBI bases w.r.t. any admissible order. *Theoret. Comput. Sci.*, 225(1-2):177–184, 1999.

[Göb00] Manfred Göbel. Rings of polynomial invariants of the alternating group have no finite SAGBI bases with respect to any admissible order. *Inform. Process. Lett.*, 74(1-2):15–18, 2000.

[KM89] Deepak Kapur and Klaus Madlener. A completion procedure for computing a canonical basis for a k-subalgebra. In *Computers and mathematics (Cambridge, MA, 1989)*, pages 1–11. Springer, New York, 1989.

[Kur02] Shigeru Kuroda. The infiniteness of the sagbi basis for certain invariant rings. *Osaka Journal of Mathematics*, (39):665–680, 2002.

[Rei02] Zinovy Reichstein. SAGBI basis in rings of multiplicative invariants. *Commentarii Math. Helvetici*, 2002. To appear.

[RS90] Lorenzo Robbiano and Moss Sweedler. Subalgebra bases. In *Commutative algebra (Salvador, 1988)*, pages 61–87. Springer, Berlin, 1990.

[Stu96] Bernd Sturmfels. *Gröbner bases and convex polytopes.* American Mathematical Society, Providence, RI, 1996.

[SW02] R. James Shank and David Wehlau. Computing modular invariants of p-groups. *Journal of Symbolic Computation*, 2002. Submitted.

[Thi01] Nicolas M. Thiéry. Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis. In *Discrete models: combinatorics, computation, and geometry (Paris, 2001)*, Discrete Math. Theor. Comput. Sci. Proc., AA, pages 315–328 (electronic). Maison Inform. Math. Discrèt. (MIMD), Paris, 2001.

E-mail address: `nthiery@users.sf.net, Stephan.Thomasse@univ-lyon1.fr`