CLASSICAL COVARIANTS AND MODULAR INVARIANTS

R. JAMES SHANK

There is a relationship between the covariants of binary forms, a central topic in classical invariant theory, and the invariants of modular representations of cyclic groups of prime order. This relationship was identified by Gert Almkvist [1] and used implicitly in both [15] and [17]. In this note we investigate the relationship and provide a progress report on an application. Our primary motivation is a desire to construct nice generating sets for the rings of invariants of modular representations of cyclic groups of prime order.

1. Modular Invariants

Let p denote a prime number, let $\mathbf{Z}/p$ denote the cyclic group of order p, and let $\mathbf{F}$ denote a field of characteristic p. A representation of a cyclic group is determined by the Jordan canonical form of (the image of) the generator. If $n \leq p$ then the $n \times n$ matrix over $\mathbf{F}$ consisting of a single Jordan block with eigenvalue 1, has order p and determines an indecomposable representation of $\mathbf{Z}/p$ which we denote by V_n (For $n > p$, the order of the matrix is greater than p.). Note that there are no non-trivial p^{th} roots of unity in $\mathbf{F}$. Thus 1 is the only eigenvalue for the image of a generator of $\mathbf{Z}/p$ under a representation over $\mathbf{F}$. Therefore, up to isomorphism, the only indecomposable $\mathbf{F}\mathbf{Z}/p$-modules are $V_1, V_2, \ldots, V_p$.

Let V be any finite dimensional vector space over an arbitrary field $\mathbf{k}$. We choose a basis, $\{x_1, \ldots, x_n\}$, for the dual, V^*, of V and consider a subgroup G of $GL(V)$. The action of G on V induces an action on V^* which extends to an action by algebra automorphisms on the symmetric algebra of V^*, $\mathbf{k}[V] := \mathbf{k}[x_1, \ldots, x_n]$. The ring of invariants of G is the subring of $\mathbf{k}[V]$ given by

$$\mathbf{k}[V]^G := \{f \in \mathbf{k}[V] \mid g \cdot f = f \text{ for all } g \in G\}.$$

If G is a finite group and $|G|$ is not invertible in $\mathbf{k}$ then we say the representation of G on V is *modular*. If $|G|$ is invertible in $\mathbf{k}$ then V is called a *non-modular* representation. We will be primarily interested in the case $G = \mathbf{Z}/p$. Note that V_n^* and V_n are isomorphic $\mathbf{Z}/p$-modules and we will usually choose the basis for V_n^* so that the generator of $\mathbf{Z}/p$ is in Jordan canonical form.

Date: October 2, 2002.

1991 *Mathematics Subject Classification.* 13A50.

For a finite G, the *transfer* is defined by:

$$\begin{array}{rccc} Tr^G: & \mathbf{k}[V] & \longrightarrow & \mathbf{k}[V]^G \\ & f & \longmapsto & \displaystyle\sum_{g\in G} g\cdot f \end{array}$$

and is a homomorphism of $\mathbf{k}[V]^G$-modules. For non-modular representations, Tr^G is surjective. For modular representations, the image of the transfer, I^G, is a proper non-zero ideal of $\mathbf{k}[V]^G$. For proofs of this fact and other general properties of the modular transfer see [16]. For $f \in \mathbf{k}[V]$, we define the *norm* of f to be the product over the orbit of f, $N(f) := \prod_{h\in G\cdot f} h$.

The central problem of invariant theory is to find (nice) generators for the algebra $\mathbf{k}[V]^G$. In practice, this problem is much harder in the modular setting. Even for representations of $\mathbf{Z}/p$, finding manageable generating sets for the ring of invariants can be difficult. Hughes & Kemper [10] have given an upper bound on the degrees of the generators for any representation of $\mathbf{Z}/p$. Therefore by taking all homogeneous invariants with degree less than or equal to the upper bound we do get a finite generating set. However such generating sets are far from manageable. Minimal generating sets for $\mathbf{F}[V_2]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_3]^{\mathbf{Z}/p}$ can be found in Dickson's Madison Colloquium [5]. Finite SAGBI bases[1] (see Section 4 for definitions) for $\mathbf{F}[V_4]^{\mathbf{Z}/p}$ and $\mathbf{F}[V_5]^{\mathbf{Z}/p}$ can be found in [15]. The problem of finding a nice generating set for $\mathbf{F}[V_n]^{\mathbf{Z}/p}$ for $n > 5$ remains open. The results of Section 6 represent preliminary work for $n = 6$. Even when the invariants of the indecomposable summands are understood, it can be difficult to construct generating sets for decomposable representations. Campbell & Hughes, in [3], describe a generating set for $\mathbf{F}[mV_2]^{\mathbf{Z}/p}$ which is refined to a minimal generating set in [18]. A SAGBI basis is given for $\mathbf{F}[V_2 \oplus V_3]^{\mathbf{Z}/p}$ in [17]. I understand that Brandon Fodden, a student at Queen's University (Canada), has constructed a SAGBI basis for $\mathbf{F}[2V_3]^{\mathbf{Z}/p}$. Example 5.4 is related to this problem and Example 5.5 is related to $\mathbf{F}[V_3 \oplus V_4]^{\mathbf{Z}/p}$

