

INVARIANTS, MOSTLY OLD ONES

GERT ALMKVIST

Dedicated to Gerhard Hochschild on the occasion of his 65th birthday

1. Introduction. Let G be the group with p elements where p is a prime number and let k be a field of characteristic p . Then

$$V_n \cong k[x]/(x-1)^n \quad \text{for } n = 1, 2, \dots, p$$

are the only indecomposable $k[G]$ -modules (observe that $V_p = k[G]$ is free). The r th symmetric power $S^r V_{n+1}$ can be written as a direct sum of indecomposables. Let $b_{n,r}$ denote the number of indecomposables for p large (i.e., $p > nr + 1$) and define the "false" Hilbert series by

$$\psi_n(t) = \sum_{r=0}^{\infty} b_{n,r} t^r.$$

One way to find e.g., $\psi_3(t)$ is to actually compute the decompositions of $S^r V_4$ and counting the components. Then we get the following series for $b_{3,r}$

$$1, 1, 2, 3, 5, 6, 8, 10, 13, 15, 18, 21, 25, 28, \dots$$

Guessing a difference equation and solving for $b_{3,r}$ and adding up we get $\psi_3(t)$. For $n = 5$ this method is too tedious and ψ_5 and ψ_6 in [1] were found by other methods (see Ch. V in [1]). After the manuscript of [1] was completed I found that ψ_n for 2, 3, 4 agreed with the generating function for the number of covariants of a binary form of degree n in Faa de Bruno [4]. Later I learned that Franklin and Sylvester a century ago computed ψ_n for $n=1, 2, \dots, 10$ and 12 and that our ψ_5 and ψ_6 up to some misprints agreed with theirs.

That this agreement is no coincidence is explained in §2. It turns out that our G -invariants are identical with what Dickson [3] calls a formal modular semi invariant. For p large they agree with the leading terms (which are semi invariants) of covariants in characteristic zero. Thus from [1] we get the following integral formula for the counting function of covariants

$$\psi_n(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1 + \cos \varphi}{\prod_{\nu=0}^n (1 - te^{i(n-2\nu)\varphi})} d\varphi.$$

In §3 it is proved that

$$\psi_n(t^{-1}) = (-1)^n t^{n+1} \psi_n(t)$$

thus solving Problem VI. 3.12 of [1]. The proof uses the integral above and residue calculus. In a private communication R. P. Stanley has given a proof using his "Combinatorial Reciprocity Theorem" [5].

In §4 we try to compute the ring $(S \cdot V_4)^G$ when $p = 5$. The twelve generators are found in Dickson [3] and in Williams [8] and the Hilbert series $\phi_3(t)$ of [1] tells us where to look for the relations. There are at least 16 relations ranging from degree 6 up to degree 10. The eight worst ones were found by Jan Bohman. Using an APL-program he had a computer write down the matrix and then solved the system of equations by hand. The results were then checked by the computer.

In [2] the number of non-free components of $S^r V_{n+1}$ was computed. In §5 similar formulas for the number of free components are found. There are several corollaries that can be formulated in pure combinatorial language with no reference to invariant theory.

R. P. Stanley corrected some mistakes in the first draft of this paper. I am most grateful for this. Finally I wish to thank Jan Bohman whose computations have been invaluable to me.

NOTATIONS.

p is an odd prime

$A(m, n, r)$ = the number of partitions of m into at most n parts all of size $\leq r$. $pd_A S$ = projective dimension of the A -module S .

2. Invariants, semi invariants and covariants.

2.1. *Classical invariants.* For the benefit of the reader we first review some of the classical invariant theory. The coefficients are the rational numbers. Let a binary form

$$f(x, y) = \sum_{i=0}^n \binom{n}{i} a_i x^{n-i} y^i$$

of degree n be given.

