AN EVALUATION APPROACH TO COMPUTING INVARIANTS RINGS OF PERMUTATION GROUPS

NICOLAS BORIE AND NICOLAS M. THIÉRY

Abstract. Using evaluation at appropriately chosen points, we propose a Gröbner basis free approach for calculating the secondary invariants of a finite permutation group. This approach allows for exploiting the symmetries to confine the calculations into a smaller quotient space, which gives a tighter control on the algorithmic complexity, especially for large groups. This is confirmed by extensive benchmarks using a `Sage` implementation.

1. Introduction

Invariant theory has been a rich and central area of algebra ever since the eighteenth theory, with practical applications [DK02, § 5] in the resolution of polynomial systems with symmetries (see e.g. [Col97a], [Gat90], [Stu93, § 2.6], [FR09]), in effective Galois theory (see e.g. [Col97b], [Abd00], [GK00]), or in discrete mathematics (see e.g. [Thi00, PT01] for the original motivation of the second author). The literature contains deep and explicit results for special classes of groups, like complex reflection groups or the classical reductive groups, as well as general results applicable to any group. Given the level of generality, one cannot hope for such results to be simultaneously explicit and tight in general. Thus the subject was effective early on: given a group, one wants to *calculate* the properties of its invariant ring. Under the impulsion of modern computer algebra, computational methods, and their implementations, have largely expanded in the last twenty years [Kem93, Stu93, Thi01, DK02, Kin07b, Kin07a]. However much progress is still needed to go beyond toy examples and enlarge the spectrum of applications.

An important obstruction is that the algorithms depend largely on efficient computations in certain quotients of the invariant ring; this is usually carried out using elimination techniques (Gröbner or SAGBI-Gröbner bases), but those do not behave well with respect to symmetries. An emerging trend is the alternative use of evaluation techniques, for example to rewrite invariants in terms of an existing generating set of the invariant ring [GST06, DSW09].

In this paper, and as a test bed, we focus on the problem of computing secondary invariants of finite permutation groups in the non modular case, using evaluation techniques.

In Section 2, we review some relevant aspects of computational invariant theory, and in particular discuss the current limitations due to quotient computations. In Section 3, we give a new theoretical characterization of secondary invariants in term of their evaluations on as many appropriately chosen points; this is achieved by perturbating slightly the quotient, and using the grading to transfer back results. In Section 4, we derive an algorithm for computing secondary invariants of permutation groups. We establish in Section 5 a worst case complexity bound for this

algorithm. This bound suggests that, for a large enough group G, at least a factor of $|G|$ is gained. This comparison remains however sloppy since, to the best of our knowledge and due to the usual lack of fine control on the complexity of Gröbner bases methods, no meaningful bound exists in the literature for the elimination based algorithms. Therefore, in Section 6 we complement this theoretical analysis with extensive benchmarks comparing in particular our implementation in `Sage` and the elimination-based implementation in `Singular`'s [GPS98, Kin07b]. Those benchmarks suggest a practical complexity which, for large enough groups, is cubic in the size $n!/|G|$ of the output. And indeed, if the evaluation-based implementation can be order of magnitudes slower for some small groups, it treats predictably large groups which are completely out of reach for the elimination-based implementation. This includes an example with $n = 14$, $|G| = 50,803,200$, and 1716 secondary invariants.

We conclude, in Section 7, with a discussion of avenues for further improvements.

2. Preliminaries

We refer to [Sta79, Stu93, CLO97, Smi97, Kem98, DK02] for classical literature on invariant theory of finite groups. Parts of what follows are strongly inspired by [Kem98]. Let V be a $\mathbb{K}$-vector space of finite dimension n, and G be a finite subgroup of $\mathrm{GL}(V)$. Tacitly, we interpret G as a group of $n \times n$ matrices or as a representation on V. Two vectors v and w are *isomorphic*, or in the same *G-orbit* (for short *orbit*), if $\sigma \cdot v = w$ for some $\sigma \in G$.

Let $\mathbf{x} := (x_1, \dots, x_n)$ be a basis of the dual of V, and let $\mathbb{K}[\mathbf{x}]$ be the ring of polynomials over V. The action of G on V extends naturally to an action of G on $\mathbb{K}[\mathbf{x}]$ by $\sigma \cdot p := p \circ \sigma^{-1}$. An *invariant polynomial*, or *invariant*, is a polynomial $p \in K[x_1, \dots, x_n]$ such that $\sigma \cdot p = p$ for all $\sigma \in G$. The *invariant ring* $\mathbb{K}[\mathbf{x}]^G$ is the set of all invariants. Since the action of G preserves the degree of polynomials, it is a graded connected commutative algebra: $\mathbb{K}[\mathbf{x}]^G = \bigoplus_{d \geq 0} \mathbb{K}[\mathbf{x}]^G_d$, with $\mathbb{K}[\mathbf{x}]^G_0 \approx \mathbb{K}$. We write $\mathbb{K}[\mathbf{x}]^G_+ = \bigoplus_{d>0} \mathbb{K}[\mathbf{x}]^G_d$ for the positive part of the invariant ring. The *Hilbert series* of $\mathbb{K}[\mathbf{x}]^G$ is the generating series of its dimensions:

$$H(\mathbb{K}[\mathbf{x}]^G, z) := \sum_{d=0}^{\infty} z^d \dim \mathbb{K}[\mathbf{x}]^G_d \,.$$

It can be calculated using Molien's formula:

$$H(\mathbb{K}[\mathbf{x}]^G, z) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(\mathrm{Id} - zM)} \,.$$

This formula reduces to Pólya enumeration for permutation groups. Furthermore, the summation can be taken instead over conjugacy classes of G, which is relatively cheap in practice.

A crucial device is the Reynolds operator:

$$\begin{array}{rccc} R: & \mathbb{K}[\mathbf{x}] & \longrightarrow & \mathbb{K}[\mathbf{x}]^G \\ & p & \longmapsto & \frac{1}{|G|} \sum_{g \in G} g \cdot p \,, \end{array}$$

which is both a graded projection onto $\mathbb{K}[\mathbf{x}]^G$ and a morphism of $\mathbb{K}[\mathbf{x}]^G$-module. Note that its definition requires $\mathrm{char}\,\mathbb{K}$ not to divide $|G|$, which we assume from now on (non-modular case).

Hilbert's fundamental theorem of invariant theory states that $\mathbb{K}[\mathbf{x}]^G$ is finitely generated: there exists a finite set S of invariants such that any invariant can be expressed as a polynomial combination of invariants in S. We call S a *generating set*. If no proper subset of S is generating, S is a *minimal generating set*. Since $\mathbb{K}[\mathbf{x}]^G$ is finitely generated, there exists a degree bound d such that $\mathbb{K}[\mathbf{x}]^G$ is generated by the set of all invariants of degree at most d. We denote by $\beta(\mathbb{K}[\mathbf{x}]^G)$ the *smallest degree bound*. Noether proved that $\beta(\mathbb{K}[\mathbf{x}]^G) \leq |G|$.

Thanks to the grading, for M a set of homogeneous invariants, the following properties are equivalent:

(i) M is a minimal generating set for $\mathbb{K}[\mathbf{x}]^G$;
(ii) M is a basis of the quotient $\mathbb{K}[\mathbf{x}]^G/\mathbb{K}[\mathbf{x}]^{G^2}_+$.

Therefore, even though the generators in M are non canonical, the number of generators of a given degree d in M is: it is given by the dimension of the component of that degree in the graded quotient $\mathbb{K}[\mathbf{x}]^G/\mathbb{K}[\mathbf{x}]^{G^2}_+$. There is no known algorithm to compute those dimensions, or even just $\beta(\mathbb{K}[\mathbf{x}]^G)$, without computing explicitly a minimal generating set.

The previous properties give immediately a naive algorithm for computing an homogeneous minimal generating set, calculating degree by degree in the finite dimensional quotient up to Noether's bound. There are however two practical issues. The first one is that Noether's bound is tight only for cyclic groups; in general it is very dull, possibly by orders of magnitude. The second issue is how to compute efficiently in the given quotient. We will get back to it.