2. Covariants of Binary Forms

Consider the contragradiant action of $SL_2(\mathbf{C})$ on the span of x and y, and extend this to an action by algebra automorphisms on $\mathbf{C}[x, y]$. There is a linear action of $SL_2(\mathbf{C})$ on the span of $\{a_0, a_1, \ldots, a_m\}$ with respect to which the binary form

$$f := \sum_{i=0}^{m} \binom{m}{i} a_i\, x^{m-i} y^i$$

is invariant. Extend the given actions of $SL_2(\mathbf{C})$ to actions by algebra automorphisms on $\mathbf{C}[a_0, \ldots, a_m]$ and $\mathbf{C}[x, y, a_0, \ldots, a_m]$. An element of $\mathbf{C}[a_0, \ldots, a_m]^{SL_2(\mathbf{C})}$ is called an *invariant* of the binary form while an element of $\mathbf{C}[x, y, a_0, \ldots, a_m]^{SL_2(\mathbf{C})}$ is called a *covariant* of the binary from. Following classical terminology, for

[1] A SAGBI basis is a particularly nice generating set.

$h \in \mathbf{C}[x, y, a_0, \ldots, a_m]$, the *degree* of h is its degree as a polynomial in the a_i's while the *order* of h is its degree as a polynomial in x and y. Thus, for example, f has degree 1 and order m. The action of $SL_2(\mathbf{C})$ on $\mathbf{C}[x, y, a_0, \ldots, a_m]$ preserves both degree and order. Since an arbitrary covariant is the sum of its homogeneous components, we need only consider elements of $\mathbf{C}[x, y, a_0, \ldots, a_m]^{SL_2(\mathbf{C})}$ which are homogeneous with respect to both degree and order. The *weight* of a monomial $a_0^{e_0} a_1^{e_1} \cdots a_m^{e_m} \in \mathbf{C}[a_0, \ldots, a_m]$ is defined to be $e_1 + 2e_2 + \cdots + me_m$. The *source* of a homogeneous covariant of order k is the coefficient of x^k and is a homogeneous element of $\mathbf{C}[a_0, \ldots, a_m]$. The covariant can be recovered from its source [9, pp. 41–43]. Furthermore, any homogeneous isobaric element of $\mathbf{C}[a_0, \ldots, a_m]$ which is invariant under the upper-triangular unipotent subgroup (a seminvariant), is the source of a homogeneous covariant([13, Theorem 9.45]). If the source has degree d, and weight ω, then the resulting covariant has order $k = m \cdot d - 2\omega$ ([9, pp. 41–43], [8, § 31]). Define

$$\sigma := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The action of σ on $\mathbf{C}[a_0, \ldots, a_m]$ is given by $\sigma(a_i) = \sum_{j=0}^{i} \binom{i}{j} a_j$ and the seminvariants are precisely the elements of $\mathbf{C}[a_0, \ldots, a_m]^\sigma$. Take $m = n - 1$ and choose a basis, $\{x_1, \ldots, x_n\}$, for the span of $\{a_0, \ldots, a_{n-1}\}$ so that σ is in Jordan canonical form, i.e., $\sigma(x_1) = x_1$ and $\sigma(x_i) = x_i + x_{i-1}$ for $1 < i \leq n$. For $n \leq 6$, a suitable change of basis is given by $a_0 = x_1$, $a_1 = x_2$, $a_2 = 2x_3 + x_2$, $a_3 = 6x_4 + 6x_3 + x_2$, $a_4 = 24x_5 + 36x_4 + 14x_3 + x_2$, $a_5 = 120x_6 + 240x_5 + 150x_4 + 30x_3 + x_2$.

3. The Connection: Integral Invariants

Define an algebra automorphism, σ, on $\mathbf{Z}[x_1, \ldots, x_n]$ by $\sigma(x_1) = x_1$ and $\sigma(x_i) = x_i + x_{i-1}$ for $1 < i \leq n$. Reducing coefficients modulo p gives a surjection from $\mathbf{Z}[x_1, \ldots, x_n]$ to $\mathbf{F}_p[x_1, \ldots, x_n]$ which induces a ring homomorphism from $\mathbf{Z}[x_1, \ldots, x_n]^\sigma = \mathbf{Z}[x_1, \ldots, x_n]^{\mathbf{Z}}$ to $\mathbf{F}_p[x_1, \ldots, x_n]^\sigma = \mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$. We will refer to elements in the image of this homomorphism as *rational* invariants.