Then a polynomial

$$F(a_0, a_1, \dots, a_n, x, y) = \sum_{j=0}^m \binom{m}{j} c_j x^{m-j} y^j$$

is called a *covariant* of *index* λ and *order* m if the following condition is fulfilled ($c_j = c_j(a_0, \dots, a_n)$ are polynomials with integral coefficients): Make the substitution

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \xi \\ \eta \end{pmatrix} = T \begin{pmatrix} \xi \\ \eta \end{pmatrix}$$

with $\det T \neq 0$. The form becomes

$$f = \sum_{i=0}^n \binom{n}{i} A_i \xi^{n-i} \eta^i.$$

Then

$$F(A_0, \dots, A_n, \xi, \eta) = (\det T)^2 F(a_0, \dots, a_n, x, y).$$

Assign a *weight* ν to a_ν . Then $c_j(a_0, \dots, a_n)$ is *homogeneous* of degree r where

$$nr = 2\lambda + m$$

and is *isobaric* (all terms have the same weight) of weight $\lambda + j$. We note the following facts:

PROPOSITION 2.1. (i) F is uniquely determined by its leading term c_0 .

(ii) The number of linearly independent covariants F of the n -form f with leading term c_0 of degree r is

$$A\left(\left[\frac{nr}{2}\right], r, n\right)$$

(see *Faa de Bruno* [4] p. 235).

A polynomial $c = c(a_0, \dots, a_n) \in Z[a_0, \dots, a_n]$ is a *semi invariant* (for f) if it is invariant under the transformation

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Then

PROPOSITION 2.2. c is a semi invariant if and only if

(1) c is homogeneous and isobaric

(2) $c(a_0, a_1, a_2 + 2a_1 + a_0, \dots, a_n + \binom{n}{1}a_{n-1} + \binom{n}{2}a_{n-2} + \dots + a_0) = c(a_0, a_1, \dots, a_n)$.

2.2. *Modular invariants.* Now we consider polynomial with coefficients in $k = Z/pZ$. Let $G = \langle \sigma \rangle$ be the group with p elements (written multiplicatively). Let G act on $k[a_0, a_1, \dots, a_n]$ via

$$\begin{aligned}\sigma a_0 &= a_0 \\ \sigma a_1 &= a_1 + a_0 \\ \sigma a_n &= a_n + \binom{n}{1} a_{n-1} + \binom{n}{2} a_{n-2} + \cdots + a_0.\end{aligned}$$

Then $c(a_0, \dots, a_n)$ is a G -invariant if and only if

$$(*) \quad c\left(a_0, a_1 + a_0, \dots, a_n + \binom{n}{1} a_{n-1} + \cdots + a_0\right) = c(a_0, \dots, a_n).$$

This is exactly what Dickson [3] calls a (*formal*) *modular semi invariant* for the binary form

$$f = \sum_{i=0}^n \binom{n}{i} a_i x^{n-i} y^i.$$

Then $c \in (S^r V_{n+1})^G$ in the notation of [1] means that c is a modular semi invariant that is homogeneous of degree r . Hence all results in Chapter V in [1] are also results for modular semi invariants of a binary form.

Let us now turn to the case when p is large. We introduce the differential operator

$$\Omega = a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + na_{n-1} \frac{\partial}{\partial a_n}.$$

If $c(a_0, \dots, a_n)$ is homogeneous of degree r and isobaric of weight w then Ωc is isobaric of weight $w-1$.

PROPOSITION 2.3. *Assume that $p > nr$ where degree $c = r$. Then c is G -invariant if and only if $\Omega c = 0$.*

Proof. In Williams [8] it is proved that c is a modular semi invariant if and only if

$$\left(\Omega + \frac{\Omega^p}{p!} + \frac{\Omega^{2p-1}}{(2p-1)!} + \cdots \right) c = 0.$$

But weight $(c) \leq nr < p$ and hence $\Omega^p c = 0$ since Ω diminishes the weight with one each time it is applied.

PROPOSITION 2.4. *Assume that $p > nr$. Then there is a basis of G -invariants homogeneous of degree r consisting of isobaric polynomials.*

Proof. Assume that $c = c_1 + c_2 + \cdots + c_s$ where the c_i 's are

isobaric of weights

$$w_1 > w_2 > \cdots > w_s .$$

Apply Ω

$$0 = \Omega c = \Omega c_1 + \cdots + \Omega c_s .$$

But weight $(\Omega c_i) = w_i - 1$ and hence $\Omega c_i = 0$ for all i .

