NUMERICAL FORMS

J. R. HUBBUCK

ABSTRACT

Let I be the graded ring of homogeneous rational polynomials in n-variables which are numerical over $\mathbb{Z}$. Then I is a subring of Γ, the divided polynomial algebra over $\mathbb{Z}$ in the n-variables. A consequence of the main theorem is that for any positive integer k, the image of the induced homomorphism $I\otimes(\mathbb{Z}/k\mathbb{Z})\to\Gamma\otimes(\mathbb{Z}/k\mathbb{Z})$ is a finite graded ring.

1. *Introduction*

A rational polynomial $r(\underline{x})\in\mathbb{Q}[x_1, x_2, \dots, x_n]$ is numerical with respect to a subring R of $\mathbb{Q}$ if $r(\underline{x})\in R$ whenever $\underline{x}=(x_1, x_2, \dots, x_n)\in R^n$. In this paper, the symbol R will denote either $\mathbb{Z}_{(p)}$ or $\mathbb{Z}$, where the former is the ring of integers localised at the prime ideal (p) of $\mathbb{Z}$ for a fixed p. We use the notation $v\colon \mathbb{Q}-\{0\}\to\mathbb{Z}$ for the function defined by $v(s/t\cdot p^u)=u$ where s and t are integers prime to p. Thus the non-zero elements of $\mathbb{Z}_{(p)}$ are those rationals satisfying $v(q)\geqslant 0$ and the units are characterised by $v(q)=0$. It is convenient to set $v(0)=\infty$.

For each positive integer r, let

$$\gamma_r(x)=\binom{x}{r}=\frac{x(x-1)\dots(x-r+1)}{r!}$$

and set $\gamma_0(x)=1$.

PROPOSITION 1.1. *The set* $\{\gamma_{i_1}(x_1)\gamma_{i_2}(x_2)\dots\gamma_{i_n}(x_n)\}$, *each* $i_k\geqslant 0$, *gives a basis over* R *for the linear space of numerical polynomials.*

The result is well known but the author does not know a reference and a proof is included in Section 2. If $r(\underline{x})$ is a numerical polynomial of degree M, one can therefore write

$$r(\underline{x})=\sum a_{i_1, i_2, \dots, i_n}\gamma_{i_1}(x_1)\gamma_{i_2}(x_2)\dots\gamma_{i_n}(x_n), \tag{1}$$

where $a_{i_1, i_2, \dots, i_n}\in R$ and $I=i_1+i_2+\dots+i_n\leqslant M$.

This paper is about homogeneous numerical polynomials or numerical forms. By considering the leading terms of (1), it follows that when $r(\underline{x})$ is a numerical M-form,

$$r(\underline{x})=\sum a_{i_1, i_2, \dots, i_n}\frac{x_1^{i_1}}{i_1!}\frac{x_2^{i_2}}{i_2!}\dots\frac{x_n^{i_n}}{i_n!}, \tag{2}$$

where only those coefficients of (1) arise with $I=M$. This will be called the standard form for a numerical M-form and the $a_{i_1, i_2, \dots, i_n}$ with $I=M$ are the coefficients of the form.

Received 13 January 1994; revised 24 December 1994 and 2 March 1995.

1991 *Mathematics Subject Classification* 11E76.

J. London Math. Soc. (2) 55 (1997) 65–75

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

An example of a numerical 4-form over R in two variables is

$$\frac{x_1^3}{3!}\frac{x_2}{1!}-\frac{x_1}{1!}\frac{x_2^3}{3!}.$$

When this numerical form is expressed as in (1), it becomes

$$\gamma_3(x_1)\gamma_1(x_2)-\gamma_1(x_1)\gamma_3(x_2)+\gamma_2(x_1)\gamma_1(x_2)-\gamma_1(x_1)\gamma_2(x_2).$$

Numerical forms are familiar objects in some areas of mathematics, but there appears to be little about them in the literature. The only significant results known to the author appear in the work of K. Knapp [**4**] and L. Schwartz [**6**]; the latter is reproduced in [**1**]. A basis for the space of numerical M-forms over $\mathbb{Z}_{(p)}$ is constructed when $n = 2$.

For any n, one can construct sequences of M-forms $\{r_M(\underline{x})\}$ such that

$$\min v\left(\frac{a_{i_1,i_2,\ldots,i_n}}{i_1!\,i_2!\ldots i_n!}\right)\longrightarrow-\infty \quad \text{as } M\longrightarrow\infty.$$

For example, one can take powers of the anti-symmetric forms given later in this section. But in such sequences

$$\min v(a_{i_1,i_2,\ldots,i_n})\longrightarrow+\infty \quad \text{as } M\longrightarrow\infty.$$

It is this phenomenon which is investigated.

THEOREM 1.2. *Let k satisfy $0<k<1$. Then, for sufficiently large M, the coefficients of a numerical M-form in n-variables satisfy*

$$v(a_{i_1,i_2,\ldots,i_n})>\frac{kM}{m^n(\log_p M)^{n-1}} \quad \textit{for } m=p-1.$$

Now let $N = M-n+1$ and define the integer t by $p^{t+1}-1 > N \geqslant p^t-1$. The letter t will be reserved to represent this integer. Theorem 1.2 is a consequence of the following proposition.