The inclusion of $\mathbf{Z}$ into $\mathbf{C}$ induces a ring monomorphism from $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$ to $\mathbf{C}[x_1, \ldots, x_n]^\sigma = \mathbf{C}[x_1, \ldots, x_n]^{\mathbf{Z}}$, the ring of seminvariants.

Theorem 3.1. *The image of $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$ in $\mathbf{C}[x_1, \ldots, x_n]^{\mathbf{Z}}$ is a generating set and the image of $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$ in $\mathbf{F}_p[x_1, \ldots, x_n]^{\mathbf{Z}/p}$ is surjective in low degrees.*

Proof. This is essentially [1, Theorem 2.5]. The proof relies on comparing Hilbert series. □

We are primarily interested in using this result to construct elements of $\mathbf{F}_p[V_n]^{\mathbf{Z}/p}$ from covariants of the binary $(n-1)$-form. If we start with a homogeneous covariant, we may easily identify the source. The source is an element of $\mathbf{C}[x_1, \ldots, x_n]^\sigma$.

If the source lies in $\mathbf{Q}[x_1, \ldots, x_n]^\sigma$, we may clear the denominators to get an element of $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$ which then projects to an element of $\mathbf{F}_p[V_n]^{\mathbf{Z}/p}$. It is a consequence of the above theorem that we may choose the generators of $\mathbf{C}[x_1, \ldots, x_n]^\sigma$ to lie in $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$. The results of Section 5 below will give us a process for explicitly constructing generating sets for $\mathbf{C}[x_1, \ldots, x_n]^\sigma$ which lie in $\mathbf{Z}[x_1, \ldots, x_n]^\sigma$. However, such a generating set will not necessarily project to a generating set for the subring of rational invariants. There are a number of serious questions about the coefficients that have yet to be addressed. Despite this, the process has been used successfully in a number of cases.

In [15, § 6], I conjectured that, for an indecomposable representation V, the ring $\mathbf{F}_p[V]^{\mathbf{Z}}$ is generated by rational invariants, the image of the transfer and the norm of the generator of the $\mathbf{Z}/p$-module V^*. I believe that this should hold for decomposable representations as well, as long as the norms of a generating set for the $\mathbf{Z}/p$-module V^* are included. Note that for representations of $\mathbf{Z}/p^i$, elements in the image of the relative transfer would need to be added. Also, in this case, the concept of rational invariant, which is essentially a large prime approximation, is less useful.

Since the degrees of a generating set for the rational invariants are independent of the prime, the conjecture implies that for all but a finite (possibly empty) set of primes, an upper bound on the degrees of a minimal generating set is given by an upper bound on the degrees of the generators for the image of the transfer. The same conclusion is reached in [10, § 2.4] using the 'periodicity' of $\mathbf{F}_p[V]$.

4. SAGBI bases

A SAGBI basis for a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$ is a **S**ubalgebra **A**nalog to a **G**öbner **B**asis for **I**deals and as such is a particularly nice generating set. SAGBI bases were introduced independently by Robbiano & Sweedler [14] and Kapur & Madlener [11]. Unfortunately, even a finitely generated subalgebra does not necessarily have a finite SAGBI basis. In fact, as demonstrated by the ring of invariants of the canonical representation of the alternating group on three letters, even the ring of invariants of a finite group may fail to have a SAGBI basis (see [6, Lemma 2.1], [7] or [20, Example 11.2]).

We use the convention that a monomial is a product of variables and that a term is a monomial with a non-zero coefficient. See [4, Chapter 2] for a detailed discussion of monomial orders. For $f \in \mathbf{k}[x_1, \ldots, x_n]$, we use $\mathrm{LT}(f)$ to denote the lead term of f and $\mathrm{LM}(f)$ to denote the lead monomial of f. Suppose that R is a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$. Let $\mathrm{LT}(R)$ denote the vector space spanned by the lead terms of elements of R. Then $\mathrm{LT}(R)$ is a subalgebra of $\mathbf{k}[x_1, \ldots, x_n]$. If C is a subset of R then let $\mathrm{LM}(C)$ denote the set of lead monomials of elements of C. If C is a subset of R such that $\mathrm{LM}(C)$ generates the algebra $\mathrm{LT}(R)$ then C generates R and C is called a *SAGBI basis* for R. Note that $\mathrm{LT}(R)$ is a graded

algebra. If the subalgebra generated by $\mathrm{LM}(C)$ coincides with $\mathrm{LT}(R)$ in degrees less than or equal to d, we say that C is a SAGBI basis through degree d. For a detailed discussion of SAGBI bases see [14], [11] or [20, Chapter 11].