THEOREM 2.5. *Let h_1, \dots, h_s be a basis over \mathbb{Q} for the covariants having leading terms of degree r . Let c_1, \dots, c_s be their leading terms (with coefficients in Z). Reduce the coefficients (mod p). If p is large then $\bar{c}_1, \dots, \bar{c}_s$ is a basis over Z/pZ for the homogeneous G -invariants of degree r .*

Proof. The c_1, \dots, c_s are isobaric and are semi invariants, hence they satisfy $\Omega c_i = 0$. It follows that $\overline{\Omega c_i} = 0$ and all the c_i 's are G -invariants. Now both the vector space of covariants having leading terms of degree r and the homogeneous G -invariants of degree r have dimension

$$s = A\left(\left[\frac{nr}{2}\right], n, r\right)$$

over \mathbb{Q} and Z/pZ respectively. Hence we need only to show that $\bar{c}_1, \dots, \bar{c}_s$ are linearly independent over Z/pZ . Express c_1, \dots, c_s as linear combinations of Z of all monomials of degree r in a_0, a_1, \dots, a_n . The resulting matrix has \mathbb{Q} -rank = s since c_1, \dots, c_s are linearly independent. Then some $s \times s$ subdeterminant is nonzero. If p is large enough then it is still nonzero after reduction (mod p). Hence $\bar{c}_1, \dots, \bar{c}_s$ are linearly independent over Z/pZ .

COROLLARY 2.6. *Let $b_{n,r}$ be the number of linearly independent covariants with leading term of degree r . Then*

$$\sum_{r=0}^{\infty} b_{n,r} t^r = \psi_n(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{1 + \cos \varphi}{\prod_{\nu=0}^n (1 - t e^{i(n-2\nu)\varphi})} d\varphi .$$

3. Proof of $\psi_n(t^{-1}) = (-1)^n t^{n+1} \psi_n(t)$. In [1] it was proved that

$$(*) \quad \psi_n(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi \text{ for } |t| < 1$$

where

$$g_n(t, \varphi) = \prod_{\nu=0}^n (1 - t e^{i(n-2\nu)\varphi})^{-1} .$$

It is also proved that ψ_n is a rational function.

THEOREM 3.1. $\psi_n(t^{-1}) = (-1)^n t^{n+1} \psi_n(t)$.

Proof. If we simply change t to t^{-1} in the integral we will get the wrong sign. This depends on the fact that (*) is not valid for $|t| > 1$. We rather have

$$(**) \quad \frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi = -\psi_n(t) \text{ if } |t| > 1.$$

Put $z = e^{i\varphi}$ and write the integral as

$$\begin{aligned} \frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi &= \frac{1}{2\pi i} \int_{\Gamma} \frac{1/2 + 1/z + 1/2z^2}{\prod_{\nu=0}^n (1 - tz^{n-2\nu})} dz \\ &= \frac{1}{2\pi i} \int_{\Gamma} f(z) dz \end{aligned}$$

where Γ is the unit circle in positive sense.

The rational function

$$f(z) = \frac{(1+z)^2}{z^2 \prod_{\nu=0}^n (1 - tz^{n-2\nu})}$$

has the following poles (remember $|t| > 1$).

(a) *Inside* Γ . $u_j(t) =$ all solutions to the equations $z^{n-2\nu} = 1/t$ for $0 \leq \nu < n/2$.

(b) *Outside* Γ . $v_j(t) = u_j(t)^{-1} =$ all solutions to the equations $z^{n-2\nu} = t$ for $0 \leq \nu < n/2$. Then

$$\frac{1}{2\pi i} \int_{\Gamma} f(z) dz = \sum_{z=u_j(t)} \text{Res } f(z) = - \sum_{z=v_j(t)} \text{Res } f(z)$$

since the sum of the residues at all poles of a rational function is zero.

Let us now for a moment think of t as satisfying $|t| < 1$. Then by (*) we have (since now the $v_j(t)$:s are inside Γ)

$$\psi_n(t) = \frac{1}{2\pi i} \int_{\Gamma} f(z) dz = \sum_{z=v_j(t)} \text{Res } f(z)$$

as a function of t . Hence for $|t| > 1$ again we get

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi = - \sum_{z=v_j(t)} \text{Res } f(z) = -\psi_n(t)$$

and (**) is proved. Now we observe that

$$(1 - 2t \cos \varphi + t^2)^{-1} = \begin{cases} (1 - t^2)^{-1} \left(1 + 2 \sum_1^{\infty} t^{\nu} \cos 2\nu\varphi\right) & \text{if } |t| < 1 \\ -(1 - t^2)^{-1} \left(1 + 2 \sum_1^{\infty} t^{-\nu} \cos 2\nu\varphi\right) & \text{if } |t| > 1. \end{cases}$$