By a celebrated result of Shepard, Todd, Chevalley, and Serre, $\mathbb{K}[\mathbf{x}]^G$ is a polynomial algebra if and only if G is a complex reflection group. In all other cases, there are non trivial relations (also called syzygies) between the generators; however $\mathbb{K}[\mathbf{x}]^G$ remains *Cohen-Macaulay*. Namely, a set of m homogeneous invariants $(\theta_1, \ldots, \theta_n)$ of $\mathbb{K}[\mathbf{x}]^G$ is called a *homogeneous system of parameters* or, for short, a *system of parameters* if the invariant ring $\mathbb{K}[\mathbf{x}]^G$ is finitely generated over its subring $\mathbb{K}[\theta_1, \ldots, \theta_n]$. That is, if there exist a finite number of invariants $(\eta_1, \ldots, \eta_t)$ such that the invariant ring is the sum of the subspaces $\eta_i.\mathbb{K}[\theta_1, \ldots, \theta_n]$. By Noether's normalization lemma, there always exists a system of parameters for $\mathbb{K}[\mathbf{x}]^G$. Moreover, $\mathbb{K}[\mathbf{x}]^G$ is *Cohen-Macaulay*, which means that $\mathbb{K}[\mathbf{x}]^G$ is a free-module over any system of parameters. Hence, if the set $(\eta_1, \ldots, \eta_t)$ is minimal for inclusion, $\mathbb{K}[\mathbf{x}]^G$ decomposes into a direct sum:

$$\mathbb{K}[\mathbf{x}]^G = \bigoplus_{i=1}^{t} \eta_i.\mathbb{K}[\theta_1, \ldots, \theta_n].$$

This decomposition is called a *Hironaka decomposition* of the invariant ring. The θ_i are called *primary invariants*, and the η_i *secondary invariants* (in algebraic combinatorics literature, the θ_i are some times called *quasi-generators* and the η_i *separators* [GS84]). It should be emphasized that primary and secondary invariants are not uniquely determined, and that being a primary or secondary invariant is not an intrinsic property of an invariant p, but rather express the role of p in a particular generating set.

The primary and secondary invariants together form a generating set, usually non minimal. From the degrees $(d_1, \ldots, d_n)$ of the primary invariants $(\theta_1, \ldots, \theta_n)$ and the Hilbert series we can compute the number t and the degrees $(d'_1, \ldots, d'_t)$ of

the secondary invariants $(\eta_1, \dots, \eta_t)$ by the formula:

$$z^{d'_1} + \cdots + z^{d'_t} = (1 - z^{d_1}) \cdots (1 - z^{d_n}) H(\mathbb{K}[\mathbf{x}]^G, z)\,.$$

We denote this polynomial by $S(\mathbb{K}[\mathbf{x}]^G, z)$. Assuming $d_1 \leq \cdots \leq d_n$ and $d'_1 \leq \cdots \leq d'_t$, it can be proved that:

$$t = \frac{d_1 \cdots d_n}{|G|}\,, \qquad d'_t = d_1 + \cdots + d_n - n - \mu\,, \qquad \beta(\mathbb{K}[\mathbf{x}]^G) \leq \max(d_n, d'_t)\,,$$

where μ is the smallest degree of a polynomial p such that $\sigma \cdot p = \det(\sigma) p$ for all $\sigma \in G$ [Sta79, Proposition 3.8].

For example, if G is the symmetric group $\mathfrak{S}_n$, the n elementary symmetric polynomials (or the n first symmetric power sums) form a system of parameters, $t = 1$, $d'_t = 0$ and $\eta_1 = 1$. This is consistent with the fundamental theorem of symmetric polynomials. More generally, if G is a permutation group, the elementary symmetric polynomials still form a system of parameters: $\mathbb{K}[\mathbf{x}]^G$ is a free module over the algebra $\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[\mathbf{x}]^{\mathfrak{S}_n}$ of symmetric polynomials. It follows that:

$$t = \frac{n!}{|G|}\,, \qquad d'_t = \binom{n}{2} - \mu\,, \qquad \beta(\mathbb{K}[\mathbf{x}]^G) \leq \binom{n}{2}\,.$$

For a review of algorithms to compute primary invariants with minimal degrees, see [DK02]. They use Gröbner bases, exploiting the property that a set $\Theta_1, \dots, \Theta_n$ of n homogeneous invariants forms a system of parameters if and only if $\mathbf{x} = 0$ is the single solution of the system of equations $\Theta_1(\mathbf{x}) = \cdots = \Theta_n(\mathbf{x}) = 0$ (see e.g. [DK02, Proposition 3.3.1]).

We focus here on the second step: we assume that primary invariants $\Theta_1, \dots, \Theta_n$ are given as input, and want to compute secondary invariants. This is usually achieved by using the following proposition to reduce the problem to linear algebra.

Proposition 2.1. *Let $\Theta_1, \dots, \Theta_n$ be primary invariants and $S := (\eta_1, \dots, \eta_t)$ be a family of homogeneous invariants with the appropriate degrees. Then, the following are equivalent:*

(i) S is a family of secondary invariants;
(ii) S is a basis of the quotient $\mathbb{K}[\mathbf{x}]^G / \langle \Theta_1, \dots, \Theta_n \rangle_{\mathbb{K}[\mathbf{x}]^G}$;
(iii) S is free in the quotient $\mathbb{K}[\mathbf{x}] / \langle \Theta_1, \dots, \Theta_n \rangle_{\mathbb{K}[\mathbf{x}]}$.

The central problem is how to compute efficiently inside one of the quotients $\mathbb{K}[\mathbf{x}] / \langle \Theta_1, \dots, \Theta_n \rangle_{\mathbb{K}[\mathbf{x}]}$ or $\mathbb{K}[\mathbf{x}]^G / \langle \Theta_1, \dots, \Theta_n \rangle_{\mathbb{K}[\mathbf{x}]^G}$. Most algorithms rely on *(iii)* using normal form reductions w.r.t. the Gröbner basis for $\Theta_1, \dots, \Theta_n$ which was calculated in the first step to prove that they form a system of parameters. The drawback is that Gröbner basis and normal form calculations do not preserve symmetries; hence they cannot be used to confine the calculations into a small subspace of $\mathbb{K}[\mathbf{x}] / \langle \Theta_1, \dots, \Theta_n \rangle_{\mathbb{K}[\mathbf{x}]}$. Besides, even the Gröbner basis calculation itself can be intractable for moderate size input ($n = 8$) in part due to the large multiplicity $(d_1 \cdots d_n)$ of the unique root $\mathbf{x} = 0$ of this system.

An other approach is to use *(ii)*. Then, in many cases, one can make use of the symmetries to get a compact representation of invariant polynomials. For example, if G is a permutation group, an invariant can be represented as a linear combination of orbitsums instead of a linear combination of monomials, saving a factor of up to $|G|$ (see e.g. [Thi01]). Furthermore, one can use SAGBI-Gröbner bases (an analogue of Gröbner basis for ideals in subalgebras of polynomial rings) to compute in the

quotient (see [Thi01, FR09]). However SAGBI and SAGBI-Gröbner basis tend to be large (in fact, they are seldom finite, see [TT04]), even when truncated.

In both cases, it is hard to derive a meaningful bound on the complexity of the algorithm, by lack of control on the behavior of the (SAGBI)-Gröbner basis calculation. In the following section, we propose to calculate in the quotient $\mathbb{K}[\mathbf{x}]^G/\langle\Theta_1,\dots,\Theta_n\rangle_{\mathbb{K}[\mathbf{x}]^G}$ using instead evaluation techniques.

3. Quotienting by evaluation

Recall that, in the good cases, an efficient mean to compute modulo an ideal is to use evaluation on its roots.

Proposition 3.1. *Let P be a system of polynomials in $\mathbb{K}[\mathbf{x}]$ admitting a finite set $\boldsymbol{\rho}_1,\dots,\boldsymbol{\rho}_r$ of multiplicity-free roots, and let I be the dimension 0 ideal they generate. Endow further $\mathbb{K}^r$ with the pointwise (Hadamard) product. Then, the evaluation map:*

$$\begin{array}{rccc}\Phi: & \mathbb{K}[\mathbf{x}] & \longrightarrow & \mathbb{K}^r \\ & p & \longmapsto & (p(\boldsymbol{\rho}_1),\dots,p(\boldsymbol{\rho}_r))\end{array}$$

induces an isomorphism of algebra from $\mathbb{K}[\mathbf{x}]/I$. In particular, $\mathbb{K}[\mathbf{x}]/I$ is a semi-simple basic algebra, a basis of which is given by the r idempotents $(p_i)_{i=1,\dots,r}$ which satisfy $p_i(\boldsymbol{\rho}_j)=\delta_{i,j}$; those idempotents can be constructed by multivariate Lagrange interpolation, or using the Buchberger-Möller algorithm [MB82].