Taking $C = R$ gives a SAGBI basis for R. Thus every subalgebra has a SAGBI basis. However, if $\mathrm{LT}(R)$ is not finitely generated then R does not have a finite SAGBI basis (at least using the given monomial order). Although the characterization of subalgebras which admit a finite SAGBI basis remains an important open problem, there are some circumstances which guarantee the existence of a finite SAGBI basis.

Theorem 4.1. ([18, Lemma 3.1]) *Suppose $\{h_1, \ldots, h_n\}$ is a homogeneous system of parameters for $\mathbf{k}[x_1, \ldots, x_n]$ with $\mathrm{LM}(h_i) = x_i^{d_i}$. If $A \subseteq \mathbf{k}[x_1, \ldots, x_n]$ is a subalgebra with $\{h_1, \ldots, h_n\} \subseteq A$, then A has a finite SAGBI basis.*

Suppose that V is a modular representation of $\mathbf{Z}/p$. Choose our basis for V^* so that the generator, say σ, is in Jordan canonical form, i.e., σ is represented by an upper-triangular unipotent matrix. Choose a monomial order with $x_1 < x_2 < \cdots < x_n$. Then $\mathrm{LM}(N(x_i)) = x_i^{[G:G_{x_i}]}$, where G_{x_i} is the isotropy subgroup of x_i, and $\{N(x_1), N(x_2), \ldots, N(x_n)\}$ is a homogeneous system of parameters for $\mathbf{F}[V]$. Therefore, using this basis and order, $\mathbf{F}[V]^{\mathbf{Z}/p}$ has a finite SAGBI basis (see [18, Theorem 3.3, Corollary 3.4]).

Suppose that $C \subseteq \mathbf{k}[V]$. A *tête-a-tête* (over C) is the analogue of an S-polynomial and consists of two factorisations of a monomial over $\mathrm{LM}(C)$. We will refer to a tête-a-tête as *trivial* if the two factorisations have a common factor greater than 1. A tête-a-tête is given by two subsets $\Lambda_1, \Lambda_2 \subseteq C$ and positive integers e_s for $s \in \Lambda_1$ and d_h for $h \in \Lambda_2$ such that

$$\prod_{s \in \Lambda_1} \mathrm{LM}(s^{e_s}) = \prod_{h \in \Lambda_2} \mathrm{LM}(h^{d_h}).$$

It is then possible to choose $c_1, c_2 \in \mathbf{k}$ so that

$$c_1 \prod_{s \in \Lambda_1} \mathrm{LT}(s^{e_s}) = c_2 \prod_{h \in \Lambda_2} \mathrm{LT}(h^{d_h}).$$

The difference

$$c_1 \prod_{s \in \Lambda_1} s^{e_s} - \; c_2 \prod_{h \in \Lambda_2} h^{d_h}$$

is either zero or has a smaller lead monomial. Despite the ambiguity, we will sometimes refer to this difference as the tête-a-tête.

Subduction is the analogue of reduction. For a homogeneous $f \in \mathbf{k}[V]$ of positive degree, if $\mathrm{LM}(f)$ has a factorisation over $\mathrm{LM}(C)$ then, there exits a finite subset $\Lambda \subseteq C$, a coefficient $c \in \mathbf{k}$ and positive integers e_h for $h \in \Lambda$ such that

$$\mathrm{LT}(f) = c \prod_{h \in \Lambda} \mathrm{LT}(h)^{e_h}.$$

The difference,

$$f - c\prod_{h\in\Lambda} h^{e_h},$$

is called a primary subduction of f and is either zero or has a lead monomial less than $\mathrm{LM}(f)$. A full subduction of f consists of iterating this process as long as the lead monomial has a factorisation over $\mathrm{LM}(C)$. If C is a SAGBI basis for the subalgebra, then subduction provides a test for subalgebra membership: f is an element of the subalgebra if and only if f subducts to zero [14, 16.6]. Subduction also provides a SAGBI basis test: C is a SAGBI basis for the subalgebra generated by C if and only if every non-trivial tête-a-tête subducts to zero [14, 2.6] (Note that we work exclusively with homogeneous polynomials.).