Assume that $n = 2m$ is even. Then

$$g_n(t, \varphi) = \begin{cases} \frac{1}{1-t} \cdot \frac{1}{(1-t^2)^m} \sum_0^{\infty} d_{\nu}(t) \cos \nu\varphi & \text{if } |t| < 1 \\ \frac{1}{1-t} \cdot \frac{(-1)^m}{(1-t^2)^m} \sum_0^{\infty} d_{\nu}\left(\frac{1}{t}\right) \cos \nu\varphi & \text{if } |t| > 1 \end{cases}$$

where the $d_{\nu}(t)$:s are rational functions of t . Multiplying by $1 + \cos \varphi$ and integrating over φ we get

$$\begin{aligned} \psi_n(t) &= \frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi = \frac{1}{1-t} \cdot \frac{1}{(1-t^2)^m} k_n(t) \quad \text{if } |t| < 1 \\ -\psi_n(t) &= \frac{1}{2\pi} \int_{-\pi}^{\pi} g_n(t, \varphi) (1 + \cos \varphi) d\varphi = \frac{1}{1-t} \cdot \frac{(-1)^m}{(1-t^2)^m} k_n\left(\frac{1}{t}\right) \\ &\quad \text{if } |t| > 1. \end{aligned}$$

Hence for $|t| < 1$ we get

$$\begin{aligned} \psi_n(t^{-1}) &= -\frac{1}{1-t^{-1}} \cdot \frac{(-1)^m}{(1-t^{-2})^m} k_n(t) = \frac{t^{n+1}}{(1-t)(1-t^2)^m} k_n(t) \\ &= t^{n+1} \psi_n(t). \end{aligned}$$

Similarly if n is odd we get

$$\psi_n(t^{-1}) = -t^{n+1} \psi_n(t).$$

COROLLARY 3.2. Define $H(\nu)$ by

$$\psi_n(t) = \sum_{\nu=0}^{\infty} A\left(\left[\frac{n\nu+1}{2}\right], \nu, n\right) t^{\nu} = \sum_{\nu=0}^n H(\nu) t^{\nu}.$$

Then

$$H(-\nu) = \begin{cases} 0 & \text{if } \nu = 1, 2, \dots, n \\ H(\nu - n - 1) & \text{if } \nu > n + 1. \end{cases}$$

Proof. First note that from Theorem 3.1 it follows that the degree of the rational function $\psi_n(t)$ is $-(n+1) < 0$. Hence there is for some N an N th root of unity ζ and polynomials p_0, \dots, p_{n-1} such that $H(\nu) = \sum_{j=0}^{N-1} \zeta^{j\nu} p_j(\nu)$. We thus can define $H(-\nu) = \sum_j \zeta^{-j\nu} p_j(-\nu)$. The rest follows from 4.7 in Stanley [6].

4. **Computation of the ring of invariants in four variables when $p = 5$.** In this section we explicitly compute the ring $S = S \cdot V_4^G$ when $G = Z/5Z$. It can be described as the set of all polynomials f in $k[x_0, x_1, x_2, x_3]$ where $\text{char } k = 5$ such that

$$f(x_0, x_1 + x_0, x_2 + 2x_1 + x_0, x_3 + 3x_2 + 3x_1 + x_0) = f(x_0, x_1, x_2, x_3).$$

The S is graded in a natural way by

$$S_i = \{f \in S; \deg f = i\}$$

and

$$\varphi_3(t) = \sum_0^{\infty} \dim_k(S_i)t^i$$

is the *Hilbert series* of S . In [1] φ_3 was computed for all p and for $p = 5$ we get

$$H_i(S) = \Phi_3(t) = \frac{1 - t + t^2 + t^3 + 2t^5}{(1 - t)^2(1 - t^4)(1 - t^5)} = \frac{1 - 2t + 2t^2}{(1 - t)^3(1 - t^5)}.$$