PROPOSITION 1.3. *There exist monotonic increasing polynomials $u_n(z)$ and $v_n(z)$ such that the coefficients of any numerical M-form in n-variables satisfy*

$$v(a_{i_1,i_2,\ldots,i_n})>\frac{M-u_n(t)}{v_n(t)}.$$

Explicit polynomials $u_n(z)$ and $v_n(z)$ are described at the end of Section 3; in particular $v_n(z)$ has degree $(n-1)$ and leading coefficient m^n. The deduction of Theorem 1.2 from Proposition 1.3 is as follows. For $n>1$ we have $M\geqslant p^t$ and so $\log_p M\geqslant t$. The ratio of $(M-u_n(t))/v_n(t)$ and $M/m^n(\log_p M)^{n-1}$ can be written as $\{m^n(\log_p M)^{n-1}/v_n(t)\}\cdot\{1-u_n(t)/M\}$. The first term in parentheses in the latter is not less than $m^n t^{n-1}/v_n(t)$ which tends to 1 as M becomes large and clearly the second term tends to one. Theorem 1.2 follows for $n>1$; a minor modification is needed in the argument for $n=1$.

As $(M-u_n(t))\,v_n(t)^{-1}$ becomes large with t, and therefore with M, there exists a smallest integer $K_p(n,s)$ such that the coefficients of any numerical M-form are

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

divisible by p^s if $M > K_p(n,s)$. The initial motivation in writing this note was to establish the existence of $K_2(n,1)$ and to evaluate it; the latter appears to be difficult and the estimate for $K_2(n,1)$ obtained from the particular polynomials $u_2(z)$ and $v_2(z)$ constructed in the proof is much larger than the known value $K_2(2,1) = 4$ which can be derived from [**1**]. For $n > 2$ the value of $K_2(n,1)$ is not known. But showing the existence of $K_p(n,1)$ has been achieved only by first showing that $K_p(n-1,r)$ exists for all r.

The conclusion of Theorem 1.2 for all primes p leads immediately to the following corollary.

COROLLARY 1.4. *Let L be a positive integer. Then there exists an integer $K(n,L)$ such that the highest common factor of the coefficients of any M-form over $\mathbb{Z}$ is divisible by L provided that $M > K(n,L)$.*

Although the dimension of the linear space of numerical M-forms over R in n-variables is the same as the dimension of the space of rational M-forms over $\mathbb{Q}$, it is difficult to write down non-trivial examples of the former for $n > 2$. As mentioned above, a basis constructed by Schwartz is reproduced in [**1**, Section 1] when $n = 2$. But some comparatively simple anti-symmetric M-forms can be described. Let

$$\Delta(i_1, i_2, \dots, i_n) = (i_1! i_2! \dots i_n!)^{-1} \det \begin{bmatrix} x_1^{i_1} & x_2^{i_1} & \dots & x_n^{i_1} \\ x_1^{i_2} & x_2^{i_2} & \dots & x_n^{i_2} \\ \vdots & \vdots & & \vdots \\ x_1^{i_n} & x_2^{i_n} & \dots & x_n^{i_n} \end{bmatrix}.$$

Then $\Delta(1,2,\dots,n)$ is a numerical $\frac{1}{2}n(n+1)$-form and $\Delta(1,3,\dots,2n-1)$ is a numerical n^2-form over $\mathbb{Z}$. A proof is given in Section 4. As the non-zero coefficients of these forms are ± 1, it follows that $K_p(n,1) \geqslant n^2$ for any p. Although $K_2(2,1) = 4$, in general $K_2(n,1) \neq n^2$. The calculations of [**2**], when combined with the technique of the final section of this paper, show that among anti-symmetric numerical forms over $\mathbb{Z}_{(2)}$ of the type being considered, those of greatest degree for small values of n are

$$\begin{array}{lll} \Delta(1,3), & \Delta(1,3,7), & \Delta(1,3,5,7), \\ \Delta(1,3,5,7,9), & \Delta(1,3,5,7,9,11), & \Delta(1,3,5,7,9,11,15). \end{array}$$

So $K_2(3,1) \geqslant 11$ and $K_2(7,1) \geqslant 51$. This list can be extended for n up to the order 2^{10}.

The property that $r(\underline{x})$ is a numerical form is shared by all members of its conjugacy class; that is, when $\mathrm{GL}(n,R)$ acts on R^n, the space of $\underline{x}$, numerical polynomials transform to numerical polynomials. Also the highest common factor of the coefficients of an M-form is an invariant of its conjugacy class: the observation here is that the action of $\mathrm{GL}(n,R)$ extends to the divided polynomial algebra on $\{x_1, x_2, \dots, x_n\}$ over R, to which numerical polynomials belong by (2).

2. *Some basic results*

The leading term of $\gamma_r(x)$ is $(r!)^{-1} x^r$ and so any rational polynomial $r(x)$ of degree M can be expressed as $\sum a_i \gamma_i(x)$, where $a_i \in \mathbb{Q}$, and the summation is for $0 \leqslant i \leqslant M$. But for $r, s \in \mathbb{Z}, r \geqslant 0$ we have that $\gamma_r(s) \in \mathbb{Z}$ and $\gamma_r(r) = 1$, while $\gamma_r(s) = 0$ for $0 \leqslant s < r$. By successively substituting $x = 0, 1, 2, \dots, M$ it follows that when $r(x)$ is numerical over R, then all $a_i \in R$.

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

Lemma 2.1. *Let* $q \in \mathbb{Z}_{(p)}$. *Then* $\gamma_r(q) \in \mathbb{Z}_{(p)}$.