For a finite subset $C \subseteq \mathbf{k}[V]$, define $d := |C|$ and $A_C := \mathbf{k}[t_1, \ldots, t_d]$. Further define $\phi : A_C \to \mathbf{k}[V]$ by $\phi(t_h) = \mathrm{LT}(h)$ and $\Phi : A_C \to \mathbf{k}[V]$ by $\Phi(t_h) = h$. The kernel of ϕ, I_C, is a toric ideal whose binomial[2] generators correspond to tête-a-têtes over C. Let $\mathcal{T}_C$ be a finite generating set for I_C consisting of binomials.

Theorem 4.2. *C is a SAGBI basis for the subalgebra generated by C if and only every element of $\Phi(\mathcal{T}_C)$ subducts to zero.*

Proof. This is essentially [20, Corollary 11.5]. The elements of $\mathcal{T}_C$ correspond to a set of generating tête-a-têtes. □

Algorithm 4.3.

Given a finite set C of homogeneous polynomials of positive degree in $\mathbf{k}[V]$, and a positive integer d, return a SAGBI basis through degree d for the subalgebra generated by C.

(1) Define $m := \min\{\mathrm{degree}(h) \mid h \in C\}$. Set G to be the set of elements of C of degree m and set $i := m + 1$.
(2) Compute a Gröbner basis of binomials through degree i for the kernel of $\phi : A_G \to \mathbf{k}[V]$. Call this basis B.
(3) Subduct each element of $\Phi(B)$ against the set C and adjoin non-zero full subductions to C.
(4) If $i + 1 = d$, return $G \cup C$. Otherwise set $i := i + 1$.
(5) Adjoin elements of degree i from C to G and go to Step 2.

Remark 4.4. *The Magma* [2] *command "Groebner(S,d)" was introduced with version 2.7 and allows the computation of a partial Gröbner basis through degree d. David Wehlau and I have written a Magma script implementing subduction. Thus the above algorithm has essentially been implemented in Magma. We note that the algorithm, as described here, does not produce a minimal SAGBI basis.*

[2]Our convention is that a binomial is a linear combination of two distinct monomials.

5. Transvectants

The transvection process can be used to produce new covariants from old. Define algebra homomorphisms $\rho : \mathbf{C}[x, y, a_0, \ldots, a_m] \to \mathbf{C}[X, Y, x, y, a_0, \ldots, a_m]$ and $\pi : \mathbf{C}[X, Y, x, y, a_0, \ldots, a_m] \to \mathbf{C}[x, y, a_0, \ldots, a_m]$ by $\rho(a_i) = a_i$, $\rho(x) = X$, $\rho(y) = Y$, $\pi(a_i) = a_i$, $\pi(X) = x$, $\pi(Y) = y$, $\pi(x) = x$ and $\pi(y) = y$. The transvectant of two covariants is defined using Cayley's Ω-operator,

$$\Omega := \frac{\partial^2}{\partial x \partial Y} - \frac{\partial^2}{\partial y \partial X}.$$

The r^{th} transvectant of h and g is $(h, g)^r := \pi(\Omega^r(h \cdot \rho(g)))$ (see [21], [8, § 48], [13, Ch. 5] and [19, § 4.3]). Note that if h is homogeneous of degree d_1 and order k_1, and g is homogeneous of degree d_2 and order k_2, then $(h, g)^r$ is homogeneous of degree $d_1 + d_2$ and order $k_1 + k_2 - 2r$. Also note that to combat coefficient bloat, Grace & Young scale the transvectant by a coefficient which depends on the degree and order of h and g.

The transvectant of two covariants is again a covariant and a generating set for the ring of covariants can be constructed by starting with the binary form and iteratively constructing transvectants. This is a key element in Gordan's proof that the ring of covariants is finitely generated [8, Chapter VI].

Example 5.1. The Cubic. A fundamental set of covariants is given by the form f, the Hessian $H := (f, f)^2$, $t := (f, H)^1$ and $\Delta := (f, t)^3$ (see [8, § 88], [9, p. 68], [19, Proposition 3.7.7],[13, p. 39] and [12, § 6.4]). The source of f gives x_1. The source of H gives an invariant with lead monomial x_2^2. The source of t gives an invariant with lead monomial x_2^3. The source of Δ gives an invariant with lead monomial $x_2^2 x_3^2$. Comparing with [15, § 4], we see that we have a SAGBI basis for the ring of rational invariants.

Example 5.2. The Quartic. A fundamental set of covariants is given by f, $H = (f, f)^2$, $i := (f, f)^4$, $t = (f, H)^1$, and $j := (f, H)^4$ [8, § 89]. The lead monomials of the corresponding rational invariants are x_1, x_2^2, x_3^2, x_2^3 and x_3^3. Subducting the tête-a-tête formed from the third and fifth invariants gives an invariant with lead monomial $x_4^2 x_3^2 x_2^2$. Comparing with [15, § 5], we see that we have a SAGBI basis for the ring of rational invariants.