Unfortunately Φ_3 does not give much information about the generators of S . In Dickson [3] and Williams [8] the following result is found: S is generated by the following twelve polynomials (the subscript indicates the degree)

$$\begin{aligned} u_1 &= x_0 \\ u_2 &= x_0x_2 - x_1^2 \\ u_3 &= x_0^2x_3 + 2x_0x_1x_2 + 2x_1^3 \\ v_3 &= (2x_1^2 - 2x_0x_2)x_3 + x_1x_2^2 - x_0^2x_1 \\ u_4 &= (x_0x_2 - x_1^2)x_3^2 + (x_0^2x_1 - x_1x_2^2)x_3 + x_1^4 + x_2^4 - x_0^2x_2^2 - x_0x_1^2x_2 \\ v_4 &= x_0^2x_3^2 - (x_0x_1x_2 + x_1^3)x_3 + 2x_1^2x_2^2 - x_0x_2^3 \\ u_5 &= -x_0^2x_3^3 - (x_0x_1x_2 + x_1^3)x_3^2 + (3x_0x_2^3 - x_1^2x_2^2)x_3 + x_0^2x_1x_2^2 - 2x_0x_1^3x_2 + x_0^4x_1 \\ v_5 &= x_2(x_0^4 - x_1^4 + x_2^4 - 2x_0^2x_2^2 + x_0x_1^2x_2) \\ w_5 &= x_3^5 + (2x_1^2 - 2x_0x_2)x_3^3 + (2x_0^2x_1 - 2x_1x_2^2)x_3^2 + (-x_0^4 + x_1^4 - x_2^4 - 2x_0^2x_2^2 \\ &\quad + 2x_0x_1^2x_2)x_3 \\ u_6 &= x_0^2x_3^4 - (2x_0x_1x_2 + x_1^3)x_3^3 + (2x_1^2x_2^2 - x_0x_2^3)x_3^2 + (x_0^4x_1 + x_0^2x_1x_2^2 - x_0x_1^3x_2 \\ &\quad + x_1x_2^4)x_3 + x_2^6 + x_0^2x_1^4 - x_0x_1^2x_2^3 - 2x_0^2x_2^4 + 2x_0^2x_2^4 \\ v_6 &= -x_0x_3^5 + x_3^5x_3 + 2x_1^5x_2 - 2x_1x_2^5 \\ v_7 &= (2x_0x_1^2 - 2x_0^2x_2)x_3^4 + x_0x_1(x_0^2 - x_2^2)x_3^3 - x_0(2x_2^4 + 2x_0^2x_2^2 + 2x_0^4 \\ &\quad + x_1^4)x_3^2 + (-x_0^4x_1x_2 - 2x_0^2x_1x_2^3 + 2x_0x_1^3x_2^2 - 2x_1^5x_2 + 2x_1x_2^5)x_3 \\ &\quad + (-x_0^5x_1^2 - 2x_0^4x_2^2 + 2x_0^2x_1^2x_2 - x_0x_1^2x_2^4 - x_1^4x_2^2 + x_2^7). \end{aligned}$$

Multiplying Φ_3 with factors of the form $1 - t^{d_i}$ where d_i is the

degree of the generator we get

$$H_t(S) = \Phi_s(t) = h(t)/(1-t)(1-t^2)(1-t^3)^2(1-t^4)^2(1-t^5)^3(1-t^6)^2(1-t^7)$$

where

$$\begin{aligned} h(t) = & 1 - 3t^6 - 3t^7 - 5t^8 - 4t^9 - t^{10} + 6t^{11} + 13t^{12} + 19t^{13} + 19t^{14} \\ & + 9t^{15} - 5t^{16} - 25t^{17} - 36t^{18} - 41t^{19} - 29t^{20} - 2t^{21} + 23t^{22} + 35t^{23} \\ & + 53t^{24} + 44t^{25} + 21t^{26} - t^{27} - 28t^{28} - 41t^{29} - 32t^{30} - 27t^{31} - 6t^{32} \\ & + 9t^{33} + 13t^{34} + 14t^{35} + 12t^{36} + 6t^{37} - 8t^{39} - 2t^{40} + t^{41} + 2t^{42} + 2t^{43}. \end{aligned}$$

Let now $A = k[y_1, \dots, y_{12}]$ be the polynomial ring in twelve variables and consider the free A -resolution of S .

$$0 \longrightarrow M_d \longrightarrow \dots \longrightarrow M_2 \longrightarrow M_1 \longrightarrow A \xrightarrow{\pi} S \longrightarrow 0$$

where $\pi(y_1) = u_1, \dots, \pi(y_{12}) = u_7$.