Proof. Let $q = u/v$ in lowest terms and so v is prime to p. Then $\gamma_r(vx)$ is a numerical polynomial over $\mathbb{Z}$ of degree r. Thus $\gamma_r(vx) = \sum a_i \gamma_i(x)$ with $a_i \in \mathbb{Z}$ and $0 \leqslant i \leqslant n$. Also $a_r = v^r$, as is seen by comparing coefficients of x^r. As $\gamma_0(q) = 1$ or $\gamma_1(q) = q$, it can be assumed inductively that $\gamma_i(q) \in \mathbb{Z}_{(p)}$ for $i < r$. Setting $x = q$ in the expression for $\gamma_r(vx)$ and rearranging gives $\gamma_r(q) = v^{-r}\{\gamma_r(u) - \sum a_i \gamma_i(q)\}$, where the sum is for $1 \leqslant i < r$. Hence $\gamma_r(q) \in \mathbb{Z}_{(p)}$.

A less elementary but more elegant proof uses the p-adic integers.

Proof of Proposition 1.1. One can establish this result using difference operators, but the proof below extends the argument of the introduction to this section.

The set of elements $\{\gamma_{i_1}(x_1)\gamma_{i_2}(x_2)\ldots\gamma_{i_n}(x_n)\}, i_k \geqslant 0$, are linearly independent over R, as they have distinct leading terms.

Let $r(\underline{x})$ be a numerical polynomial in n-variables over R of degree M. One can therefore write

$$r(\underline{x}) = \sum a_{i_1, i_2, \ldots, i_n} \gamma_{i_1}(x_1)\gamma_{i_2}(x_2)\ldots\gamma_{i_n}(x_n)$$

with $a_{i_1, i_2, \ldots, i_n} \in \mathbb{Q}$ and $I = i_1 + i_2 + \ldots + i_n \leqslant M$. By setting $\underline{x} = \underline{0}$, it follows that $a_{0,0,\ldots,0} \in R$. So that it can be assumed that $a_{i_1, i_2, \ldots, i_n} \in R$ whenever $I < P$; let $j_1 + j_2 + \ldots + j_n = P$. Then

$$r(j_1, j_2, \ldots, j_n) = a_{j_1, j_2, \ldots, j_n} + \sum a_{i_1, i_2, \ldots, i_n} \gamma_{i_1}(j_1)\gamma_{i_2}(j_2)\ldots\gamma_{i_n}(j_n),$$

where the summation is for $I < P$. Therefore $a_{j_1, j_2, \ldots, j_n} \in R$.

In the remainder of this section and in Section 3, attention will be restricted to numerical polynomials over $\mathbb{Z}_{(p)}$. Proposition 1.3 will be proved by induction on n. It follows that it can and will be assumed that when a numerical M-form is expressed in standard form as in (2), in each term of the sum, $i_k > 0$ for $1 \leqslant k \leqslant n$. Otherwise, if there is a term in which $i_k = 0$, by setting $x_k = 0$ one has a numerical M-form in $(n-1)$-variables. So if N is defined by $M = N + n - 1$, as after the statement of Theorem 1.2, then whenever $k!$ occurs in a denominator of (2) it follows that $k \leqslant N$.

Let the positive integer k have p-adic expansion $k = a_0 + a_1 p + \ldots + a_s p^s$, where $0 \leqslant a_i \leqslant p-1$, and set $\alpha(k) = \sum a_i$. Repeated use will be made of the well-known formula

$$v(k!) = \frac{k - \alpha(k)}{m} \quad \text{for } m = p - 1.$$

So if $p^{k+1} - 1 > N \geqslant p^k - 1$ and $1 \leqslant k \leqslant N$ then $\alpha(k) < m(t+1)$ and so

$$\frac{k}{m} > v(k!) > \frac{k}{m} - (t+1). \tag{3}$$

DEFINITION 2.2. Let $\gamma_r(x, y) = (r!)^{-1} x(x-y)\ldots(x-(r-1)y)$ for $r > 0$.

So $\gamma_r(x, 1) = \gamma_r(x)$. It is clear that $\gamma_r(x, y)$ is not a numerical form, but by Lemma 2.1, $\gamma_r(k, l) \in \mathbb{Z}_{(p)}$ whenever $k, l \in \mathbb{Z}_{(p)}$ and l is a unit. The first inequality in (3) implies that when $k, l \in \mathbb{Z}_{(p)}$ with $k \neq 0$ and neither is a unit, $\gamma_r(k, l) \in \mathbb{Z}_{(p)}$.