The next three examples involve simultaneous covariants of a system of binary forms. Although Sections 2 and 3 dealt only with covariants of a single form, there are natural generalisations to a system of forms. Furthermore, a generating set for the ring of simultaneous covariants for a finite set of binary forms can be constructed by starting with the binary forms and iteratively constructing transvectants [8, Chapter VIII].

Example 5.3. A linear form ℓ and a quadratic form f. A fundamental set of covariants is given by ℓ, f, the discriminant $\Delta := (f, f)^2$, $(f, \ell)^1$, and $(f, \ell^2)^2$

[8, § 138 A] [3]. If we use $\{x_1, y_1, x_2, y_2, z_2\}$ as our basis for $V_2^* \oplus V_3^*$, the lead monomials of the corresponding rational invariants are x_1, x_2, y_2^2, x_2y_1 and $x_2y_1^2$. Comparing with [17, § 5], we see that we have a SAGBI basis for the ring of rational invariants.

Example 5.4. Two quadratics: f_1 and f_2. A fundamental set of covariants is given by f_1, f_2, $(f_1, f_1)^2$, $(f_2, f_2)^2$, $(f_1, f_2)^1$ and $(f_1, f_2)^2$ [8, § 139]. If we use $\{x_1, y_1, z_1, x_2, y_2, z_2\}$ as our basis for $V_3^* \oplus V_3^*$, the lead monomials of the corresponding rational invariants are x_1, x_2, y_1^2, y_2^2, x_2y_1 and x_2z_1. The only non-trivial tête-a-tête is formed from the second, third and fifth generators. This subducts to 0. Therefore we have a SAGBI basis for the rational invariants. This is consistent with unpublished work of Brandon Fodden on $\mathbf{F}_p[2V_3]^{\mathbf{Z}/p}$.

Example 5.5. A quadratic ϕ and a cubic f. A fundamental set of covariants is given in [8, § 140]. We use $\{x_1, y_1, z_1, x_2, y_2, z_2, w_2\}$ as our basis for $V_3^* \oplus V_4^*$. Below we describe the fundamental covariants along with the lead monomials of the corresponding rational invariants. The covariant $c_{i,j}$ has degree i and order j. The fundamental covariants:
$\phi,\ x_1; \quad f,\ x_2; \quad D := c_{2,0} := (\phi, \phi)^2,\ y_1^2; \quad H := c_{2,2} := (f, f)^2,\ y_2^2;$
$T := c_{3,3} := (f, H)^1,\ y_2^3; \quad \Delta := c_{4,0} := (H, H)^2,\ z_2^2y_2^2;$
$c_{2,3} := (\phi, f)^1,\ x_2y_1; \quad c_{2,1} := (\phi, f)^2,\ x_2z_1;$
$c_{3,2} := (\phi, H)^1,\ y_2^2y_1; \quad c_{3,1} := (\phi^2, f)^3,\ x_2z_1y_1; \quad c_{3,0} := (\phi, H)^2,\ y_2^2z_1;$
$c_{4,1} := (\phi, T)^2,\ y_2^3z_1; \quad c_{5,1} := (\phi^2, T)^3,\ y_2^3z_1y_1; \quad c_{5,0} := (\phi^3, f^2)^6,\ x_2^2z_1^3;$
$c_{7,0} := (\phi^3, fT)^6,\ y_2^3x_2z_1^3.$
For a covariant c, let $\mathrm{inv}(c)$ denote a corresponding rational invariant. The tête-a-tête given by $(\mathrm{inv}(c_{2,1})\,\mathrm{inv}(H), \mathrm{inv}(f)\,\mathrm{inv}(c_{3,0}))$ subducts to an invariant with lead monomial $y_2^3y_1$. A Magma [2] calculation based on Theorem 4.2 verifies that we now have a SAGBI basis for the $\mathbf{Q}[x_1, y_1, z_1, x_2, y_2, z_2, w_2]^{\mathbf{Z}}$.

6. The Binary Quintic

A fundamental set of covariants for the binary quintic can be found either in [8, Ch. VII] or [21]. The descriptions are slightly different but yield the same lead monomials for the corresponding rational invariants. Grace & Young describe each covariant as a transvectant in terms of f, i, H and t while Sylvester uses various lower degree covariants in his description. There is a certain elegance to the Grace & Young description but Sylvester's description is more computationally efficient – a Magma [2] construction using the Grace & Young description takes four times longer than one based on Sylvester's construction. Below we give Sylvester's description of the fundamental covariants along with the lead monomial of the corresponding rational invariant. The covariant $c_{i,j}$ has degree i and order j. Sylvester's covariants:

[3] Beware the typographical error in the last line of [8, § 138] : $(f, \ell)^2 = 0$.