It follows that M_1 is the ideal generated by the relations between the u_1, \dots, u_7 . Let $\{y_{ij}\}$ be a minimal A -basis for M_i with $\deg y_{ij} = d_{ij}$. Then we get the Hilbert series

$$\begin{aligned} H_t(S) &= (1 + \sum_{ij} (-1)^i t^{d_{ij}}) H_t(A) \\ &= h(t)/(1-t)(1-t^2)(1-t^3)^2(1-t^4)^2(1-t^5)^3(1-t^6)^2(1-t^7). \end{aligned}$$

Unfortunately the Hilbert series does not completely determine the number of relations, first syzigies etc. There can be cancellations in the numerator. The following example (due to R. P. Stanley) shows the difficulties: The ring

$$T = k[x, y, z, w]/(xw, yw, zw, xyz)$$

has the Hilbert series

$$H_t(T) = \frac{1 - 3t^2 + 2t^3}{(1-t)^4}$$

but T has 4 relations and $pd_{k[x,y,z,w]}(T) = 3$. Thus we should really write

$$H_t(T) = \frac{1 - (3t^2 + t^3) + (3t^3 + t^4) - t^4}{(1-t)^4}.$$

Much work was spent on finding the relations. Let us indicate the difficulties for the five relations of degree eight. There are 47 monomials $u_1^8, u_1^6 u_2, \dots, u_1 u_7$ of degree 8. Expressing these in the $\binom{8+3}{3} = 165$ monomials $x_0^8, x_0^7 x_1, \dots, x_3^8$ we get a homogeneous linear system of equations with 47 unknowns and 165 equations. Several

reductions can be made but the relations were essentially found by Jan Bohman by solving these equations by hand. Using the computer language APL he could easily check the relations found.

THEOREM 4.1. *Let $p = 5$. Then $S = S \cdot V_4^G$ has 12 generators $u_1, u_2, u_3, v_3, u_4, u_5, v_5, w_5, u_6, v_6, u_7$ and at least the following 16 relations*

$$\begin{aligned}
R_1 &= u_3^2 - u_2^3 - u_1^2 v_4 \\
R_2 &= v_3^2 + u_2 u_4 - u_2^3 + u_1^4 u_2 - u_1 v_5 \\
R_3 &= u_3 v_3 + u_1^2 u_4 + u_2 v_4 + u_1^2 u_2^2 \\
R_4 &= u_1^2 u_5 + u_3 v_4 + 2u_1^2 u_2 u_3 + u_2^2 v_3 + u_1^4 v_3 \\
R_5 &= u_3 u_4 + v_3 v_4 - u_2 u_5 - u_2^2 u_3 - u_1^2 u_2 v_3 \\
R_6 &= u_1 v_6 + u_1^2 w_5 - u_3 u_4 + v_3 v_4 + u_2^2 u_3 \\
R_7 &= u_2 v_6 - u_3 v_5 + u_1 u_2 w_5 - u_1 v_3 u_4 + u_1^3 u_2 u_3 - u_1 u_2^2 v_3 \\
R_8 &= u_2 u_6 - v_3 u_5 - u_1^3 v_5 + 2u_1^2 u_2 u_4 + u_4 v_4 - u_2^2 v_4 - u_1^6 u_2 + 2u_1^2 u_3^2 \\
R_9 &= u_1 u_7 - u_2 u_6 - v_3 u_5 + 2u_1^2 u_2 u_4 + 2u_1^4 v_4 - u_1^2 u_3^2 \\
R_{10} &= u_1^2 u_6 - u_3 u_5 + u_1 u_2 v_5 - 2v_4^2 + u_1^4 u_2^2 \\
R_{11} &= u_3 u_5 - u_1^4 u_4 - u_2^2 u_4 + v_4^2 + u_1^2 u_2 v_4 - u_1^4 u_2^2 + u_2^4 \\
R_{12} &= u_1 v_3 w_5 + u_1 u_4^2 - u_1^3 u_2 v_4 + v_4 v_5 + v_3 v_6 - u_1 u_4^4 \\
R_{13} &= -2u_1^2 u_2 v_5 + u_1 u_3^2 u_4 + u_1 u_4^2 + 2u_1^3 u_2 v_4 - 2u_2 u_7 - v_4 v_5 + 2u_1^5 u_2^2 \\
&\quad - 2u_1 u_4^4 \\
R_{14} &= -u_1^2 u_2 w_5 + 2u_1^2 v_3 u_4 - v_3 u_6 - u_2^2 u_5 + u_4 u_5 - u_1^4 u_2 u_3 + u_1^2 u_2^2 v_3 \\
R_{15} &= u_1 v_3 v_5 + u_1^4 w_5 + u_1^2 v_3 v_4 - u_1^2 u_3 u_4 + u_1^6 u_3 - u_1^2 u_2^2 u_3 - 2u_1^4 u_2 v_3 \\
&\quad + 2u_3 u_6 - 2v_4 u_5 \\
R_{16} &= u_1^3 u_3 v_4 - u_1^3 u_2 w_5 - u_1^3 v_3 u_4 - 2u_1 u_4 u_5 - 2u_3 u_7 + u_2 v_3 v_5 + u_1 u_2^2 u_5 \\
&\quad - u_1^2 u_3 v_5 - u_1^3 u_2^2 v .
\end{aligned}$$