This proposition does not apply directly to the ideal $\langle\Theta_1,\dots,\Theta_n\rangle$ because it has a single root with a very high multiplicity $d_1\dots d_n$. The central idea of this paper is to blowup this single root by considering instead the ideal $\langle\Theta_1,\dots,\Theta_{n-1},\Theta_n-\epsilon\rangle$, where ϵ is a non zero constant, and then to show that the grading can be used to transfer back the result to the original ideal, modulo minor complications. This approach is a priori general: assuming the field is large enough, the ideal $\Theta_1,\dots,\Theta_n$ can always be slightly perturbed to admit $d_1\cdots d_n$ multiplicity-free roots; those roots are obviously stable under the action of G, and can be grouped into orbits. Yet it can be non trivial to compute and describe those roots.

For the sake of simplicity of exposition, we assume from now on that G is a permutation group, that $\Theta_1,\dots,\Theta_n$ are the elementary symmetric functions $e_1,\dots,e_n$, and that $\epsilon=(-1)^{n+1}$. Finally we assume that the ground field $\mathbb{K}$ contains the n-th roots of unity; this last assumption is reasonable as, roughly speaking, the invariant theory of a group depends only on the characteristic of $\mathbb{K}$. With those assumptions, the roots $\boldsymbol{\rho}_i$ take a particularly nice and elementary form, and open connections with well know combinatorics. Yet we believe that this case covers a wide enough range of groups (and applications) to contain all germs of generality. In particular, the results presented here should apply mutatis mutandis to any subgroup G of a complex reflection group.

Remark 3.2. *Let ρ be a n-th primitive root of unity, and set $\boldsymbol{\rho}:=(1,\rho,\dots,\rho^{n-1})$. Then, $e_1(\boldsymbol{\rho})=\cdots=e_{n-1}(\boldsymbol{\rho})=0$ and $e_n(\boldsymbol{\rho})=\epsilon$.*

Proof. Up to sign, $e_i(\boldsymbol{\rho})$ is the i-th coefficient of the polynomial

$$(X^n-1)=\prod_{i=0}^{n-1}(X-\rho^i)\,.$$

□

For $\sigma \in \mathfrak{S}_n$, write $\boldsymbol{\rho}_\sigma := \sigma \cdot \boldsymbol{\rho}$ the permuted vector. It follows from the previous remark that the orbit $(\boldsymbol{\rho}_\sigma)_{\sigma\in\mathfrak{S}_n}$ of $\boldsymbol{\rho}$ gives all the roots of the system

$$e_1(\mathbf{x}) = \cdots = e_{n-1}(\mathbf{x}) = e_n(\mathbf{x}) - \epsilon = 0\,.$$

Let $\mathcal{I}$ be the ideal generated by $e_1, \ldots, e_{n-1}, e_n - \epsilon$ in $\mathbb{K}[\mathbf{x}]$, that is the ideal of symmetric relations among the roots of the polynomial $X^n - 1$; it is well known that the quotient $\mathbb{K}[\mathbf{x}]/\mathcal{I}$ is of dimension $n!$. We define the evaluation map $\Phi : p \in \mathbb{K}[\mathbf{x}] \mapsto (p(\boldsymbol{\rho}_\sigma))_\sigma$ as in Proposition 3.1 to realize the isomorphism from $\mathbb{K}[\mathbf{x}]/\mathcal{I}$ to $\mathcal{E} = \mathbb{K}^{\mathfrak{S}_n}$.

Obviously, the evaluation of an invariant polynomial p is constant along G-orbits. This simple remark is the key for confining the quotient computation into a small subspace of dimension $n!/|G|$, which is precisely the number of secondary invariants. Let $\mathcal{E}^G$ be the subalgebra of the functions in $\mathcal{E}$ which are constant along G-orbits. Obviously, $\mathcal{E}^G$ is isomorphic to $\mathbb{K}^L$ where L is any transversal of the right cosets in $\mathfrak{S}_n/G$. Let $\mathcal{I}^G$ be the ideal generated by $(e_1, \ldots, e_{n-1}, e_n - \epsilon)$ in $\mathbb{K}[\mathbf{x}]^G$; as the notation suggests, it is the subspace of invariant polynomials in $\mathcal{I}$.

Remark 3.3. *The restriction of Φ on $\mathbb{K}[\mathbf{x}]^G$, given by:*

$$\begin{array}{rccc} \Phi: & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathcal{E}^G \\ & p & \longmapsto & (p(\boldsymbol{\rho}_\sigma))_{\sigma\in L} \end{array}$$

is surjective and induces an algebra isomorphism between $\mathbb{K}[\mathbf{x}]^G/\mathcal{I}^G$ and $\mathcal{E}^G$.

Proof. For each evaluation point $\boldsymbol{\rho}_\sigma$, $\sigma \in L$, set

$$\overline{p}_{\boldsymbol{\rho}_\sigma} := \sum_{\tau\in\sigma G} p_{\boldsymbol{\rho}_\tau}\,,$$

where $p_{\boldsymbol{\rho}_\tau}$ is the Lagrange interpolator of Proposition 3.1. Then, their images $(\Phi(\overline{p}_{\boldsymbol{\rho}_\sigma}))_{\sigma\in L}$ are orthogonal idempotents and, by dimension count, form a basis of $\mathcal{E}^G$. □

From now on, we call evaluation points the family $(\boldsymbol{\rho}_\sigma)_{\sigma\in L}$.

We proceed by showing that the grading can be used to compute modulo the original ideal $\langle e_1, \ldots, e_n\rangle$, modulo minor complications.

Lemma 3.4. *Let G be a subgroup of $\mathfrak{S}_n$ and $\mathbb{K}$ be a field of characteristic 0 containing a primitive n-th root of unity. Let S be a set of secondary invariants w.r.t. the primary invariants $e_1, \ldots, e_n$, and write $\langle S\rangle_{\mathbb{K}}$ for the vector space they span (equivalently, one could choose a graded supplementary of the graded ideal $\langle e_1, \ldots, e_n\rangle$ in $\mathbb{K}[\mathbf{x}]^G$). Write S_d for the secondary invariants of degree d. Then,*

$$\begin{array}{rl} \text{for } 0 \leqslant d < n: & \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d\rangle_{\mathbb{K}})\,, \\ \text{for } d \geqslant n: & \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d\rangle_{\mathbb{K}}) \oplus \Phi(\mathbb{K}[\mathbf{x}]^G_{d-n})\,. \end{array}$$

In particular, Φ restricts to an isomorphism from $\langle S\rangle_{\mathbb{K}}$ to $\mathcal{E}^G$.

Proof. For ease of notation, we write the Hironaka decomposition by grouping the secondary invariants by degree:

$$\mathbb{K}[\mathbf{x}]^G = \bigoplus_{i=1}^{t} \eta_i \mathbb{K}[e_1, \ldots, e_n] = \bigoplus_{d=0}^{d_{\max}} \langle S_d\rangle_{\mathbb{K}} \mathbb{K}[e_1, \ldots, e_n]\,,$$

where $d_{\max}$ is the highest degree of a secondary invariant. Then, using that

$$\Phi(e_1) = \cdots = \Phi(e_{n-1}) = 0_{\mathcal{E}^G} \quad \text{and} \quad \Phi(e_n) = 1_{\mathcal{E}^G}\,,$$

we get that $\Phi(\mathbb{K}[e_1,\dots,e_n]) = \Phi(\mathbb{K}[e_n]) = \mathbb{K}.1_{\mathcal{E}^G}$, and thus:

$$\mathcal{E}^G = \Phi(\mathbb{K}[\mathbf{x}]^G) = \sum_{d=1}^{d_{\max}} \Phi(\langle S_d\rangle_{\mathbb{K}})\Phi(\mathbb{K}[e_1,\dots,e_n]) = \sum_{d=1}^{d_{\max}} \Phi(\langle S_d\rangle_{\mathbb{K}})\,,$$

where, by dimension count, the sum is direct. Using further that e_n is of degree n:

$$\begin{aligned}\Phi(\mathbb{K}[\mathbf{x}]^G_d) &= \Phi(\langle S_d\rangle_{\mathbb{K}}) + \Phi(\langle S_{d-n}\rangle_{\mathbb{K}} e_n) + \Phi(\langle S_{d-2n}\rangle_{\mathbb{K}} e_n^2) + \cdots \\ &= \Phi(\langle S_d\rangle_{\mathbb{K}}) \oplus \Phi(\langle S_{d-n}\rangle_{\mathbb{K}}) \quad \oplus \Phi(\langle S_{d-2n}\rangle_{\mathbb{K}}) \quad \oplus \cdots\end{aligned}$$