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

Let $r(\underline{x})$ be a rational M-form in n-variables which is not necessarily numerical (but assume that each x_i occurs to a positive power in each monomial of $r(\underline{x})$). So $r(x_1, \dots, x_{s-1}, 1, x_{s+1}, \dots, x_n)$ is a rational polynomial of degree less than M in $(n-1)$-variables. This latter will be denoted by $r_s(\underline{x})$ and can be written as

$$r_s(\underline{x}) = \sum b_{j_1, \dots, j_{s-1}, j_{s+1}, \dots, j_n} \gamma_{j_1}(x_1) \dots \gamma_{j_{s-1}}(x_{s-1}) \gamma_{j_{s+1}}(x_{s+1}) \dots \gamma_{j_n}(x_n), \tag{4}$$

where $b_{j_1, \dots, j_{s-1}, j_{s+1}, \dots, j_n} \in \mathbb{Q}$ and $J = j_1 + \dots + j_{s-1} + j_{s+1} + \dots j_n < M$. The original $r(\underline{x})$ can be recovered from $r_s(\underline{x})$ by making the latter homogeneous of degree M; that is, by multiplying each of its monomials by the appropriate power of x_s. Writing $r^{(s)}(\underline{x})$ for the resulting expression

$$\begin{aligned} r^{(s)}(\underline{x}) = \sum b_{j_1, \dots, j_{s-1}, j_{s+1}, \dots, j_n} \gamma_{j_1}(x_1, x_s) \\ \dots \gamma_{j_{s-1}}(x_{s-1}, x_s) \gamma_{j_{s+1}}(x_{s+1}, x_s) \dots \gamma_{j_n}(x_n, x_s) x_s^{M-J}. \end{aligned} \tag{5}$$

We therefore have n alternative expressions for $r(\underline{x})$, namely,

$$r(\underline{x}) = r^{(1)}(\underline{x}) = r^{(2)}(\underline{x}) = \dots = r^{(n)}(\underline{x}). \tag{6}$$

If $r(\underline{x})$ is a numerical M-form over $\mathbb{Z}_{(p)}$, then the coefficients $\{b_{j_1, \dots, j_{s-1}, j_{s+1}, \dots, j_n}\}$ of (4) and (5) lie in $\mathbb{Z}_{(p)}$. It is a converse statement which is of interest.

PROPOSITION 2.3. *Let $r(\underline{x})$ be a rational M-form in n-variables and assume that $r_s(\underline{x})$ is a numerical polynomial for $1 \leqslant s \leqslant n$. Then $r(\underline{x})$ is a numerical M-form.*

Proof. Proposition 1.1 implies that the coefficients in (4) lie in $\mathbb{Z}_{(p)}$. If $r(\underline{x})$ is evaluated at $\underline{a} = (a_1, a_2, \dots, a_n)$ and a_s is a unit, then $r^{(s)}(\underline{a}) \in \mathbb{Z}_{(p)}$ by remarks following Definition 2.2, that is, $r(\underline{a}) \in \mathbb{Z}_{(p)}$. Otherwise all a_i in $\underline{a}$ are non-units and any $r^{(s)}(\underline{a}) \in \mathbb{Z}_{(p)}$, again by comments following Definition 2.2. So $r(\underline{x})$ is a numerical M-form.

An example when $p = 2$ illustrating that in Proposition 2.3 it is necessary that $r_s(\underline{x})$ is a numerical polynomial for all s in $1 \leqslant s \leqslant n$, is

$$\frac{x_1(x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n)}{2}.$$

When $n = 1$, a numerical M-form can be written as $b x_1^M$ with $b \in \mathbb{Z}_{(p)}$. If this is expressed in standard form as $a_1 x^N / N!$, then $v(a_1) \geqslant v(N!) > m^{-1}M - (t+1)$ by (3). So Proposition 1.3 is proved, setting $u_1(z) = m(z+1)$ and $v_1(z) = m$. The first non-trivial case of Proposition 1.3 occurs with $n = 2$ and this will be discussed to motivate the argument in the general case.

Let $r(\underline{x})$ be a numerical M-form with $n = 2$. For the remainder of this section, $\underline{x} = (x, y)$. From (1), (2), (5) (with $s = 1$ and $s = 2$) and (6), we have four different expressions for $r(\underline{x})$, as follows:

$$\left.\begin{aligned} &\text{(i)} \quad r(\underline{x}) = \sum a_{i,j} \gamma_i(x) \gamma_j(y), \text{where } i + j \leqslant M = N + 1, \\ &\text{(ii)} \quad r(\underline{x}) = \sum a_{i,j} \frac{x^i}{i!} \frac{y^j}{j!}, \text{where } i + j = M, \\ &\text{(iii)} \quad r^{(1)}(\underline{x}) = \sum a_{1,j} \gamma_j(y, x) x^{M-j}, \text{where } 1 \leqslant j \leqslant N, \\ &\text{(iv)} \quad r^{(2)}(\underline{x}) = \sum a_{i,1} \gamma_i(x, y) y^{M-i}, \text{where } 1 \leqslant i \leqslant N. \end{aligned}\right\} \tag{7}$$

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

It is the coefficients in (ii) that concern us. The numerical form is determined by the N coefficients which occur in (ii), (iii) or (iv) and we exploit the relationships among them to obtain the required divisibility conditions. By substituting particular values for x and y in (ii), it is not difficult to check that when i or j is small compared with M, then $a_{i,M-i}$ and $a_{M-j,j}$ are divisible by a high power of p; it is the terms 'in the middle' which cause the problem.

The proof of Proposition 1.3 proceeds in three steps which are now described; some details are left to be considered in the general case. Proposition 2.3 is used only for $n > 2$.

First by considering (7)(ii) and (iv), it is established that

$$p^{qt}\frac{a_{q,M-q}}{q!(M-q)!}\in\mathbb{Z}_{(p)}. \tag{8}$$

For example by equating coefficients of xy^N, one has

$$\frac{a_{1,N}}{N!}=(-1)^{N-1}\left\{\frac{a_{N,1}}{N}-\frac{a_{N-1,1}}{N-1}+\ldots+(-1)^{N-1}a_{1,1}\right\}.$$

But $p^t/k\in\mathbb{Z}_{(p)}$ whenever $k\leqslant N$. So $p^t a_{1,N}/(N!)\in\mathbb{Z}_{(p)}$, which is (8) for $q=1$. The general proof is contained in Lemma 3.2.