The case $p = 7$. In his paper [8] Williams also found the 20 generators when $p = 7$. In this case the Hilbert series is

$$\Phi_3(t) = \frac{1 + t^3 + 2t^5 + 2t^6 + t^7 + t^8}{(1-t)(1-t^2)(1-t^4)(1-t^7)} .$$

Multiplying by the 16 factors $1 - t^{d_i}$ corresponding to the other 16 generators we get

$$\Phi_3(t) = \frac{1 - t^8 - t^7 - 2t^8 - 4t^9 - 7t^{10} - 5t^{11} - 4t^{12} + 2t^{13} + \dots + t^{137}}{(1-t)(1-t^2)(1-t^3)(1-t^4)(1-t^5)^2(1-t^6)^2(1-t^7)^3(1-t^8) \\ (1-t^9)^2(1-t^{10})^3(1-t^{11})^2(1-t^{12})} .$$

Hence there are at least 24 relations; probably 1 of degree 6, 1 of

degree 7, 2 of degree 8, 4 of degree 9, 7 of degree 10, 5 of degree 11 and 4 of degree 12. We see that the difficulties also increase with the prime p .

Problem. (i) Compute the minimal number $m = m(p, n)$ of generators of $S = S \cdot V_{n+1}^G$.

(ii) Let $A = k[y_1, \dots, y_m]$ as above.

Compute $pd_A S$.

5. The number of free components of $S^r V_{n+1}$ and some combinatorial formulas. In Chapter III and V of [1] we studied the decomposition of the symmetric power

$$S^r V_{n+1} = \bigoplus_{j=1}^p c_j V_j .$$

We found methods to compute c_j for $j = 1, 2, \dots, p-1$. Here we find a simple formula for c_p , the number of free components of $S^r V_{n+1}$. To indicate the dependence on n and r we denote this number by $d_{n,r}$. Recall that in [1] and [2] we get the following results:

Let

$a_{n,r}$ = the number of components of $S^r V_{n+1}$

$e_{n,r}$ = the number of non-free components of $S^r V_{n+1}$.

Then

$$a_{n,r} = \begin{cases} \sum_{\substack{m=0 \\ 2m \equiv rn}}^{rn} A(m, n, r) & \text{if } r \text{ or } n \text{ is even} \\ \sum_{\substack{m=0 \\ 2m \equiv rn+1}}^{rn} A(m, n, r) & \text{if both } r \text{ and } n \text{ are odd.} \end{cases}$$

$$e_{n,r} = (-1)^{nr} \left(\sum_{\substack{m=0 \\ 2m \equiv rn}}^{rn} A(m, n, r) - \sum_{\substack{m=0 \\ 2m \equiv rn+1}}^{rn} A(m, n, r) \right)$$

(all congruences are mod p).

Then

$$d_{n,r} = a_{n,r} - e_{n,r} \text{ and we get}$$

PROPOSITION 5.1. *The number of free components of $S^r V_{n+1}$ is*

$$d_{n,r} = \begin{cases} \sum_{\substack{m=0 \\ 2m \equiv rn+1}}^{rn} A(m, n, r) & \text{if } r \text{ or } n \text{ is even} \\ \sum_{\substack{m=0 \\ 2m \equiv rn}}^{rn} A(m, n, r) & \text{if both } r \text{ and } n \text{ are odd.} \end{cases}$$

We get several corollaries that can be formulated in pure combinatorial language. In all the following formulas $0 < r, n < p$.