$f, x_1;\quad H = (f,f)^2, x_2^2;\quad i := (f,f)^4, x_3^2;$
$t = (f,H)^1,\ x_2^3;\quad c_{3,5} := (i,f)^1,\ x_3^2x_2;\quad c_{3,3} := (i,f)^2,\ x_3^3;$
$c_{4,6} := (c_{3,3},f)^1,\ x_3^3x_2;\quad c_{4,4} := (c_{3,3},f)^2,\ x_3^4;\quad c_{4,0} := (i,i)^2,\ x_4^2x_3^2;$
$c_{5,7} := (c_{4,4},f)^1,\ x_3^4x_2;\quad c_{5,3} := (c_{3,3},i)^1,\ x_4^2x_3^2x_2;\quad c_{5,1} := (c_{3,3},i)^2,\ x_4^2x_3^3;$
$c_{6,4} := (c_{4,4},i)^1,\ x_4^2x_3^3x_2;\quad c_{6,2} := (c_{3,3},c_{3,3})^2,\ x_4^2x_3^4;$
$c_{7,5} := (c_{4,4},c_{3,3})^1,\ x_4^2x_3^4x_2;\quad c_{7,1} := (c_{4,4},c_{3,5})^4,\ x_4^3x_3^4;$
$c_{8,2} := (c_{4,4},c_{4,6})^4,\ x_4^3x_3^5;\quad c_{8,0} := (c_{4,4},c_{4,4})^4,\ x_4^4x_3^4;$
$c_{9,3} := (c_{6,2},c_{3,3})^1,\ x_4^3x_3^6;\quad c_{11,1} := (c_{5,1},c_{6,2})^1,\ x_4^5x_3^6;\quad c_{12,0} := (c_{6,2},c_{6,2})^2,\ x_4^6x_3^6;$
$c_{13,1} := (c_{7,1},c_{6,2})^1,\ x_4^6x_3^7;\quad c_{18,0} := (c_{13,1},c_{5,1})^1,\ x_5^2x_4^5x_3^{11}.$
For comparison, the Grace & Young degree 18 covariant is $(i^7, ft)^{14}$.

A SAGBI basis for $\mathbf{Q}[x_1,x_2,x_3,x_4,x_5,x_6]^{\mathbf{Z}}$ through degree 25 was computed using a variation of Algorithm 4.3 in Magma [2] on Medicis[4]. The lead monomials for the 60 generators:
$x_1,\ x_2^2,\ x_3^2,\ x_2^3,\ x_3^2x_2,\ x_3^3,\ x_4^2x_2^2,\ x_3^3x_2,\ x_4^2x_3^2,$
$x_4^2x_2^3,\ x_4^2x_3^2x_2,\ x_4^2x_3^3,\ x_4^3x_2^3,\ x_4^2x_3^3x_2,\ x_4^3x_3^2x_2,\ x_4^3x_2^4,\ x_4^4x_2^3,\ x_4^3x_2^2x_2^2,\ x_4^3x_3^3x_2,\ x_4^3x_3^4,$
$x_4^5x_2^3,\ x_4^3x_3^3x_2^2,\ x_5^2x_4^2x_3^2x_2^2,\ x_4^3x_3^5,\ x_4^5x_2^4,\ x_4^5x_3^2x_2^2,\ x_4^6x_2^4,\ x_4^5x_3^3x_2^2,\ x_4^6x_3^2x_2^2,$
$x_4^7x_2^4,\ x_4^6x_3^3x_2^2,\ x_5^2x_4^2x_3^6x_2,\ x_4^8x_2^4,\ x_5^2x_4^2x_3^7x_2,\ x_5^2x_4^2x_3^8,\ x_4^8x_2^5,\ x_5^2x_4^2x_3^9,\ x_4^9x_2^5,\ x_4^8x_3^3x_2^3,$
$x_4^{10}x_2^5,\ x_4^9x_3^3x_2^3,\ x_4^{11}x_2^5,\ x_4^9x_3^5x_2^2,\ x_4^{11}x_2^6,\ x_4^{10}x_3^4x_2^3,\ x_5^2x_4^5x_3^9x_2,$
$x_4^{12}x_2^6,\ x_4^{11}x_3^3x_2^4,\ x_5^2x_4^5x_3^{11},\ x_4^{13}x_2^6,\ x_4^{14}x_2^6,\ x_4^{14}x_2^7,\ x_4^{13}x_3^4x_2^4,$
$x_4^{15}x_2^7,\ x_4^{14}x_3^3x_2^5,\ x_4^{14}x_3^4x_2^4,\ x_4^{16}x_2^7,\ x_4^{14}x_3^5x_2^4,\ x_4^{17}x_2^7,\ x_4^{17}x_2^8.$