The desired result follows by induction. □

In practice, this lemma adds to Proposition 2.1 two new equivalent characterizations of secondary invariants:

Theorem 3.5. *Let $G \subset \mathfrak{S}_n$ be a permutation group, take $e_1,\dots,e_n$ as primary invariants, and let $S = (\eta_1,\dots,\eta_t)$ be a family of homogeneous invariants with the appropriate degrees. Then, the following are equivalent:*

(i) S is a set of secondary invariants;
(iv) $\Phi(S)$ forms a basis of $\mathcal{E}^G$;
(v) The elements of $\Phi(S_d)$ are linearly independent in $\mathcal{E}^G$, modulo the subspace

$$\sum_{0\le j<d,\ n\,|\,d-j} \langle \Phi(S_j)\rangle_{\mathbb{K}}\,.$$

Furthermore, when any, and therefore all of the above hold, the sum in (v) is a direct sum.

Proof. Direct application of Lemma 3.4, together with recursion for the direct sum. □

Example 3.6. *Let $G = \mathcal{A}_3 = \langle(1,2,3)\rangle$ be the alternating group of order 3. In that case, ρ is the third root of unity j, and $\mathbb{K} = \mathbb{Q}(j) = \mathbb{Q} \oplus_{\mathbb{Q}} \mathbb{Q}.j \oplus_{\mathbb{Q}} \mathbb{Q}.j^2$. We are looking for $n!/|G| = 2$ secondary invariants, whose degree are given by the numerator of the Hilbert series:*

$$H(\mathbb{K}[\mathbf{x}]^G, z) = \frac{1}{3}\left(\frac{1}{(1-z)^3} + 2\frac{1}{(1-z^3)}\right) = \frac{1+z^3}{(1-z)(1-z^2)(1-z^3)}$$

Simultaneously, the $\mathfrak{S}_n$-orbit of $(1,\rho,\rho^2)$ splits in two G-orbits. We can, for example, take as evaluation points the two G-orbit representatives $\boldsymbol{\rho}_{()} = (1,\rho,\rho^2)$ and $\boldsymbol{\rho}_{(2,1)} = (\rho,1,\rho^2)$, and the evaluation morphism is given by:

$$\begin{array}{rccl}\Phi: & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathcal{E}^G = \mathbb{K}^2 \\ & p & \longmapsto & (p(\boldsymbol{\rho}_{()}), p(\boldsymbol{\rho}_{(1,2)}))\end{array}$$

For example, $\Phi(1) = \Phi(e_3) = (1,1)$, whereas $\Phi(e_1) = \Phi(e_2) = 0$. Let us evaluate the orbitsum of the monomial $x_1^2x_2 = \mathbf{x}^(2,1,0)$, using Remark 4.4:

$$\begin{aligned}o(\mathbf{x}^{(2,1,0)})(\boldsymbol{\rho}_{()}) &= j^{\langle(2,1,0),(0,1,2)\rangle} + j^{\langle(2,1,0),(1,2,0)\rangle} + j^{\langle(2,1,0),(2,0,1)\rangle} = 3j\,, \\ o(\mathbf{x}^{(2,1,0)})(\boldsymbol{\rho}_{(1,2)}) &= j^{\langle(2,1,0),(1,0,2)\rangle} + j^{\langle(2,1,0),(0,2,1)\rangle} + j^{\langle(2,1,0),(2,1,0)\rangle} = 3j^2\,.\end{aligned}$$

That is $\Phi(o(x_1^2x_2)) = 3.(j, j^2)$. *It follows that:*

$$\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \mathbb{K}.(1,1)$$
$$\Phi(\mathbb{K}[\mathbf{x}]_1^G) = \Phi(\mathbb{K}[\mathbf{x}]_2^G) = \{(0,0)\}$$
$$\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \mathbb{K}.(1,1) \oplus \mathbb{K}.(3,3) = \mathbb{K}.\Phi(1) \oplus \mathbb{K}.\Phi(o(x_1^2x_2))\,.$$

In particular, 1 *and* $o(x_1^2x_2)$ *are two secondary invariants, both over* $\mathbb{K}$ *or* $\mathbb{Q}$*:*

$$\mathbb{K}[\mathbf{x}]^G = \mathrm{Sym}(\mathbf{x}) \oplus \mathrm{Sym}(\mathbf{x}).o(x_1^2x_2)\,.$$

We consider now the two extreme cases. For $G = \mathfrak{S}_n$*, there is a single evaluation point and a single secondary invariant* 1*; and indeed,* $\Phi(1) = (1)$ *spans* $\Phi(\mathbb{K}[\mathbf{x}]^G) = \mathbb{K}$. *Take now* $G = \{()\}$ *the trivial permutation group on* n *points. Then, the evaluation points are the permutations of* $(1, j, j^2, \ldots, j^{n-1})$. *In that case, Theorem 3.5 states in particular that the matrix* $(j^{\langle m,\sigma\rangle})_{m,\sigma}$*, where* m *and* σ *run respectively through the integer vectors below the staircase and through* $\mathfrak{S}_n$*, is non singular.*

4. An algorithm for computing secondary invariants by evaluation

Algorithm 1 is a straightforward adaptation of the standard algorithm to compute secondary invariants in order to use the evaluation morphism Φ together with Theorem 3.5.

For the sake of the upcoming complexity analysis, we now detail how the required new invariants in each degree can be generated and evaluated in the case of a permutation group.

It is well known that the ring $\mathbb{K}[\mathbf{x}]$ is a free $\mathrm{Sym}(\mathbf{x})$-module of rank $n!$. It admits several natural bases over $\mathrm{Sym}(\mathbf{x})$, including the Schubert polynomials, the descent monomials, and the monomials under the staircase. We focus on the later. Namely, encoding a monomial $m = \mathbf{x}^\alpha$ in $\mathbb{K}[\mathbf{x}]$ by its exponent vector $\alpha = (\alpha_1, \ldots, \alpha_n)$, m is *under the staircase* if $\alpha_i \leqslant n - i$ for all $1 \leqslant i \leqslant n$. Given a permutation group $G \subset \mathfrak{S}_n$, a monomial m is *canonical* if m is maximal in its G-orbit for the lexicographic order: $\sigma(m) \leqslant_{\mathrm{lex}} m$, $\forall \sigma \in G$. The following lemma is a classical consequence of the Reynolds operator being a $\mathbb{K}[\mathbf{x}]^G$-module morphism.

Lemma 4.1. *Let* M *be a family of polynomials which spans* $\mathbb{K}[\mathbf{x}]$ *as a* $\mathrm{Sym}(\mathbf{x})$*-module. Then, the set of invariants* $\{R(m) \mid m \in M\}$ *spans* $\mathbb{K}[\mathbf{x}]^G$ *as a* $\mathrm{Sym}(\mathbf{x})$ *module.*

In particular, taking for M *the set of monomials under the staircase, one gets that the orbitsums of monomials which are simultaneously canonical and under the staircase generate* $\mathbb{K}[\mathbf{x}]^G$ *as a* $\mathrm{Sym}(\mathbf{x})$*-module. One can further remove non zero integer partitions from this set.*

Proof. Let $p \in \mathbb{K}[\mathbf{x}]^G$ be an invariant polynomial, and write it as $p = \sum_{m\in M} f_m m$, where the f_m are symmetric polynomials. Then, using that the Reynolds operator R is a $\mathbb{K}[\mathbf{x}]^G$-module morphism, one gets as desired that:

$$p = R(p) = R(\sum_{m\in M} f_m m) = \sum_{m\in M} f_m R(m)\,. \qquad \square$$

Remark 4.2. *The canonical monomials under the staircase can be iterated through efficiently using orderly generation* [Rea78, McK98] *and a strong generating system of the group* G [Ser03]*; the complexity of this iteration can be safely bounded*

Algorithm 1 Computing secondary invariants and irreducible secondary invariants of a permutation group G, w.r.t. the symmetric functions as primary invariants, and using the evaluation morphism Φ.