COROLLARY 5.2. *If $n + r \geq p$ the $S^r V_{n+1}$ is free and*

$$a_{n,r} = d_{n,r} = \frac{1}{p} \binom{n+r}{n}.$$

COROLLARY 5.2'. *If $n + r \geq p$ then*

$$\sum_{\substack{m=0 \\ 2m \equiv r n + 1}}^{r n} A(m, n, r) = \sum_{\substack{m=0 \\ 2m \equiv r n}}^{r n} A(m, n, r) = \frac{1}{p} \binom{n+r}{n}.$$

COROLLARY 5.3. *If $r + n = p - 1$ then*

$$d_{n,r} = \begin{cases} \frac{1}{p} \left(\binom{p-1}{n} - 1 \right) & \text{if } n \text{ is even} \\ \frac{1}{p} \left(\binom{p-1}{n} - p + 1 \right) & \text{if } n \text{ is odd.} \end{cases}$$

COROLLARY 5.3'. *If $r + n = p - 1$ then*

$$\sum_{\substack{m=0 \\ 2m \equiv r n + 1}}^{r n} A(m, n, r) = \begin{cases} \frac{1}{p} \left(\binom{p-1}{n} - 1 \right) & \text{if } n \text{ is even} \\ \frac{1}{p} \left(\binom{p-1}{n} - p + 1 \right) & \text{if } n \text{ is odd and } r \text{ is even} \end{cases}$$

$$\sum_{\substack{m=0 \\ 2m \equiv r n}}^{r n} A(m, r, n) = \frac{1}{p} \left(\binom{p-1}{n} - p + 1 \right) \text{ if both } n \text{ and } r \text{ are odd.}$$

COROLLARY 5.4. *If $r + n = p - 2$ then*

$$d_{n,r} = \begin{cases} \frac{1}{p} \left(\binom{p-2}{n} - p + n \right) & \text{if } n \text{ is even} \\ \frac{1}{p} \left(\binom{p-2}{n} - n \right) & \text{if } n \text{ is odd.} \end{cases}$$

COROLLARY 5.4'. *If $r + n = p - 2$ then*

$$\sum_{\substack{m=0 \\ 2m \equiv r n + 1}}^{r n} A(m, n, r) = \begin{cases} \frac{1}{p} \left(\binom{p-2}{n} - p + n \right) & \text{if } n \text{ is even} \\ \frac{1}{p} \left(\binom{p-2}{n} - n \right) & \text{if } n \text{ is odd and } r \text{ is even} \end{cases}$$

$$\sum_{\substack{m=0 \\ 2m=rn}}^{rn} A(m, n, r) = \frac{1}{p} \left(\binom{p-2}{n} - n \right) \text{ if both } n \text{ and } r \text{ are odd.}$$

Proofs. 5.2 and 5.3 follow from III. 2.10 in [1] and 5.4 from Theorem 2 of [2].

REFERENCES

1. G. Almkvist and R. Fossum, *Decompositions of exterior and symmetric powers of indecomposable Z/pZ -modules in characteristic p and relations to invariants*, Sém. P. Dubreil 1966-67, Springer Lecture Notes nr 641.
2. G. Almkvist, *The number of non-free components of symmetric powers in characteristic p* , to appear in Pacific J. Math.
3. L. E. Dickson, *On invariants and the theory of numbers*, The Madison Colloquium (1913), AMS, reprinted by Dover, 1966.
4. F. Faa de Bruno, *Théorie des formes binaires*, Turin, 1876.
5. R. P. Stanley, *Combinatorial reciprocity theorems*, Adv. in Math., **14** (1974), 194-253.
6. ———, *Hilbert functions of graded algebras*, Adv. in Math, to appear.
7. J. J. Sylvester, *Collected Mathematical Papers*, Chelsea, 1973.
8. W. L. G. Williams, *Fundamental systems of formal modular semi invariants of the binary cubic*, Trans. Amer. Math. Soc., **21** (1921), 56-79.

Received April 24, 1978 and in revised form October 16, 1978.

INSTITUTE OF ALGEBRAIC MEDITATION
 PL 500
 S 24300 HÖÖR, SWEDEN