Conjecture 6.1. *Using the graded reverse lexicographic order with* $x_1 < x_2 < x_3 < x_4 < x_5 < x_6$,
(i) For a given $k > 1$, *the smallest* j *such that* $x_4^k x_2^j$ *is the lead monomial of a rational invariant is given by* $j = \lfloor \frac{k}{3} \rfloor + 2$;
(ii) The rational invariants do not have a finite SAGBI basis.

Reviewing the SAGBI basis through degree 25 verifies (i) for $k \leq 17$. The second part of the conjecture is easily seen to be a consequence of the first.

The preceding analysis of the binary quintic originated in an attempt to construction of a finite SAGBI basis for $\mathbf{F}_p[V_6]^{\mathbf{Z}/p}$. We know that $\mathbf{F}_p[V_6]^{\mathbf{Z}/p}$ does have a finite SAGBI basis. However, the rôle that the subring of rational invariants will play in the description of this SAGBI basis is unclear.

Acknowledgements. I thank Eddy Campbell and David Wehlau for organising the *Workshop on Invariant Theory*. I thank Medicis (CNRS/École Polytechnique) for access to computer resources including Magma version 2.8 .

References

[1] G. Almkvist, *Invariants, mostly old ones*, Pacific J. of Math. **86** (1980) no. 1, 1–13.
[2] W. Bosma, J.J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Sym. Comp. **24** (1997) 235–265.

[4] http://www.medicis.polytechnique.fr/medicis/cri-eng.html

[3] H.E.A. Campbell and I.P. Hughes, *Vector invariants of $U_2(\mathbf{F}_p)$: A proof of a conjecture of Richman*, Adv. in Math. **126** (1997) 1–20.
[4] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, 1992.
[5] L.E. Dickson, *On invariants and the theory of numbers*, The Madison Colloquium (1913) Amer. Math. Soc., reprinted by Dover, 1966.
[6] M. Göbel, *Computing Bases for Rings of Permutation-invariant Polynomials*, J. Sym. Comp. **19** (1995) 285–291.
[7] M. Göbel, *A Constructive Description of SAGBI Bases for Polynomial Invariants of Permutation Groups*, J. Sym. Comp. **26** (1998) 261–272.
[8] J. H. Grace and A. Young, *The Algebra of Invariants*, Cambridge Univ. Press, 1903.
[9] D. Hilbert, *Theory of Algebraic Invariants (1897)*, translated by R.C. Laubenbacher, edited and with an introduction by B. Sturmfels, Cambridge Univ. Press, 1993.
[10] I. Hughes and G. Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. in Alg. **28** (2000) 2059–2088.
[11] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis of a k-subalgebra*, Proceedings of Computers and Mathematics 89, editors: E. Kaltofen and S. Watt, 1–11, MIT, 1989.
[12] J.P.S. Kung and G.-C. Rota, *The Invariant Theory of Binary Forms*, Bull. Amer. Math. Soc., **10** (1984) no. 1, 27–92.
[13] P.J. Olver, *Classical Invariant Theory*, Cambridge Univ. Press, 1999.
[14] L. Robbiano and M. Sweedler, *Subalgebra bases*, Lecture Notes in Mathematics **1430**, pp. 61–87, Springer–Verlag, 1990.
[15] R.J. Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants*, Commentarii Mathematici Helvetici **73** (1998) no. 4, 548–565.
[16] R.J. Shank and D.L. Wehlau, *The Transfer in Modular Invariant Theory*, J. of Pure and Applied Algebra **142** (1999) no. 1, 63–77.,
[17] R.J. Shank and D.L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002) 438–450.
[18] R.J. Shank and D.L. Wehlau, *Computing modular invariants of p-groups*, IMS Technical Report, UKC/IMS/01/27, June 2001 (revised April 2002), to appear in J. Sym. Comp.
[19] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, 1993.
[20] B. Sturmfels, *Gröbner bases and convex polytopes*, Amer. Math. Society, 1996.
[21] J.J. Sylvester, *A synoptical table of the irreducible invariants and covariants to a binary quintic, with a scholium on a theorem in conditional hyperdeterminants*, Amer. J. Math. **1** (1878) 370–378.

Institute of Mathematics & Statistics,
University of Kent at Canterbury, CT2 7NF, UK
E-mail address: R.J.Shank@ukc.ac.uk