We assume that the following have been precomputed from the Hilbert series:

- s_d: the number of secondary invariants of degree d
  (this is the coefficient of degree d of $S(\mathbb{K}[\mathbf{x}]^G, z)$)
- e_d: the dimension of $\dim \Phi(\mathbb{K}[\mathbf{x}]_d^G)$
  (this is s_d if $d < n$ and $e_{d-n} + s_d$ otherwise)

At the end of each iteration of the main loop:

- S_d is a set S_d of secondary invariants of degree d;
- I_d is a set of irreducible secondary invariants of degree d;
- E_d models the vector space $\Phi(\mathbb{K}[\mathbf{x}]_d^G)$.

Code, in pseudo-`Python` syntax:

```
def SecondaryInvariants(G) :
    for d ∈ {0, 1, 2, ..., deg(S(K[x]^G, z))} :
        I_d = {}
        S_d = {}
        if d ⩾ n :
            E_d = E_{d-n}        #Defect of direct sum of Theorem 3.5
        else :
            E_d = {0⃗}
        # Consider all products of secondary invariants of lower degree
        for (η, η') ∈ S_k × I_l  with k + l = d :
            if Φ(ηη') ∉ E_d :
                S_d = S_d ∪{ηη'}
                E_d = E_d ⊕K.Φ(ηη')
        # Complete with orbitsums of monomials under the staircase
        for m ∈ CanonicalMonomialsUnderStaircaseOfDegree(d) :
            if dim E_d == e_d :
                break      #All secondary invariants were found
            η = OrbitSum(m)
            if Φ(η) ∉ E_d :
                I_d = I_d ∪{η}
                S_d = S_d ∪{η}
                E_d = E_d ⊕K.Φ(η)
    return ({S_0, S_1, ...}, {I_0, I_1, ...})
```

above by $\mathcal{O}(n!)$, though in practice it is much better than that (see Figures 4 and 4, and [Nic11] *for details).*

Remark 4.3. *Let $\mathbf{x}^\alpha$ be a monomial. Then, evaluating it on a point $\boldsymbol{\rho}_\sigma$ requires at most $\mathcal{O}(n)$ arithmetic operations in $\mathbb{Z}$. Assume indeed that ρ^k has been precomputed in $\mathbb{K}$ and cached for all k in $0, \ldots, n-1$; then, one can use:*

$$\mathbf{x}^\alpha(\boldsymbol{\rho}_\sigma) = \rho^{\langle \alpha | \sigma \rangle \mod n},$$

where σ is written, in the scalar product, as a permutation of $\{0, \ldots, n-1\}$.

Remark 4.4. *Currently, the evaluation of the orbitsum $o(\mathbf{x}^\alpha)$ of a monomial on a point $\boldsymbol{\rho}_\sigma$ is carried out by evaluating each monomial in the orbit. This gives a*

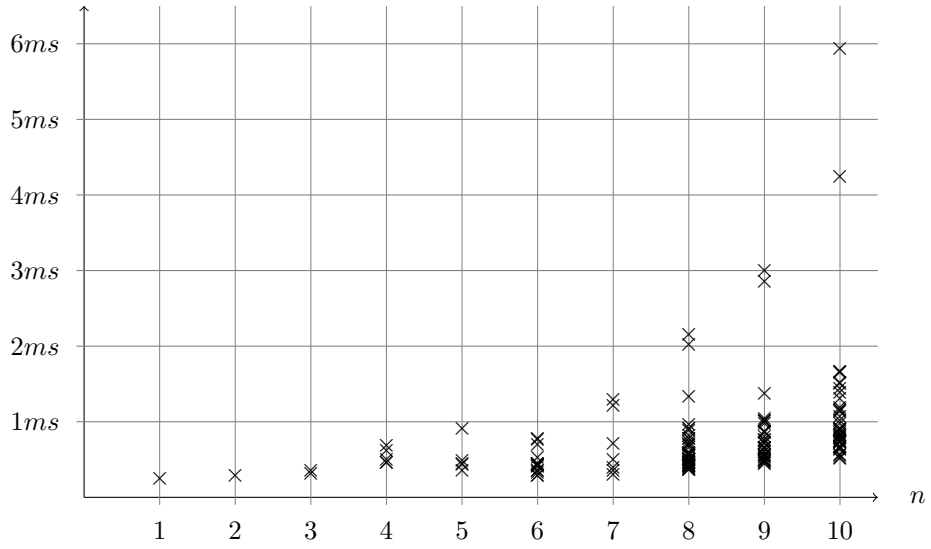

FIGURE 1. This figure plots, for $n \leq 10$ and for each transitive permutation group $G \subset \mathfrak{S}_n$, the average computation time per canonical integer vectors below the staircase. If one ignores the two top groups for each n (which correspond to $\mathfrak{A}_n$ and $\mathfrak{S}_n$ respectively), the worst case complexity is seemingly roughly linear in the size of the result: $\mathcal{O}(nC(G))$.

complexity of $\mathcal{O}(n|G|)$ arithmetic operations in $\mathbb{Z}$ (for counting how many times each ρ^k appears in the result) and $\mathcal{O}(n)$ additions in $\mathbb{K}$ (for expressing the result in $\mathbb{K}$). This can be roughly bounded by $\mathcal{O}(|G|)$ arithmetic operations in $\mathbb{K}$. This bounds the complexity of calculating $\Phi(o(\mathbf{x}^\alpha))$ on all $\frac{n!}{|G|}$ points by $\frac{n!}{|G|}\mathcal{O}(|G|) = \mathcal{O}(n!)$.

This worst case complexity gives only a very rough overestimate of the average complexity in our application. Indeed, in practice, most of the irreducible secondary invariants are of low degree; thus Algorithm 1 only need to evaluate orbitsums of monomials m of low degree; such monomials have many multiplicities in their exponent vector, and tend to have a large automorphism group, that is a small orbit.

Furthermore, it is to be expected that such evaluations can be carried out much more efficiently by exploiting the inherent redundancy (*à la* Fast Fourrier Transform). In particular, one can use the strong generating set of G to apply a divide and conquer approach to the evaluation of an orbitsum on a point. The complexity analysis and benchmarking remains to be done to evaluate the practical gain. Finally, the evaluation of an orbitsum on many points is embarrassingly parallel (though fine grained), a property which we have not exploited yet.

5. Complexity analysis

For the sake of simplicity, all complexity results are expressed in terms of arithmetic operations in the ground field $\mathbb{K} = \mathbb{Q}(\rho)$. This model is realistic, because, in practice, the growth of coefficients does not seem to become a bottleneck; a possible explanation for this phenomenon might be that the natural coefficient growth

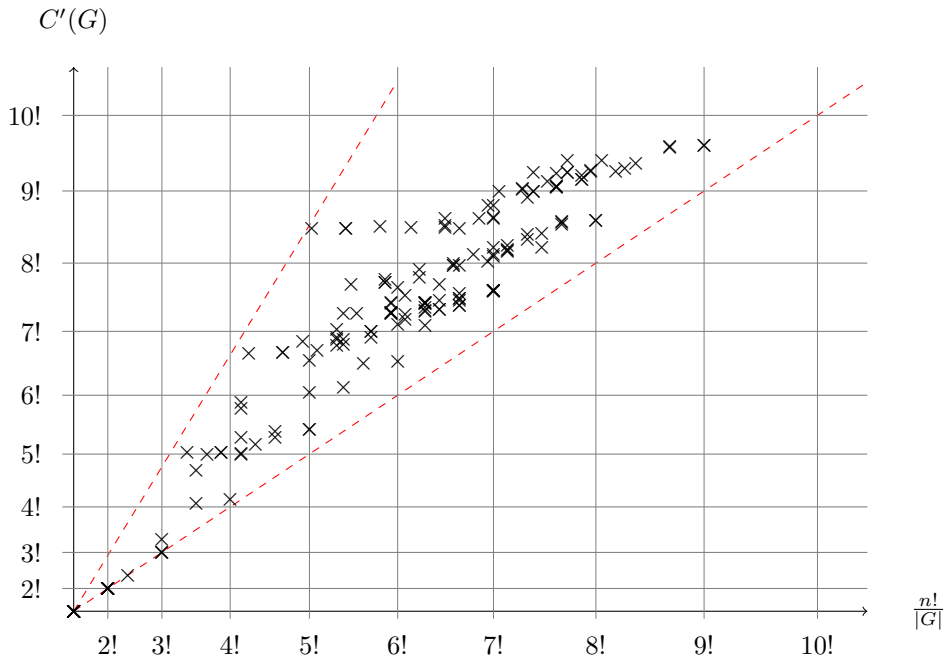

FIGURE 2. This figure plots, for $n \leq 10$ and for each transitive permutation group $G \subset \mathfrak{S}_n$, the number $C'(G) := C(G) - \text{catalan}(n) + 1$ of canonical integer vectors below the staircase for G which are *not* non zero partitions, versus the number $n!/|G|$ of secondary invariants. The dotted lines suggest that, in practice, $n!/|G| \leq C'(G) \leq (n!/|G|)^{2.5}$.