The second step is to use (8) and (7)(iii) to show that

$$p^{qt}\frac{a_{1,M-q}}{(M-q)!}\in\mathbb{Z}_{(p)}. \tag{9}$$

This result will be used in Section 3 and so it is now proved by induction on q.

When $q=1$, the coefficient of xy^{M-1} in (7)(iii) comes from $a_{1,M-1}\gamma_N(y,x)\,x$ and is $a_{1,M-1}/(M-1)!$. So by (8), $p^t a_{1,M-1}/(M-1)!\in\mathbb{Z}_{(p)}$. In general, the coefficient of $x^q y^{M-q}$ in (7)(iii) arises from the terms

$$a_{1,M-1}\gamma_N(y,x)\,y+a_{1,M-2}\gamma_{N-1}(y,x)\,y^2+\ldots+a_{1,M-q}\gamma_{N-q}(y,x)\,x^q.$$

Therefore, for some $b_{M-s}\in\mathbb{Z}_{(p)}$, this coefficient is

$$\frac{a_{1,M-1}}{(M-1)!}b_{M-1}+\frac{a_{1,M-2}}{(M-2)!}b_{M-2}+\ldots+\frac{a_{1,M-(q-1)}}{(M-(q-1))!}b_{M-(q-1)}+\frac{a_{1,M-q}}{(M-q)!}$$

and must equal $a_{q,M-q}/q!(M-q)!$. Thus, combining (9) for values less than q and (8) gives $\{(M-q\}!\}^{-1}p^{qt}a_{1,M-q}\in\mathbb{Z}_{(p)}$ as required.

The proof of Proposition 1.3 for $n=2$ is completed as follows. Let $v(a_{c,d})=\beta$ where $c+d=M$. So the exponent of p in the coefficient of $x^c y^d$ in (7)(ii) is

$$\beta-v(c!)-v(d!)<\beta-\frac{(c+d)}{m}+2(t+1)\quad\text{(by (3))}$$

$$=\beta-\frac{M}{m}+2(t+1).$$

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

Let e_j be the coefficient of $x^c y^d$ in $a_{1,j}\gamma_j(y,x)\,x^{M-j}$ of (7)(iii). For any rational numbers q_1 and q_2 we have $v(q_1+q_2)\geqslant \min\{v(q_1), v(q_2)\}$. So comparing coefficients of $x^c y^d$ in (7)(ii) and (iii), there must exist some j_0 with

$$v(e_{j0}) < \beta - M/m + 2(t+1). \tag{10}$$

But when $j \leqslant M - m(\beta+2(t+1))$, as the denominator of $\gamma_j(y,x)\,x^{M-j}$ is $j!$ and using (3), we have

$$v(e_j) \geqslant -v(j!) > -j/m \geqslant \beta - M/m + 2(t+1).$$

So $j_0 > M - m(\beta+2(t+1))$, or, setting $j_0 = M - q_0$, we have $q_0 < m(\beta+2(t+1))$. But by (9), $\{(M-q_0)!\}^{-1} p^{q_0 t} a_{1,M-q_0} \in \mathbb{Z}_{(p)}$ and so $v(e_{j_0}) \geqslant -q_0 t > -mt(\beta+2(t+1))$. Combining the latter with (10) gives

$$\beta - M/m + 2(t+1) > -mt(\beta+2(t+1))$$

or

$$(1+mt)\beta > M/m - 2(t+1)(mt+1)$$

or

$$\beta > (M - 2m(t+1)(mt+1))/m(1+mt).$$

This establishes Proposition 1.3 for $n=2$, with $u_2(z) = 2m(z+1)(mz+1)$ and $v_2(z) = m(1+mz)$. In fact, the general form of the argument we shall give in Section 3, derives slightly less efficient values for $u_2(z)$ and $v_2(z)$ resulting from the inequalities of (3).

3. *The proof of Proposition* 1.3

LEMMA 3.1. (a) *Let $c_{r,l}$ be the coefficient of $x^l y^{r-l}$ in $\gamma_r(x,y)$ for $1 \leqslant r \leqslant N$. Then $p^{lt} c_{r,l} \in \mathbb{Z}_{(p)}$.*

(b) *Let $d_{r,l}$ be the coefficient of $(x^{r-l}/(r-l)!)\,y^l$ in $\gamma_r(x,y)$ for $1 \leqslant r \leqslant N$. Then $p^{lt} d_{r,l} \in \mathbb{Z}_{(p)}$.*

Proof. (a) Multiplying out $(r!)^{-1} x(x-y)\dots(x-(r-1)y)$ without assembling terms, it follows that

$$c_{r,l} = \sum \pm \frac{\alpha_1 \alpha_2 \dots \alpha_{r-1}}{r!} \quad \text{(where the } \alpha_i \text{ are distinct and } 1 \leqslant \alpha_i \leqslant r-1\text{)}$$

$$= \sum \pm \frac{1}{\beta_1 \beta_2 \dots \beta_l} \quad \text{(where } 1 \leqslant \beta_i \leqslant r\text{)}.$$

As $p^t/\beta_i \in \mathbb{Z}_{(p)}$ it follows that $p^{lt} c_{r,l} \in \mathbb{Z}_{(p)}$.

Part (b) just says that $p^{lt}/((r-l+1)(r-l+2)\dots r) \in \mathbb{Z}_{(p)}$.

Let $r(\underline{x})$ be a numerical M-form in n variables and write $r(\underline{x}) = \sum x_n^l\, Q^l(\underline{x}')$, where $Q^l(\underline{x}')$ is a homogeneous rational polynomial of degree $M-l$ in $\{x_1, x_2, \dots, x_{n-1}\}$.

LEMMA 3.2. *With notation as above, $p^{lt} Q^l(\underline{x}')$ is a numerical $(M-l)$-form.*

Proof. When $n=2$, this is the same statement as (8) since any numerical 1-form equals $b x^{M-l}$ for $b \in \mathbb{Z}_{(p)}$.

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

Let $1 \leqslant s \leqslant n-1$ and consider $r^{(s)}(\underline{x})$ as in (5). In each term of the summation of (5), the powers of x_n arise only from the term $\gamma_{j_n}(x_n, x_s)$. So with $c_{r,l}$ as in Lemma 3.1(a),

$$Q^l(\underline{x}') = \sum b_{j_1,\dots,j_{s-1},j_{s+1},\dots,j_n} \gamma_{j_1}(x_1, x_s) \dots \gamma_{j_{s-1}}(x_{s-1}, x_s) \gamma_{j_{s+1}}(x_{s+1}, x_s)$$
$$\dots \gamma_{j_{n-1}}(x_{n-1}, x_s) c_{j_n - l, l} x_s^{M-J+(j_n-l)},$$

where $b_{j_1,\dots,j_{s-1},j_{s+1},\dots,j_n} \in \mathbb{Z}_{(p)}$ as $r(\underline{x})$ is a numerical form. When $n = 2$, this gives $p^{lt}Q^l(x_1) = \sum b_{j_2} p^{lt} c_{j_2-l,l} x_1^{M-l}$ and the result follows from Lemma 3.1(a). When $n > 2$, then $p^{lt}Q_s^l(\underline{x}')$, in the notation of (4), is a numerical polynomial for $1 \leqslant s \leqslant n-1$, again using Lemma 3.1(a). Therefore by Proposition 2.3, $p^{lt}Q^l(\underline{x}')$ is a numerical $(M-l)$-form in $(n-1)$-variables.

It will be assumed inductively that Proposition 1.3 is established with fewer than n-variables, $n > 1$. So when $p^{lt}Q^l(\underline{x}')$ is expressed in the standard form (2), the coefficients of the form are all divisible by a power of p with exponent which exceeds

$$\frac{M-l-u_{n-1}(t')}{v_{n-1}(t')} \quad \text{for } p^{t'+1}-1 > N-1 \geqslant p^{t'}-1.$$

As $u_{n-1}(z)$ and $v_{n-1}(z)$ are monotonically increasing, t' can be replaced by t in this expression, where $p^{t+1}-1 > N \geqslant p^t - 1$.

Let $w_l = (M-l-u_{n-1}(t))/v_{n-1}(t) - lt$. So if $r(\underline{x})$ is expressed as

$$r(\underline{x}) = \sum d_{i_1,i_2,\dots,i_{n-1},l} \frac{x_1^{i_1}}{i_1!} \frac{x_2^{i_2}}{i_2!} \dots \frac{x_{n-1}^{i_{n-1}}}{i_{n-1}!} x_n^l,$$

by Lemma 3.2

$$v(d_{i_1,i_2,\dots,i_{n-1},l}) > w_l. \tag{11}$$

In the next lemma, the 'lth summand of $r^{(n)}(\underline{x})$' denotes the terms in (5) with $M-J = l$ and the notation of (5) is used in the statement.

LEMMA 3.3. *In the lth summand of $r^{(n)}(\underline{x})$, each $v(b_{j_1,j_2,\dots,j_{n-1}}) > w_l$.*

Proof. When $n = 2$ we have $r^{(2)}(\underline{x}) = \sum b_{j_1} \gamma_{j_1}(x_1, x_2) x_2^{M-j_1}$ and therefore $b_{j_1} = a_{M-j_1,1}$ of (7)(iv). By the 'dual' of (9), $\{(M-j_1)!\}^{-1} p^{j_1 t} a_{M-j_1,1} \in \mathbb{Z}_{(p)}$. So

$$v(b_l) \geqslant v((M-l)!) - lt \geqslant (M-l)/m - (t+1) - lt = w_l,$$

using (3), as $u_1(z) = m(t+1)$ and $v_1(z) = m$.

For $n > 2$, the argument is by induction on l. When $l = 1$, only the first summand of (5) has a term involving $x_1^{j_1} x_2^{j_2} \dots x_{n-1}^{j_{n-1}} x_n$ and these are

$$\sum b_{j_1,j_2,\dots,j_{n-1}} \frac{x_1^{j_1}}{j_1!} \frac{x_2^{j_2}}{j_2!} \dots \frac{x_{n-1}^{j_{n-1}}}{j_{n-1}!} x_n.$$

Setting $x_n = 1$ and after multiplying through by p^t, this is a numerical form, by Lemma 3.2. So by the induction hypothesis on n, we have

$$v(b_{j_1,j_2,\dots,j_{n-1}}) > (M-1-u_{n-1}(t))/v_{n-1}(t) - t,$$

as required.