would be compensated by the pointwise product which tends to preserve and increase sparseness. We also consider that one operation in $\mathbb{K}$ is equivalent to n operations in $\mathbb{Q}$. This is a slight abuse; however $\dim_{\mathbb{Q}} \mathbb{Q}(\rho) = \phi(n) \geq 0.2n$ for $n \leq 10000$ which is far beyond any practical value of n in our context.

Theorem 5.1. *Let G be a permutation group, and take the elementary symmetric functions as primary invariants. Then, the complexity of computing secondary invariants by evaluation using Algorithm 1 is bounded above by $\mathcal{O}(n!^2 + n!^3/|G|^2)$ arithmetic operations in $\mathbb{K}$.*

Proof. To get this upper bound on the complexity, we broadly simplify the main steps of this algorithm to:

(1) Group theoretic computations on G: strong generating set, conjugacy classes, etc;
(2) Computation of the Hilbert series of $\mathbb{K}[\mathbf{x}]^G$;
(3) Construction of canonical monomials under the staircase;
(4) Computation by Φ of the evaluation vectors of the orbitsums of those monomials;
(5) Computation of products $\Phi(\eta)\Phi(\eta')$ of evaluation vectors of secondary invariants;

(6) Row reduction of the evaluation vectors.

The complexity of (1) is a small polynomial in n (see e.g. [Ser03]) and is negligible in practice as well as in theory. (2) can be reduced to the addition of c polynomials of degree at most $\binom{n}{2}$, where $c \leq |G| \leq n!$ is the number of conjugacy classes of G (the denominator of the Hilbert series is known; the mentioned polynomials contribute to its numerator, that is the generating series of the secondary invariants); it is negligible as well. Furthermore, by Remark 4.2 (3) is not a bottleneck.

Using Lemma 4.1 and Remark 4.4, the complexity of (4) is bounded above by $\mathcal{O}(n!^2)$ (at most $\mathcal{O}(n!)$ orbitsums to evaluate, for a cost of $\mathcal{O}(n!)$ each).

For a very crude upper bound for (5), we assume that the algorithm computes all products of evaluation vectors of two secondary invariants. This gives $(n!/G)^2$ products in $\mathcal{E}^G$ which is in $\mathcal{O}(n!/G)^3$.

Finally, in (6), the cost of the row reduction of $\mathcal{O}(n!)$ evaluation vectors in $\mathcal{E}^G$ is of $\mathcal{O}(n!^3/|G|^2)$. □

This complexity bound gives some indication that the symmetries are honestly taken care of by this algorithm. Consider indeed any algorithm computing secondary invariants by linear algebra in $\mathbb{K}[x]/\operatorname{Sym}(\mathbf{x})^+$ (say using Gröbner basis or orthogonal bases for the Schur-Schubert scalar product). Then the same estimation gives a complexity of $\mathcal{O}(n!^2/|G|)$ (reducing $n!$ candidates to get $n!/|G|$ linearly independent vectors in a vector space of dimension $n!$). Therefore, for G large enough, a gain of $|G|$ is obtained.

That being said, this is a *very* crude upper bound. For a fixed group G, one could use the Hilbert series to calculate explicitly a much better estimate: indeed the grading splits the linear algebra in many smaller problems and also greatly reduces the number of products to consider. However, it seems hard in general to get enough control on the Hilbert series, to derive complexity information solely in term of basic information on the group (n, $|G|$, ...). Also, in practice, there usually are only few irreducible invariants, and they are of small degrees. Thus only few of the canonical monomial need actually to be generated and evaluated.

It is therefore essential to complement this complexity analysis with extensive benchmarks to confirm the practical gains. This is the topic of the next section.

6. Implementation and benchmarks

Algorithm 1, and many variants, have been implemented in the open source mathematical platform `Sage` [S$^+$09]. The choice of the platform was motivated by the availability of most of the basic tools (group theory via `GAP` [GAP99], cyclotomic fields, linear algebra, symmetric functions, etc), and the existence of a community to share with the open-source development of the remaining tools (e.g. Schubert polynomials or the orderly generation of canonical monomials) [SCc08]. Thanks to the `Cython` compiler, it was also easy to write most of the code in a high level interpreted language (`Python`), and cherry pick just those critical sections that needed to be compiled (orderly generation, evaluation). The implementation is publicly available in alpha version via the `Sage-Combinat` patch server. It will eventually be integrated into the `Sage` library.

We ran systematic benchmarks (see Figure 6 and 6), comparing the results with the implementation of secondary invariants in `Singular` [GPS98, Kin07b]. Note that `Singular`'s implementation deals with any finite group of matrices. Also, it

precomputes and uses its own primary invariants instead of the elementary symmetric functions. Therefore, the comparison is not immediate: on the one hand, `Singular` has more work to do (finding the primary invariants); on the other hand, when the primary invariants are of small degree, the size of the result can be much smaller. Thus, those benchmarks should eventually be complemented by:

- Calculations of secondary invariants w.r.t. the elementary symmetric functions, using Gröbner basis using `Singular` and `Magma`;
- Calculations of secondary invariants using `Singular` and `Magma`;
- Calculations of secondary invariants w.r.t. the elementary symmetric functions, using SAGBI-Gröbner basis (for example by using `MuPAD-Combinat` [Thi, HT04]).

A similar benchmark comparing `Magma` [CP96] and `MuPAD-Combinat` is presented in [Thi01, Figure 1] (up to a bias: the focus in `MuPAD-Combinat` is on a minimal generating set, but this is somewhat equivalent to irreducible secondary invariants). This benchmark can be roughly compared with that of Figure 6 by shifting by a speed factor of 10 to compensate for the hardware improvements since 2001. Related benchmarks are available in [Kin07b, Kin07a].

We used the transitive permutation groups as test bed. A practical motivation is that there are not so many of them and they are easily available through the `GAP` database [Hul05]. At the same time, we claim that they provide a wide enough variety of permutation groups to be representative. In particular, the computation for non transitive permutation groups tend to be easier, since one can use primary invariants of much smaller degrees, namely the elementary symmetric functions in each orbit of variables.

The benchmarks were run on the computation server `sage.math.washington.edu`[1] which is equipped with 24 Intel(R) Xeon(R) CPU X7460 @2.66GHz cores and 128 GB of RAM. We did not use parallelism, except for running up to four tests in parallel. The memory usage is fairly predictable, at least for the `Sage` implementation, so we did not include it into the benchmarks. In practice, the worst calculation used 12 GB. Any calculation running over 24 hours was aborted.

7. Further developments

At this stage, the above sections validate the potential of the evaluation approach. Yet much remains to be done, both in theory and practice, to design algorithms making an optimal use of this approach. The main bottleneck so far is the calculation of evaluations by Φ, and we conclude with a couple problems we are currently investigating in this direction.

Problem 7.1. *Construct invariants with nice properties under evaluation by Φ (sparsity, ...). A promising starting point are Schubert polynomials* [LS82, Las03]*, as they form a basis of $\mathbb{K}[\mathbf{x}]$ as $\mathrm{Sym}(\mathbf{x})$-module whose image under Φ is triangular. However, it is not clear whether this triangularity can be made somehow compatible with the coset distribution of G in $\mathfrak{S}_n$.*

Another approach would be to search for invariants admitting short Straight Line Programs.

[1]This server is part of the `Sage` cluster at the University of Washington at Seattle and is devoted to `Sage` development; it was financed by "National Science Foundation Grant No. DMS-0821725".