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

Assume that the result is established for $1 \leqslant l < r$ and consider the lth summand of $r^{(n)}(\underline{x})$, that is,

$$\sum b_{k_1, k_2, \dots, k_{n-1}} \gamma_{k_1}(x_1, x_n)\, \gamma_{k_2}(x_2, x_n) \dots \gamma_{k_{n-1}}(x_{n-1}, x_n)\, x_n^l.$$

By Lemma 3.1(b), the coefficient of

$$\frac{x_1^{j_1}}{j_1!}\frac{x_2^{j_2}}{j_2!}\cdots\frac{x_{n-1}^{j_{n-1}}}{j_{n-1}!}x_n^{r-l}$$

in $\gamma_{k_1}(x_1, x_n) \dots \gamma_{k_{n-1}}(x_{n-1}, x_n)$ lies in $\mathbb{Z}_{(p)}$ after multiplication by $p^{(r-l)t}$. As $v(b_{k_1, k_2, \dots, k_{n-1}}) > w_l$ by the inductive assumption, the coefficients of

$$\frac{x_1^{j_1}}{j_1!}\frac{x_2^{j_2}}{j_2!}\cdots\frac{x_{n-1}^{j_{n-1}}}{j_{n-1}!}x_n^{r}$$

in the lth summand have exponent of p greater than $w_l - t(r-l) > w_r$. The coefficient of this same term in the rth summand of $r^{(n)}(\underline{x})$ is $b_{j_1, j_2, \dots, j_{n-1}}$. But by (11), $v(d_{j_1, j_2, \dots, j_{n-1}, r}) > w_r$. Therefore $v(b_{j_1, j_2, \dots, j_{n-1}}) > w_r$ as required.

The proof of Proposition 1.3. Let $v(a_{k_1, k_2, \dots, k_n}) = \beta$. So the exponent of p in the coefficient of $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ in $r(\underline{x})$, by (3), is

$$\beta - v(k_1!) - v(k_2!) - \cdots - v(k_n!) < \beta - M/m + n(t+1).$$

Let $r \leqslant M - m(\beta + n(t+1))$. For any positive integers u and v we have

$$v((u+v)!) \geqslant v(u!) + v(v!)$$

and so when $r = j_1 + j_2 + \dots + j_{n-1}$, it follows that

$$-v(j_1!) - v(j_2!) - \dots - v(j_n!) \geqslant -v(r!) > -r/m \geqslant \beta + n(t+1) - M/m.$$

So, as in the proof at the end of Section 2, there must be a term in the q_0th summand of $r^{(n)}(\underline{x})$ with $q_0 < m(\beta + n(t+1))$, where the p-primary exponent of the coefficient of $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ is no greater than $\beta + n(t+1) - M/m$; that is

$$v(b_{j_1, j_2, \dots, j_{n-1}}) - v(j_1!) - v(j_2!) - \dots - v(j_{n-1}!) \leqslant \beta + n(t+1) - M/m.$$

But by (3), $v(j_1!) + v(j_2!) + \cdots + v(j_{n-1}!) < M/m$ and using Lemma 3.3, this gives $w_{q_0} - M/m < \beta + n(t+1) - M/m$. So

$$\begin{aligned}\beta + n(t+1) &> \frac{M - q_0 - u_{n-1}(t)}{v_{n-1}(t)} - q_0 t \\ &> \frac{M - m(\beta + n(t+1)) - u_{n-1}(t)}{v_{n-1}(t)} - mt(\beta + n(t+1)).\end{aligned}$$

This simplifies to $\beta > (M - u_n(t))/v_n(t)$, where

$$v_n(t) = (1+mt)\, v_{n-1}(t) + m = ((1+mt)^n - 1)/t \quad \text{with } v_1(t) = m,$$

and

$$\begin{aligned}u_n(t) &= u_{n-1}(t) + n(t+1)\, v_n(t) \\ &= \frac{(t+1)(1+mt)}{m^2 t}\frac{d}{dt}\{v_{n+1}(t)\} - \frac{n(n+1)}{2}\frac{(t+1)}{t} \quad \text{with } u_1(t) = m(t+1).\end{aligned}$$

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

4. *Concluding comments*

First it is established that $\Delta(1,2,\dots,n)$ and $\Delta(1,3,\dots,2n-1)$ are numerical $\frac{1}{2}n(n+1)$ and n^2-forms respectively over $\mathbb{Z}$.

Let J be the linear space of numerical polynomials in n-variables over $\mathbb{Z}$. Let I_M be the subspace of numerical M-forms. If $r(\underline{x})\in J$, then $r(\underline{x})\in I_M$ if and only if $r(k\underline{x}) = k^M r(\underline{x})$ for all $k\in\mathbb{Z}$. We define V to be the free $\mathbb{Z}$-module on $\{\gamma_i(\xi)\}$ for $i\geqslant 1$ and so $\Lambda^n V$ has a basis $\{\gamma_{i_1}(\xi)\gamma_{i_2}(\xi)\dots\gamma_{i_n}(\xi)\}$ with $i_1<i_2<\dots<i_n$. The skew-symmetrisation homomorphism $s\colon \Lambda^n V\to J$ is determined by

$$s(\gamma_{i_1}(\xi)\gamma_{i_2}(\xi)\dots\gamma_{i_n}(\xi)) = \sum \varepsilon_\sigma \sigma(\gamma_{i_1}(x_1)\gamma_{i_2}(x_2)\dots\gamma_{i_n}(x_n)),$$