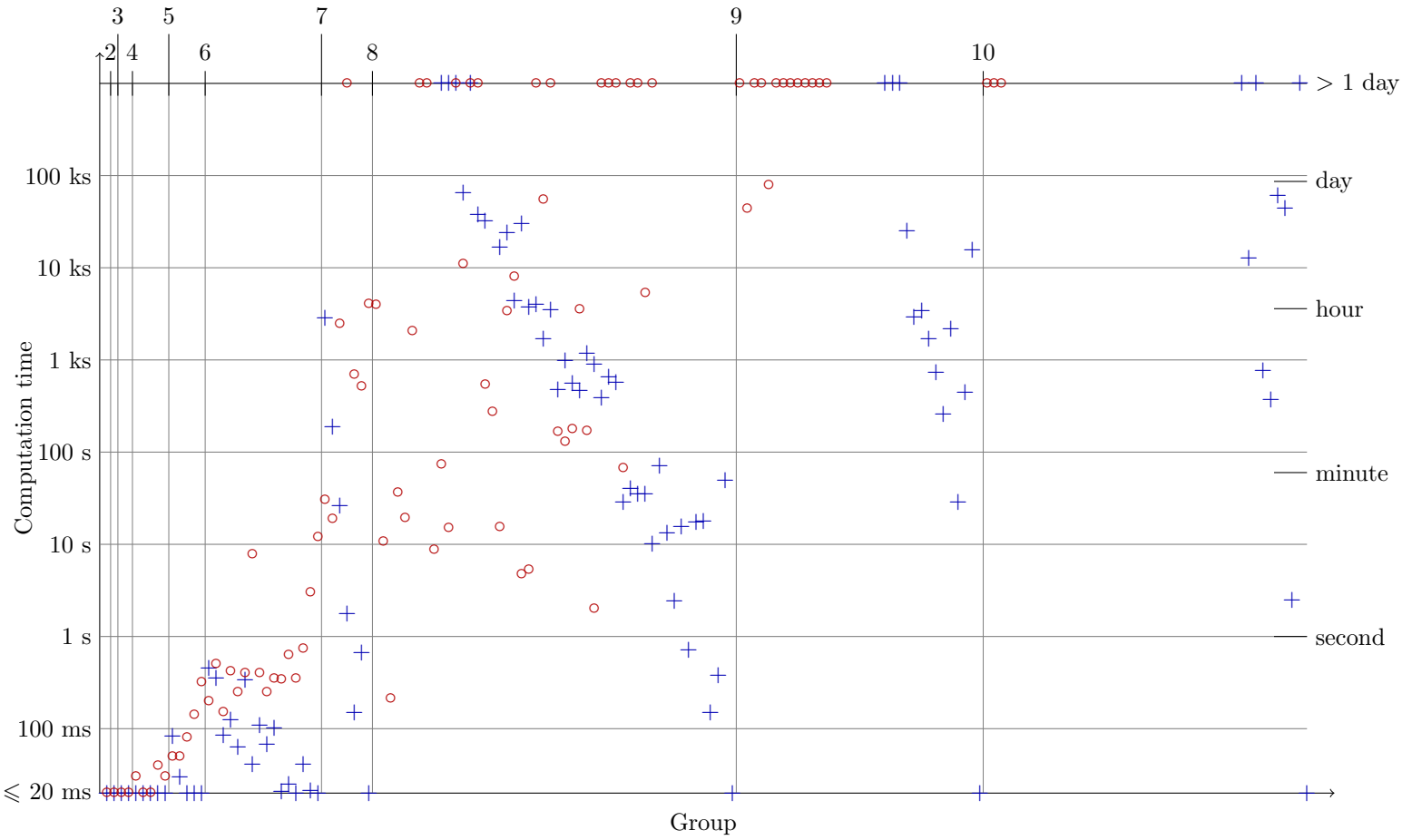

FIGURE 3. Comparative benchmark for the computation of secondary invariants for all transitive permutation groups for $n \leq 10$ using `Sage`'s evaluation implementation (+) and `Singular`'s elimination implementation (○). The groups are sorted horizontally by increasing n and then by increasing cardinality.

Note that a good solution to this problem, combined with the evaluation approach of this paper, could possibly open the door for the solution of a long standing problem, namely the *explicit* construction of secondary invariants; currently such a description is known only in the very simple case of products of symmetric groups [GS84]. Even just associating in some canonical way a secondary invariant to each coset in $\mathfrak{S}_n/G$ seems elusive.

From a practical point of view, the following would be needed.

Problem 7.2. *Find a good algorithm to compute Φ on the above invariants. This is similar in spirit to finding an analogue of the Fast Fourier Transform w.r.t. the Fourier Transform.*

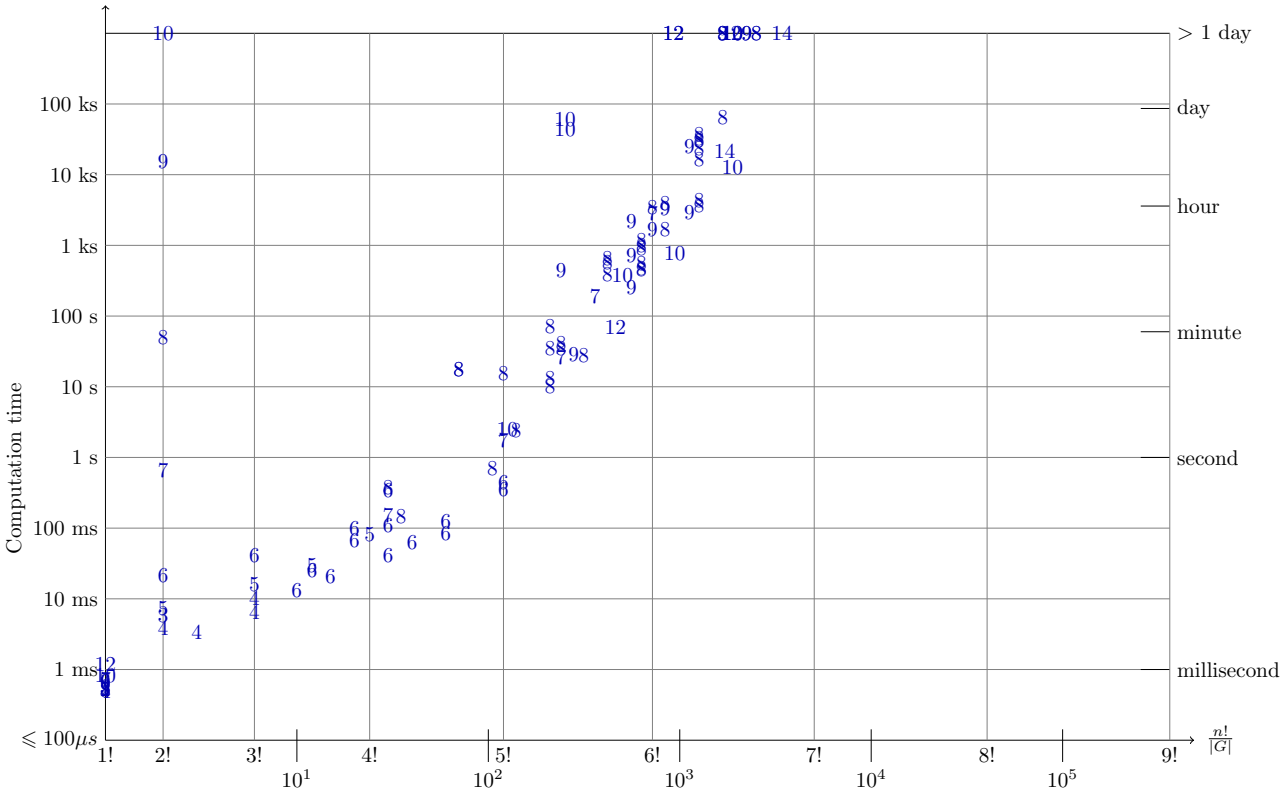

FIGURE 4. Benchmark for the computation of secondary invariants for all transitive permutation groups for $n \leq 10$ (and for some below $n \leq 14$), using `Sage`'s evaluation implementation. For each such group, n is written at position (k, t), where $k = n!/|G|$ is the number of secondary invariants and t is the computation time. In particular, the symmetric groups $\mathfrak{S}_n$ and the alternating groups $\mathfrak{A}_n$ are respectively above 1! and 2!.