where σ runs over the symmetric group Σ_n and acts on the subscripts of the γ_{i_j} and ε_σ is the sign of the permutation. Then

$$s(\gamma_{i_1}(k\xi)\gamma_{i_2}(k\xi)\dots\gamma_{i_n}(k\xi)) = \sum \varepsilon_\sigma \sigma(\gamma_{i_1}(kx_1)\gamma_{i_2}(kx_2)\dots\gamma_{i_n}(kx_n))$$

for all $k\in\mathbb{Z}$. Clearly $\gamma_1(k\xi)\gamma_2(k\xi)\dots\gamma_n(k\xi) = k^{n(n+1)/2}\gamma_1(\xi)\gamma_2(\xi)\dots\gamma_n(\xi)$ and so $s(\gamma_1(\xi)\gamma_2(\xi)\dots\gamma_n(\xi)) = \Delta(1,2,\dots,n)$ is a numerical $\frac{1}{2}n(n+1)$-form.

But this procedure can be strengthened. Let

$$\delta_q(x) = \gamma_{2q-1}(x+q-1) = \frac{x(x^2-1)(x^2-2^2)\dots(x^2-(q-1)^2)}{(2q-1)!}$$

as in [**5**]. Then $\delta_q(x)$ is an odd numerical polynomial over $\mathbb{Z}$ and $\delta_q(kx)$ is an integral linear combination of the $\delta_i(x)$ for $i\leqslant q$ with leading term $k^{2q-1}\delta_q(x)$. Hence

$$s(\delta_1(k\xi)\delta_2(k\xi)\dots\delta_n(k\xi)) = k^{n^2}\delta_1(\xi)\delta_2(\xi)\dots\delta_n(\xi)$$

and $s(\delta_1(\xi)\delta_2(\xi)\dots\delta_n(\xi)) = \Delta(1,3,\dots,2n-1)$ is a numerical n^2-form over $\mathbb{Z}$.

The referee has suggested a more direct argument. The use of elementary row operations establishes that

$$\det(x_j^i/i!) = \det(\gamma_i(x_j)) \quad\text{and}\quad \det(x_j^{2i-1}/(2i-1)!) = \det(\delta_i(x_j)),$$

where in each case $i,j = 1,2,\dots,n$. The left-hand side of each equation is homogeneous and the right-hand side is numerical.

Finally, we remark that an area of mathematics where numerical polynomials arise frequently is algebraic topology, particularly in the homotopy theory of Lie groups. The argument immediately above gives the algebraic content of a stable topological transfer map suggested by Michael Crabb. The author's original interest in determining $K_2(n,1)$ arose in trying to establish certain non-splitting results in stable homotopy theory for classical Lie groups. If T is an n-torus, the complex K-homology Pontrjagin ring $K(BT)$ can be identified with J. The linear space I_M coincides with the eigenspace of the dual Adams operators ψ_k with $k>1$, corresponding to eigenvalue k^M and lies naturally inside $H_{2M}(BT)$. Theorem 1.2 implies that for any fixed r, all eigenvectors of ψ_k are zero in $H_{2M}(BT,\mathbb{Z}/p^r\mathbb{Z})$ for sufficiently large M. There are also connections with the dual Peterson conjecture on the subring of elements of $H_*(BT,\mathbb{Z}/2\mathbb{Z})$ annihilated by all Steenrod squares of

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press

positive degree. In particular, setting $r = 1$ above and using the fact that all Steenrod squares of positive degree vanish on any such class in $H_{2M}(BT, \mathbb{Z}/2\mathbb{Z})$, the main theorem of [**7**] implies that $K_2(n, 1)$ is an integer of the form $2^{\alpha_1} + 2^{\alpha_2} + \ldots + 2^{\alpha_n} - n$, where each $\alpha_i \geqslant 0$.

The author is grateful for the hospitality provided by the SFB 170 at Göttingen during the autumn of 1993 when a first draft [**3**] of this paper for the prime 2 was written. Thanks are due to Michael Crabb for his comments, particularly for those which led to the examples in Section 4, and also to the referee for several useful suggestions.

References

1. A. Baker, F. Clarke, N. Ray and L. Schwartz, 'On the Kummer congruences and the stable homotopy of *BU*', *Trans. Amer. Math. Soc.* 316 (1989) 385–432.
2. J. Hubbuck, 'Hopf structures on Stiefel manifolds', *Math. Ann.* 262 (1983) 529–547.
3. J. Hubbuck, 'On numerical forms', Mathematica Gottingensis 3 (1994) 1–12.
4. K. Knapp, 'Some applications of *K*-theory to framed bordism, *e*-invariant and transfer', Habilitationsschrift, Bonn, 1979.
5. J. McCall, Ph.D. Thesis, Aberdeen, 1990.
6. L. Schwartz, '*K*-theorie et homotopie stable', Thesis, Université de Paris-VII, 1983.
7. R. M. Wood, 'Steenrod squares of polynomials and the Peterson conjecture', *Math. Proc. Cambridge Philos. Soc.* 105 (1989) 307–309.

Department of Mathematical Sciences
University of Aberdeen
Dunbar Street
Aberdeen AB24 3PQ

https://doi.org/10.1112/S0024610796004395 Published online by Cambridge University Press