Theorem 3.5 further suggests that, using the grading, it could be sufficient to consider only a subset of the evaluation points.This is corroborated by computer exploration; for example, for the cyclic group C_7 of order 7, 110 evaluation points out of 720 were enough for constructing the secondary invariants. Possible approaches include lazy evaluation strategies, or explicit choices of evaluation points, or some combination of both.

Problem 7.3. *Get some theoretical control on which evaluation points are needed so that Φ restricted on those points remains injective on some (resp. all) homogeneous component $\mathbb{K}[\mathbf{x}]_d^G$.*

Here again, Schubert polynomials are natural candidates, with the same difficulty as above. A step toward Problem 7.3 would be to solve the following.

Problem 7.4. *For $G \subset \mathfrak{S}_n$ a permutation group, and to start with for G the trivial permutation group, find a good description of the subspaces $\Phi(\mathbb{K}[\mathbf{x}]_d^G)$.*

Last but not least, one would want to generalize the evaluation approach to any matrix groups, following the line sketched in the introduction. The issue is whether one can get enough control on perturbations of the primary invariants so that:

- The orbits of the simple roots are large, in order to benefit from the gain of taking a single evaluation point per orbit;
- Only few of the primary invariants need to be perturbated, to best exploit the grading in the analogue of Theorem 3.5.

8. Acknowledgments

We would like to thank Marc Giusti, Alain Lascoux, Romain Lebreton, and Éric Schost, for fruitful discussions, as well as the anonymous referees of the extended abstract presented at MEGA 2011 [BT11] for their many useful suggestions for improvements.

This research was driven by computer exploration using the open-source mathematical software `Sage` [S$^+$09]. In particular, we perused its algebraic combinatorics features developed by the `Sage-Combinat` community [SCc08], as well as its group theoretical and invariant theoretical features provided respectively by `GAP` [GAP97] and `Singular` [GPS98]. The extensive benchmarks were run on the computational server `sage.math.washington.edu`, courtesy of the `Sage` developers group at the University of Washington (Seattle, USA) and the "National Science Foundation Grant No. DMS-0821725".

References

[Abd00] Ines Abdeljaouad. *Théorie des Invariants et Applications à la Théorie de Galois effective*. PhD thesis, Université Paris 6, 2000.

[BT11] Nicolas Borie and Nicolas M. Thiéry. An evaluation approach to computing invariants rings of permutation groups. In *Proceedings of MEGA 2011*, March 2011. Accepted, 8 pages.

[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.

[Col97a] Antoine Colin. Solving a system of algebraic equations with symmetries. *J. Pure Appl. Algebra*, 117/118:195–215, 1997. Algorithms for algebra (Eindhoven, 1996).

[Col97b] Antoine Colin. *Théorie des invariants effective; Applications à la théorie de Galois et à la résolution de systèmes algébriques; Implantation en AXIOM*. PhD thesis, École polytechnique, 1997.

[CP96] John Cannon and Catherine Playoust. MAGMA: a new computer algebra system. *Euromath Bull.*, 2(1):113–144, 1996.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[DSW09] Xavier Dahan, Éric Schost, and Jie Wu. Evaluation properties of invariant polynomials. *J. Symbolic Comput.*, 44(11):1592–1604, 2009.

[FR09] J.C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 151–158. ACM, 2009.

[GAP97] The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland. *GAP – Groups, Algorithms, and Programming, Version 4*, 1997.

[GAP99] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999.

[Gat90] K. Gatermann. *Symbolic solution of polynomial equation systems with symmetry*. Konrad-Zuse-Zentrum für Informationstechnik Berlin, 1990.

[GK00] Katharina Geissler and Jürgen Klüners. Galois group computation for rational polynomials. *J. Symbolic Comput.*, 30(6):653–674, 2000. Algorithmic methods in Galois theory.

[GPS98] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular version 1.2 User Manual . In *Reports On Computer Algebra*, number 21. Centre for Computer Algebra, University of Kaiserslautern, June 1998.

[GS84] A. M. Garsia and D. Stanton. Group actions of Stanley - Reisner rings and invariants of permutation groups. *Adv. in Math.*, 51(2):107–201, 1984.

[GST06] Pierrick Gaudry, Éric Schost, and Nicolas M. Thiéry. Evaluation properties of symmetric polynomials. *Internat. J. Algebra Comput.*, 16(3):505–523, 2006. http://hal.inria.fr/inria-00000629.

[HT04] Florent Hivert and Nicolas M. Thiéry. MuPAD-Combinat, an open-source package for research in algebraic combinatorics. *Sém. Lothar. Combin.*, 51:Art. B51z, 70 pp. (electronic), 2004. `http://mupad-combinat.sf.net/`.

[Hul05] Alexander Hulpke. Constructing transitive permutation groups. *J. Symbolic Comput.*, 39(1):1–30, 2005.

[Kem93] Gregor Kemper. The *invar* package for calculating rings of invariants. IWR Preprint 93-94, University of Heidelberg, 1993.

[Kem98] Gregor Kemper. Computational invariant theory. In *The Curves Seminar at Queen's. Vol. XII (Kingston, ON, 1998)*, pages 5–26. Queen's Univ., Kingston, ON, 1998.

[Kin07a] S. King. Minimal generating sets of non-modular invariant rings of finite groups. *Arxiv preprint math/0703035*, 2007.

[Kin07b] S.A. King. Fast Computation of Secondary Invariants. *Arxiv preprint math/0701270*, 2007.

[Las03] Alain Lascoux. *Symmetric functions and combinatorial operators on polynomials*, volume 99 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2003.

[LS82] Alain Lascoux and Marcel-Paul Schützenberger. Polynômes de Schubert. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(13):447–450, 1982.

[MB82] H. M. Möller and B. Buchberger. The construction of multivariate polynomials with preassigned zeros. In *Computer algebra (Marseille, 1982)*, volume 144 of *Lecture Notes in Comput. Sci.*, pages 24–31. Springer, Berlin, 1982.

[McK98] Brendan D. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26(2):306–324, 1998.

[Nic11] Nicolas.Borie. *Calcul des invariants des groupes de permutations par transformée de Fourier*. PhD thesis, Laboratoire de Mathématiques, Université Paris Sud, 2011.

[PT01] Maurice Pouzet and Nicolas M. Thiéry. Invariants algébriques de graphes et reconstruction. *C. R. Acad. Sci. Paris Sér. I Math.*, 333(9):821–826, 2001. arXiv:0812.3079v1 [math.CO].

[Rea78] Ronald C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Math.*, 2:107–120, 1978. Algorithmic aspects of combinatorics (Conf., Vancouver Island, B.C., 1976).

[S+09] W. A. Stein et al. *Sage Mathematics Software (Version 3.3)*. The Sage Development Team, 2009. `http://www.sagemath.org`.

[SCc08] The Sage-Combinat community. Sage-Combinat: enhancing Sage as a toolbox for computer exploration in algebraic combinatorics, 2008. `http://combinat.sagemath.org`.

[Ser03] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[Smi97] Larry Smith. Polynomial invariants of finite groups. A survey of recent developments. *Bull. Amer. Math. Soc. (N.S.)*, 34(3):211–250, 1997.

[Sta79] Richard P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (N.S.)*, 1(3):475–511, 1979.

[Stu93] Bernd Sturmfels. *Algorithms in invariant theory*. Springer-Verlag, Vienna, 1993.

[Thi] Nicolas M. Thiéry. `PerMuVAR`, a library for `MuPAD` for computing in invariant rings of permutation groups. `http://permuvar.sf.net/`.

[Thi00] Nicolas M. Thiéry. Algebraic invariants of graphs: a study based on computer exploration. *SIGSAM Bulletin (ACM Special Interest Group on Symbolic and Algebraic Manipulation)*, 34(3):9–20, September 2000. arXiv:0812.3082v1 [math.CO].

[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., Paris, 2001.

[TT04] Nicolas M. Thiéry and Stéphan Thomassé. Convex cones and SAGBI bases of permutation invariants. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 259–263. Amer. Math. Soc., Providence, RI, 2004. arXiv:0607380 [math.AC].

Univ. Paris-Sud, Laboratoire de Mathématiques d'Orsay, Orsay Cedex, F-91405; CNRS, France